
The Parliament of the Commonwealth of Australia

Cybersafety for Seniors: A Worthwhile Journey

Second Interim Report

Joint Select Committee on Cyber-Safety

March 2013
Canberra

© Commonwealth of Australia 2013

ISBN 978-1-74366-008-9 (Printed version)

ISBN 978-1-74366-009-6 (HTML version)

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs 3.0 Australia License.



The details of this licence are available on the Creative Commons website: <http://creativecommons.org/licenses/by-nc-nd/3.0/au/>.



Contents

Foreword	ix
Membership of the Committee	xi
Terms of reference	xiii
List of abbreviations	xiv
List of recommendations	xix
1 Introduction	1
Conduct of the inquiry	3
Online survey for seniors	4
This report	5
2 How seniors use information and communication technologies	7
How seniors are using ICT	9
Using ICT in remote, regional and rural areas	11
Computer clubs for seniors	13
Seniors and online social networking	14
Seniors' use of internet for banking and ecommerce	16
Shopping online	16
Shift of government services to the internet	17
Government initiatives to engage seniors with ICT	18
Barriers to internet access for seniors	21
The cost of ICT as a barrier for seniors	23
Concluding comments	25
3 Cybersafety risks and threats for seniors	27
Introduction	27

The nature and prevalence of cybercrime	27
Emergent cyber threats	29
Identity theft by 'phishing'	31
Computer hacking	32
Superannuation fraud and boiler room investment schemes	33
Online dating and romance scams	34
Money transfer, lottery and charity scams	35
Are seniors more at risk?	36
Wealthy or seeking wealth	37
Reluctant and online	39
Unfamiliarity with cyber 'conventions'	40
Increased social networking	42
The NBN and technology take-up	44
Seniors' responses to risk	45
Building seniors' confidence and safety online	46
Keep it simple: key messages for keeping safe	47
Keep it clear: user friendly web design and interfaces	49
Make it safe: access to computers and security advice	51
Make it easy: a single portal for reporting and advice	52
Concluding comments	55
4 Cybersafety education and training for seniors	57
Introduction	57
How seniors prefer to learn	58
Inter-generational cybersafety help	60
Cybersafety education for the most vulnerable	61
Cybersafety education for life	62
Cybersafety education currently available for seniors	63
Off-line cybersafety education for seniors	65
Incidental cybersafety education for seniors	66
Government cybersafety training initiatives	67
Suggestions for future cybersafety education and training	72
Research into appropriate cybersafety education	76
Targeting cybersafety training appropriately	78

	Overseas cybersafety training initiatives.....	78
	The cost of training.....	80
	Concluding comments	81
5	Consumer protection, regulation and enforcement.....	83
	Introduction	83
	Australia’s cybersafety framework.....	84
	Federal agencies.....	84
	State and Territory consumer protection activities	91
	Updating the law	92
	International co-operation and law enforcement	93
	Protection of personal information.....	94
	Support for enhanced protections	95
	Cross-jurisdictional collaboration.....	96
	Mandatory reporting of data breaches	98
	Secure government information systems — PCEHR	99
	Consumer awareness measures	102
	Central collection and analysis of data.....	105
	Concluding comments	107
6	The role of industry.....	109
	Introduction	109
	Building productive capacity under a digital economy	110
	Industry security and consumer protection codes	111
	Mandatory codes for industry?	114
	Self-regulation and data monitoring.....	115
	ISPs, data monitoring and ‘walled gardens’	116
	Private networks.....	119
	Regulating online transactions and money transfer.....	120
	The obligations of banks	120
	Online shopping and money transfer	122
	Industry’s cybersafety services to seniors.....	122
	Privacy and security advice.....	123
	Defensive web design	125

Product training and technical support	127
Computer and security product costs	128
Raising industry’s cybersafety and security awareness	129
Industry/government partnerships for cybersafety	131
Bringing all partners together	133
Concluding comments	135
7 Concluding comments	137
Appendix A — Submissions	141
Appendix B — Exhibits	145
Appendix C — Witnesses	147
Appendix D — Online survey evaluation	153
The survey	153
Launching and advertising the survey	153
Closing the survey	154
YOURLifeChoices survey	154
Other research	155
Discussion of responses to the Committee’s survey	155
Who completed the survey	155
How seniors use the internet	155
How seniors acquire their online skills	158
How safe do seniors feel when online?	161
Scams and internet fraud	163
Seniors’ perception of government involvement	165
Education about cybersafety and regulation	166
Concluding comments	168
Appendix E — Online resources	169
Appendix F – Phishing Scam	171

LIST OF TABLES

Table 1	Question: Do you have a computer at home?.....	154
Table 2	Question: What do you use the internet for?.....	155
Table 3	Question: Where did you acquire your computer skills?	157
Table 4	Question: Where did you acquire your computer skills?	158
Table 5	Question: Do you find using the internet difficult or frustrating?.....	158
Table 6	Question: Are you worried about online safety?.....	160
Table 7	Question: Have you been affected by e-mail scams, identity theft or fraud?.....	161
Table 8	Question: Level of comfort accessing Government information/services online	163
Table 9	Questions on Education and regulation	164



Foreword

Cyber technology has developed dramatically in the last 20 years and the internet and other new communications technologies have infiltrated our lives in ways most of us would not have imagined only a few years ago. Australians are now communicating with government, business, family and friends, as well as shopping and banking, online. While many senior Australians may have been reluctant to venture into the cyber world initially, seniors are now the fastest growing online user group in the country.

Anyone who uses the internet is vulnerable to cyber security threats but the Committee found that seniors are particularly vulnerable for several reasons. In the words of Dr Helen Kimberley from the Brotherhood of St Laurence, senior Australians are 'digital immigrants' not 'digital natives' as young people are. Seniors have not grown up using the technology and, in the case of the older senior cohort, they did not even have the advantage of using computers in their work before retirement. Many seniors therefore have a lot of catching up to do when it comes to being 'cyber savvy'.

Additionally, seniors are attractive targets for criminals because many seniors own substantial assets and have access to life savings and their superannuation. In many cases, seniors are looking for opportunities to invest their money, so they might be receptive to scams and fraudulent investment opportunities.

The Committee spoke to seniors who have enthusiastically embraced the internet and other communications technology, and who act safely online. However, the Committee also received a lot of evidence showing that there are many senior Australians who either are not using the internet at all, or are using it with caution, because they are afraid of becoming involved in cyber security issues. Additionally, many are now too embarrassed to admit to family and others that they have no knowledge of the internet and no idea how they would go about 'getting online'. For these seniors, education and training will be their key to becoming cyber savvy and cyber safe.

Paradoxically, it is often the seniors who could most benefit from being online in their own home – that is, the geographically isolated or those who are housebound through disability or for other reasons – who have been left behind and are not yet online. Many of these seniors are hesitant to venture into the cyber world, if indeed they even knew how to do so.


The Committee found that there is a lot of help available for seniors who want to go online, particularly in the more populated parts of the country. Many seniors' groups, public libraries and government departments around the nation are helping seniors start the journey towards being cyber savvy. Some seniors' clubs are teaching computing with a cybersafety component and some also teach dedicated cybersafety courses. The Universities of the Third Age are experiencing very high demand for their computer courses. Public libraries around the nation are doing an impressive job of helping seniors to safely use email, smartphones, social networking and to access government sites and services. Over 2,000 Broadband for Seniors kiosks are located around the nation offering free internet access and training for seniors.

At the back of this report we have included a list of on-line resources which offer cybersafety advice and guidance. As a starting point I would advise seniors with cybersafety concerns to look at the Department of Broadband, Communications and the Digital Economy's Stay Smart Online webpage or the FaHCSIA Staying-Safe-Online website. The FaHCSIA website also has information about the Broadband for Seniors kiosks.

In conclusion, I would like to express my appreciation to the Committee's Deputy Chair and my colleagues on the Committee. On behalf of the Committee, I would also like to thank the Secretariat for the enthusiasm and dedication they have shown to this inquiry. My thanks also go to everyone who sent in a submission, or appeared as a witness, either at a public hearing or at the round table in Hobart. Thanks also to each of the 536 seniors who took the time to complete the Committee's online cybersafety for seniors' survey. All of the information provided to the Committee was invaluable in the writing of this report.

The Committee has made 13 recommendations in this unanimous report, all of which we believe will improve cybersafety for senior Australians. As the report title suggests, the journey to help all seniors enjoy the benefits of being online while staying cyber-safe is a worthwhile one.

Senator Catryna Bilyk
Chair



Membership of the Committee

Chair Senator Catryna Bilyk

Deputy Chair Mr Alex Hawke MP

Members Mr Michael Danby MP

Senator David Bushby

Ms Nola Marino MP

Senator Scott Ludlam

Mr Graham Perrett MP

Senator Stephen Parry

Ms Amanda Rishworth MP

Senator Louise Pratt

Mr Tony Zappia MP

Committee Secretariat

Secretary	Mr Russell Chafer <i>(from 9/7/12)</i>
	Mr James Catchpole <i>(until 9/7/12)</i>
	Mr David Monk <i>(from 26/3/12 until 11/5/12)</i>
Inquiry Secretary	Dr Cathryn Ollif <i>(from 3/4/12)</i>
	Ms Loes Slattery <i>(until 27/3/12)</i>
Research Officers	Ms Loes Slattery <i>(14/05/12 until 6/07/2012 and from 14 /12/2012)</i>
Administrative Officers	Ms Heidi Lushtinetz
	Mrs Dorota Cooley <i>(from 23/7/12)</i>
	Ms Michaela Whyte <i>(until 20/7/12)</i>



Terms of reference

The Joint Select Committee on Cyber-Safety shall inquire and report on the cybersafety of senior Australians, and make recommendations aimed at ensuring Australian law, policy and programs represent best practice measures for the cybersafety of senior Australians. Cybersafety for senior Australians includes issues of consumer protection, such as financial security and protecting personal information, and issues involving using social networking sites safely. In particular, the Committee shall inquire into:

- a) the nature, prevalence and level of cybersafety risks and threats experienced by senior Australians;
- b) the impact and implications of those risks and threats on access and use of information and communication technologies by senior Australians;
- c) the adequacy and effectiveness of current government and industry initiatives to respond to those threats, including education initiatives aimed at senior Australians; and
- d) best practice safeguards, and any possible changes to Australian law, policy or practice that will strengthen the cybersafety of senior Australians.



List of abbreviations

ABACUS	Australian Business Assessment of Computer User Security
ABS	Australian Bureau of Statistics
ACC	Australian Crime Commission
ACCC	Australian Competition and Consumer Commission
ACFT	Australasian Consumer Fraud Taskforce
ACL	Australian Consumer Law
ACMA	Australian Communications and Media Authority
ADIs	Australian Deposit-taking Institutions
AFP	Australian Federal Police
AGIMO	Australian Government Information Management Office
A-Gs	Attorney-General's Department
AHRC	Australian Human Rights Commission
AIC	Australian Institute of Criminology
AISA	Australian Information Security Association
ALIA	Australian Library and Information Association
AO	Officer of the Order of Australia
APPs	Australia Privacy Principles

ARC	Centre of Excellence for Creative Industries and Innovation
ASCCA	Australian Seniors Computer Clubs' Association
ASIC	Australian Securities and Investments Commission
ATO	Australian Tax Office
ATM	Automated teller machine
BPAY	Bill payment service
BSOL	Brisbane Seniors Online Association
CALD	Culturally and Linguistically Diverse
CCI	Creative Industries and Innovation
C/CSPs	Carriers and carriage service providers
CDPP	Commonwealth Director of Public Prosecutions
CEO	Chief Executive Officer
CERT	Computer Emergency Response Team
CIS	Centre for Internet Safety
CLC	Communications Law Centre
CSOC	Cyber Security Operations Centre
CWP	Consultative Working Party
DBCDE	Department of Broadband, Communications and the Digital Economy
DMARC	Domain-based Message Authentication, Reporting and Conformance
DPP	Director of Public Prosecutions
EFTPOS	Electronic funds transfer at point of sale
FaHCSIA	Department of Families, Housing, Community Services and Indigenous Affairs

FECCA	Federation of Ethnic Communities' Councils of Australia
GDP	Gross Domestic Product
HTCO	High Tech Crime Operations
ICT	Information and communication technologies
IIA	Internet Industry Association of Australia
ISP	Internet Service Provider
IT	Internet technology
LACVI	Life Activities Clubs Victoria Inc.
NBN	National Broadband Network
NEHTA	National E-Health Transition Authority
NSA	National Seniors Australia
NSIPC	National Security and International Policy Group
NSLA	National & State Libraries Australasia
OCS	Online Content Scheme
PA-DSS	Payment Application Data Security Standard
PCEHR	Personally Controlled Electronic Health Record
PDF	Portable Document Format (PDF) - Adobe Reader
PINs	Personal Identification Numbers
PTS	PIN Transaction Security
PM&C	Department of the Prime Minister and Cabinet
PCI DSS	Payment Card Industry Data Security Standards
SAT	Security Analysis Toolkit
SIR	Security Incident Response
SMEs	Small and Medium Enterprises

SOIF	Serious and Organised Investment Fraud
TIO	Telecommunications Industry Ombudsman
UTS	University of Technology, Sydney
U3A	University of the Third Age
VoIP	Voice Over the Internet Protocol
VMR	Vulnerability Management and Research



List of recommendations

2 How seniors use information and communication technologies

Recommendation 1

That the Australian Government investigates innovative ways of providing low cost internet connection to financially disadvantaged housebound and geographically isolated seniors who request it.

Recommendation 2

That an advertising campaign targeting seniors be devised to alert seniors around the nation to the existence and location of the Broadband for Seniors kiosks.

Recommendation 3

That the Department of Broadband, Communications and the Digital Economy prioritise including some cybersafety information on their website in languages other than English.

3 Cybersafety risks and threats for seniors

Recommendation 4

That the Australian Government develops, as a supplement to its *Web Guide*, a web style guide prescribing the key elements of web design to ensure simplicity of language, visual clarity in design and logical navigation tools. This could be supported by graphical step-by-step tutorials for use where applicable.

Recommendation 5

In support of the previous recommendation, the Committee also recommends that, in addition to conducting compliance audits based on the web style guide requirements, the Australian Government

Information Management Office should offer an Annual Award for user friendly web design, in part based on public input on the utility of government websites.

Recommendation 6

That the Australian Government develops a centralised user friendly reporting and cybersafety awareness portal for all types of cybercrime with links to relevant regulators.

The site should feature a dedicated reporting tab, a seniors tab and be backed up by a telephone service which links individuals to appropriate victim support, training and other advice.

Recommendation 7

In support of the above, the Australian Government should investigate options for the contracting of appropriate non-government organisations or private organisations to provide support and advice to victims of online and technology related crime.

4 Cybersafety education and training for seniors

Recommendation 8

That the Australian Government advertise the Broadband for Seniors initiative widely, including:

- launching a campaign publicising the internet kiosks using seniors clubs, magazines, newspapers, radio and television; and
- widely advertising the new cybersafety telephone helpline, including on all government websites which host cybersafety information.

Recommendation 9

That the Australian Government work with the States and Territories to support public libraries or community resource centres where no public library exists, for the purpose of meeting the demand for cybersafety training for seniors.

5 Consumer protection, regulation and enforcement

Recommendation 10

That Australian Government's cyber awareness campaigns should headline clear and practical messages for cybersafety on the central reporting and awareness portal, and appear up front of all published cyber awareness material for the general community.

Recommendation 11

That the cybercrime reporting tab on the central reporting and awareness portal be designed for ease of access to users and to facilitate data collation and assessment. The system should be supported by simple online instructions and accessible to the visually and aurally impaired, and for print in hard copy.

6 The role of industry**Recommendation 12**

That the Australian Government establish a consultative working group, with wide stakeholder representation, to co-ordinate and promote government and industry partnerships and initiatives in support of a healthy and secure online environment.

Recommendation 13

That the proposed consultative working group should examine the effectiveness and promote awareness of relevant industry codes of practice, and make recommendations to governments at all levels on these matters.

Introduction

- 1.1 In June 2011, the Joint Select Committee on Cyber-Safety tabled a report in Parliament on cybersafety and the young.¹ The opening paragraph of that report spoke of the extent to which the internet now permeates our lives:

The online environment is an integral part of modern economic and social activities, and a vast resource of information, communication, education and entertainment.²

- 1.2 Following completion of that inquiry, the Committee was pleased to receive a reference from the Minister for Broadband, Communications and the Digital Economy on 23 November 2011 to conduct an inquiry and report on the cybersafety of senior Australians.
- 1.3 The terms of reference, which can be found at the start of this report, asked the Committee to make recommendations aimed at ensuring Australian law, policy and programs represent best practice measures for the cybersafety of senior Australians.
- 1.4 This reference to the Committee was timely because while senior Australians are the fastest growing online user group, research indicates that fears about risks to privacy and security prevent many seniors from participating in online activity.
- 1.5 Cyber technology has developed rapidly and dramatically in the last 20 years and the digital economy has become essential to Australia's long-

1 *High-Wire Act Cyber-Safety and the Young*, Joint Select Committee on Cyber-Safety, June 2011.

2 *High-Wire Act Cyber-Safety and the Young*, Joint Select Committee on Cyber-Safety, June 2011, p. 3.

term prosperity. The internet has infiltrated aspects of the lives of everyone, including older people in ways that they could never have expected, from communicating with government, business, family and friends, to shopping and banking.³

- 1.6 Seniors are not the only demographic who are vulnerable to security threats from the internet. All users are vulnerable, but Dr Cassandra Cross told the Committee that:

... seniors can be attractive targets for criminals for a variety of reasons. Seniors generally have access to the superannuation, life savings and own their own assets. In many cases, seniors are also looking for opportunities to invest their money, and can be easily manipulated into fraudulent transactions.⁴

- 1.7 Many seniors are competent and regular users of the internet and it is not the intention of the Committee to imply that senior Australians cannot be every bit as capable of using information technology as any other Australian. To quote Life Activities Clubs Victoria:

... there are quite a few octogenarians and nonagenarians with cyberskills that would shame many people 50 years younger.⁵

- 1.8 However, there are many seniors who have limited knowledge about how the internet operates or how to stay safe while enjoying the benefits of being online. Even where seniors have acquired computer literacy, the ever-changing nature of the digital world means that their knowledge dates at an alarming rate. As a result, many seniors tend to have knowledge gaps about the application of cyber security, and they are particularly vulnerable to myths and scams.⁶

- 1.9 In its discussion paper *Connecting with Confidence: Optimising Australia's Digital Future*⁷, the Department of Prime Minister and Cabinet makes a distinction between cybersafety, cybersecurity and cybercrime to assist in the management of cyber issues. In this report, however, the term cybersafety is used in its broadest sense, incorporating issues relating to cybersecurity and cybercrime, as well as those relating to cybersafety.

3 COTA NSW, *Submission 39*, p. 1.

4 Dr Cassandra Cross, *Submission 49*, p. 3.

5 Life Activities Clubs Victoria Inc., *Submission 5*, p. 2.

6 COTA NSW, *Submission 39*, p. 1.

7 Department of the Prime Minister and Cabinet, *Connecting with Confidence: Optimising Australia's Digital Future*, 2012, p. 30.

- 1.10 Responsibility for cybersafety is shared by many bodies, including government, not-for-profit organisations, industry and the end-users engaged in online activities and the Committee heard often during the inquiry that it is important that all sectors work together to achieve a safe digital future for senior Australians.
- 1.11 For the purpose of this inquiry, seniors are defined as anyone 55 years or older.

Conduct of the inquiry

- 1.12 In February 2012, the Committee wrote to a range of stakeholders inviting submissions to the inquiry. Those invited to submit included federal Ministers, Premiers and Chief Ministers, heads of Australian Government departments, statutory bodies and other relevant authorities, and seniors' clubs and organisations.
- 1.13 The general public was invited to make submissions. The inquiry was advertised in *The Australian* at fortnightly intervals and it was also advertised in *About the House*⁸ and via House of Representatives media releases. As the inquiry progressed, various seniors' organisations helpfully advertised the inquiry in their online newsletters.
- 1.14 A total of 49 submissions and six supplementary submissions were received. A list of submissions is at Appendix A.
- 1.15 A list of other documents of relevance to the inquiry that were formally received by the Committee as exhibits is at Appendix B.
- 1.16 The Committee took evidence at public hearings in Sydney, Melbourne and Canberra. On several occasions the Canberra public hearings included teleconferencing with people in other states. Evidence was also taken at a roundtable discussion in Hobart. While in Tasmania, the Committee visited a digital hub at the Pittwater Community Centre in Midway Point to observe a computer class for seniors.
- 1.17 A list of organisations and individuals who gave evidence to the inquiry at public hearings and at the roundtable is at Appendix C.
- 1.18 In conjunction with the inquiry, the Committee conducted an online survey of seniors. The survey is discussed below.

8 The House of Representatives' quarterly current affairs magazine which is read by 80 000 Australians from a range of age groups and backgrounds.

Online survey for seniors

- 1.19 When the inquiry into cybersafety for senior Australians was in its initial stages, the Committee decided to complement the evidence that it would take through submissions and public hearings with an online survey. The purpose of the survey was to give as many seniors as possible the opportunity to tell the Committee about their internet use and their concerns, if any, about cybersafety.
- 1.20 Questions explored how seniors use the internet, for what purposes, how they learned their computer skills and what their fears about cybersafety are.
- 1.21 The survey was accessible through the main page of the Committee's website via a 'button' labelled '*Take our online survey*'. The survey could be printed in PDF format and posted to the secretariat if preferred. This option was an attempt to capture people who, for whatever reason, did not wish to complete the survey online.
- 1.22 It is acknowledged that most of the people who responded to the survey online would typically be those who have at least enough computer skills to complete and lodge an online survey. Therefore, to try to reach seniors who may not be online, or with limited online skills, the survey was distributed by Committee Members in hard copy on those occasions when they were speaking to groups of seniors in their electorates. When completed, these could be returned to the Committee Member for forwarding to the secretariat, or they could be posted to the secretariat.
- 1.23 On the last page of the survey some demographic information was collected with questions asking about gender; age group; state or territory of address; whether the respondent lives in a metropolitan, regional, rural or remote area; and whether or not they identify as Aboriginal or Torres Strait Islander.
- 1.24 When the survey was closed in November 2012, it had received 505 online responses and 31 completed surveys were posted to the Committee in hardcopy, making a total of 536 completed surveys. An evaluation of the results of the survey is at Appendix D.
- 1.25 In some places in this report data from the survey is used to substantiate, or not, the evidence being reported. Additionally, comments from the survey responses have occasionally been quoted where they are illustrative of the point being made.

This report

- 1.26 Over the course of the inquiry the Committee took hundreds of pages of evidence in the form of submissions and during public hearings. This evidence is all available on the Committee's website.
- 1.27 During evidence gathering several themes emerged and the Committee heard them repeatedly. Briefly, they were:
- many seniors do not go online for banking or other services because they have concerns about the security of their financial and personal information;
 - many seniors who could benefit greatly from the use of online services miss out on those benefits because of their fears of online risks;
 - seniors are just as able as anyone to understand cybersafety principles given adequate training and information;
 - seniors need access to appropriate education and training to help them to be cybersafe online;
 - government could play an increased role in providing funds to those volunteer groups and public libraries which are already training seniors in cybersafety;
 - with increased funding volunteer groups and public libraries could create new, appropriate training opportunities for seniors;
 - there may be some laws and policy which could be updated to improve cybersafety for seniors; and
 - Internet Service Providers (ISPs) could play an increased role in helping seniors be cybersafe.
- 1.28 The only point above which the Committee took conflicting evidence about was the need to change Australian law. Some authorities told the Committee that the current laws are quite adequate to keep seniors cybersafe while others told the Committee that there are laws which need to be changed or amended. The adequacy of Australian law and policy is discussed in Chapter 5.
- 1.29 In the report which follows, the Committee has made 13 recommendations which reflect the Committee's findings.

How seniors use information and communication technologies

- 2.1 In the last twenty years, a revolution in information and communication technologies (ICT) has seen the internet and cyber technologies almost completely replace personal, paper-based and phone-based means of commercial and personal transactions in Australia and in most other countries. The consequence for seniors is that for those who are equipped to take part in this revolution, it will 'give rise to new, more accessible products and services satisfying the needs of older people.'¹ However, not all senior Australians are participating in the ICT revolution.
- 2.2 In a community where views and preferences are increasingly being expressed online, seniors who fear the internet will miss out on the social interaction which it provides. Likewise, as governments move towards electronic means of communication with online publications, forms and eHealth initiatives, seniors who are not online might find it increasingly difficult to access these items.²
- 2.3 The Committee found that while many seniors are enthusiastically embracing ICT, others lack confidence and have little, if any, ability to use the internet or other ICT. The speed of the information technology revolution has meant that many older Australians have found themselves 'on the wrong side of the digital divide'³ and seniors without access to email, which is increasingly becoming a necessary tool for participation in

1 The European Commission, *Ageing well in the Information Society: Action Plan on Information and Communication Technologies and Ageing* (2007) <www.europa.eu/legislation_summaries/information_society/strategies/124292_en.htm> viewed 29 November 2012.

2 Government of Western Australia, *Submission 19*, p. 4.

3 Australian Human Rights Commission (AHRC), *Submission 2*, p. 4.

society, are at risk of reduced participation in critical aspects of modern living.

2.4 Where seniors have embraced ICT, most say that access to the internet is important to them⁴ and research has found that the more time people spend online, the more comfortable they are likely to be when engaging in online activities.⁵

2.5 For housebound seniors the internet has the potential to improve the quality of their life considerably. The Australian Human Rights Commission (AHRC) said that:

With internet access to medical services, online grocery shopping, online payment of bills and social networking possibilities, older Australians can potentially live autonomously in their homes for longer.⁶

2.6 However, housebound seniors who are without internet access at home are at risk of becoming isolated and those who are not computer literate will be severely affected as business and community sectors rely more heavily than ever on ICT for disseminating and seeking information.⁷

2.7 The 2011 Australian Census found that approximately 80 per cent of dwellings have some type of internet connection.⁸ Many seniors who do not have access to the internet at home but who are mobile can access the internet at no cost at their local library's public access computers and at seniors' kiosks at various locations around the country. The Australian Library and Information Association and National & State Libraries Australasia told the Committee that:

On library floors, every day, throughout Australia, library staff are showing library patrons how to use the internet or other communications devices.⁹

4 93.5 per cent of respondents to the Committee's online survey said that 'internet access is important to my quality of life' and 87.3 per cent use the internet daily.

5 Communications Law Centre, UTS, *Submission 31*, p. 3.

6 AHRC, *Submission 2*, p. 4.

7 Australian Seniors Computer Clubs Association (ASCCA), *Submission 7*, p. 4.

8 Australian Bureau of Statistics 2011 Census of Population and Housing Australia: 1 525 108 out of 7 760 319 dwellings have no Internet connection and a further 272 257 did not answer the question: <www.censusdata.abs.gov.au/census_services/getproduct/census/2011/communityprofile/0?opendocument&navpos=230> viewed 9 January 2013.

9 Australian Library and Information Association and National & State Libraries Australasia, *Submission 6*, p. 4.

- 2.8 More than 60 per cent of Australians aged 55 to 64 use the internet, with more than 30 per cent of those over 65 spending time online.¹⁰ However, many seniors 'have high levels of concern about cybersafety, to the extent that they are either limiting the ways in which they use the internet, or not using it at all.'¹¹
- 2.9 This chapter will explore how seniors who are online use ICT and the range of reasons why some seniors are not online. The risks and threats concomitant with using ICT are discussed in Chapter 3 of this report.

How seniors are using ICT

- 2.10 The Australian Communications and Media Authority (ACMA) said that statistics from the Australian Bureau of Statistics (ABS) show an increase in overall internet participation by senior Australians but there is a marked difference between the '55–64 year olds' and the '65 years and over' group, with those aged 65 years and over having a much lower participation level or access to internet services.¹²
- 2.11 ACMA undertook research in 2010 to find out 'how and why' senior Australians were accessing the internet. The research found that Australians aged '55 and over' were most likely to use the internet for communications activities and for research and information. They were less likely than 'Australians under 55' to participate in blogs and online communities, buying/selling/shopping online, or other interactive purposes.¹³ The research identified the three main reasons for seniors not using the internet for online transactions as:
- they have no need to do so;
 - they prefer to shop in person to see the product; and/or
 - they have security concerns.¹⁴
- 2.12 However, ACMA noted that research done by the Australian Research Council Centre of Excellence for Creative Industries and Innovation in

10 Department of Health and Ageing (DoHA), *Submission 16*, p. 1.

11 National Seniors Australia (NSA), *Submission 29*, p. 1.

12 Australian Communications and Media Authority (ACMA), *Submission 24*, p. 5.

13 ACMA, *Submission 24*, p. 6.

14 ACMA, *Submission 24*, p. 6.

2011 found the reasons seniors use online communication technologies varied greatly from person to person.¹⁵

- 2.13 In its submission, the Australian Seniors Computer Clubs Association (ASCCA) advised that its members want to learn how to use the internet for a whole range of reasons: to shop, chat, research, buy and sell shares, and pay bills. One lady wanted to learn how to use a computer because at 93, she wanted to write her memoirs. With the help of her newly-learned computer skills she went on to publish two volumes.¹⁶
- 2.14 Ms Carol Bennet, CEO of Consumers Health Forum of Australia (CHF), said that those seniors who are active online are particularly likely to be among the 80 per cent of Australians who use the internet to seek health care information.¹⁷
- 2.15 The Hobart Older Persons Reference Group told the Committee that, among other uses, its members appreciate being able to download music from the internet and also to communicate with people interstate and overseas.¹⁸
- 2.16 On the other hand, Mr Malcolm Grant, Hobart Older Persons Reference Group, said that some seniors just do not want to spend their time using the internet, even though they may be highly educated and are quite capable of being savvy internet users:
- ...there are a lot of people of my generation who are not all that interested, quite frankly, and who are quite happy to use their [computer] for emailing their friends and for accessing some information, but beyond that have got other things in life, or what is left of life ... it does not necessarily have to do with one's educational background, one's ethnic background...there are people, plenty of whom are tertiary educated, who really have other things in their life as well as their daily dose of internet technology.¹⁹
- 2.17 Many seniors use the internet to research their options then revert to other forms of contact, such as the telephone or possibly posting a cheque, to

15 ACMA, *Submission 24*, p. 6.

16 ASCCA, *Submission 7*, p. 12.

17 Ms Carol Bennet, CEO, Consumers Health Forum of Australia (CHF), *Committee Hansard*, 19 September 2012, p. 1.

18 Hobart Older Persons Reference Group, Hobart City Council, *Submission 8*, p. 1.

19 Mr Malcolm Grant, Member, Hobart Older Persons Reference Group, *Committee Hansard*, 7 August 2012, p. 8.

complete the transaction. Mr Michael O'Neill, CEO of National Seniors Australia (NSA), said:

...we have noticed that people get on the internet and get quotes ...but they stop at that point and then ring...and say 'I've been on the internet. I've found your price is X. I would like to proceed with that purchase'. [When we ask why they did not complete the transaction they say] 'Oh, no I don't want to put my details on the internet. I am just not confident about that'.²⁰

- 2.18 Seniors are using Skype in large numbers, as it gives them the ability to keep in touch with their children and grandchildren if they live interstate or overseas.
- 2.19 Among seniors who do enjoy using the internet it is clear that they use it frequently. Mrs Kay Fallick reported that a survey of YOURLifeChoices' members found that 94 per cent of 2,500 responses are online daily.²¹

Using ICT in remote, regional and rural areas

- 2.20 Access to the internet can be particularly beneficial for older people living in rural, regional and remote communities who have limited alternative means of remaining engaged with the wider community. Unfortunately, access issues, cost and fear of technology means that many seniors in these areas are not benefitting as they might from ICT.
- 2.21 Numerous reports have outlined the difficulties of providing ICT to remote areas, particularly getting communication technologies into remote Indigenous communities and 'small communities experience significant limitations when it comes to communication'.²²
- 2.22 As well as experiencing a lack of reliability of internet connection in regional and rural areas, there is limited competition which means prices are relatively high and 'alternate services are not always easy to arrange'.²³

20 *Committee Hansard*, 31 October 2012, p. 2.

21 Mrs Kay Fallick, Publisher, Owner, Director, YOURLifeChoices website, newsletters and magazine, *Committee Hansard*, 18 May 2012, p. 1.

22 ARC Centre of Excellence for Creative Industries and Innovation, the Centre for Appropriate Technology and the Central Land Council, *Home Internet for Remote Indigenous Communities*, 2011, p. 20.

23 Tandara Lodge Community Care Inc., *Submission 1*, p. 1.

2.23 The Department of Broadband, Communications and the Digital Economy (DBCDE) has stated that a key objective for the National Broadband Network (NBN) is that:

...a person's ability to receive affordable high-speed broadband services should not be affected by where they live or work. The NBN will ensure that every community in regional Australia gets fair access to affordable high-speed broadband.²⁴

2.24 Public libraries are providing free internet access and tuition to rural and remote areas for those who are able to get to a library. Ms Vanessa Little from the Australian Library and Information Association (ALIA) said that:

There are libraries from Millicent in the south-east of South Australia, right through the country into the very heart of the Northern Territory offering these services to communities, particularly to seniors.²⁵

2.25 ASCCA helps rural, regional and remote Australians who would like to set up a computer club for seniors with a development kit which is available to anyone. Mrs Nancy Bosler, President of ASCCA, said that people in rural, regional and remote areas can also phone or email the Association for help.²⁶

2.26 Keeping up-to-date with changes in ICT in rural and remote areas and remaining cybersafe is an issue particularly for vulnerable groups, including Aboriginal people and older people from culturally and linguistically diverse backgrounds. The South Australian Government told the Committee that:

This inability to keep up to date with technology can in turn widen the 'digital divide' and result in social isolation from friends and family.²⁷

2.27 Commander Glen McEwen, Manager of Cyber Crime Operations with the Australian Federal Police (AFP), told the Committee that the AFP's cybercrime prevention team has worked in partnership with the Northern Territory Department of Justice to deliver the 'Strong Choices' program in remote locations. The AFP ran a number of sessions with Indigenous

24 The Department of Broadband, Communications and the Digital Economy (DBCDE), *#au20 National Digital Economy Strategy. Leveraging the National Broadband Network to drive Australia's Digital Productivity*, Canberra, 2011.

25 Ms Vanessa Little, President, ALIA, *Committee Hansard*, 9 May 2012, p. 6.

26 *Committee Hansard*, 23 March 2012, p. 16.

27 South Australian Government, *Submission 37*, p. 3.

elders, both men's and women's groups, regarding how they could assist in protecting young people online.²⁸

Computer clubs for seniors

- 2.28 The Committee heard from various seniors' groups which come together to share their knowledge of computing and to enjoy it as a pastime. Some groups offer their members a range of services and activities including computer training, which will usually include some cybersafety training and information. The African Seniors Club, for example, serves the welfare needs of the aged and ageing African population in Queensland and conducts 'small group workshops in which the members are constantly educated and trained on how best to use computers including the online and internet services'.²⁹
- 2.29 LACVI comprises 22 clubs with over 4 000 members. It told the Committee it has a focus on keeping older people active and participating in the community and many of its clubs offer computer-related activities.³⁰
- 2.30 The peak body for seniors' computer clubs, ASCCA has more than 156 member clubs and is run by seniors for seniors. It assists older and disabled Australians to access computer technology. ASCCA told the Committee that it helps start new clubs and it advises and assists existing clubs. Also, it provides:
- ...a channel for communication between likeminded people, who want to share in the potential of the computer age to serve their individual and community goals.³¹
- 2.31 ASCCA has created a development kit to help seniors set up a computer club. The kit is free and available on ASCCA's website. It takes people through the process of forming a club from the start and also offers email or telephone help. Mrs Bosler said that 'every aspect they need for setting up that club is available'.³²
- 2.32 There are numerous computer clubs in retirement complexes. Mrs Bosler told the Committee that:
- ...larger groups such as the Anglican retirement villages have been very supportive in helping to get internet access and

28 *Committee Hansard*, 13 March 2013, p. 2.

29 African Seniors Club – Australia Inc., *Submission 18*, p. 3.

30 Life Activities Clubs Victoria Inc. (LACVI), *Submission 5*, p. 1.

31 ASCCA, *Submission 7*, p. 10.

32 *Committee Hansard*, 23 March 2012, p. 16.

computer training into their facilities... We must make sure that we do not eliminate any section of the aged community – and that means those in aged care facilities and even those in nursing homes.³³

- 2.33 The Committee heard from various witnesses that ‘seniors helping seniors is a most effective medium’³⁴ when it come to passing on cybersafety tips and advice. The Brotherhood of St Laurence noted that socially isolated seniors would be helped by:

Government support and funding to recruit technically savvy older people to run internet workshops in places such as libraries, neighbourhood houses and men’s sheds [and it] would improve people’s ability to use the internet safely.³⁵

- 2.34 When socially isolated seniors overcome their fears or other obstacles and become active online the evidence is that their social isolation is lessened. As WorkVentures told the Committee:

When we talk to seniors who have purchased a computer they rave about the benefits of being able to access online services, of the reduced social isolation that comes from contacting family, friends or people they’ve never met but have similar interests, and of the joy they get from using computers for entertainment.³⁶

Seniors and online social networking

- 2.35 The internet offers unprecedented opportunities for social networking and many seniors are active on social networking sites. For housebound seniors online social networking allows them to stay connected and engaged with family and friends.³⁷

- 2.36 Telstra told the Committee that:

... instant messaging, Facebook and Twitter has given Australians from all walks of life a feeling of being more connected to loved ones, family and friends regardless of the tyranny of distance,

33 Mrs Bosler, President, ASCCA, *Committee Hansard*, 23 March 2012, p. 18.

34 Brisbane Seniors Online Association Inc. (BSOL), *Submission 34*, p. 2.

35 Brotherhood of St Laurence, *Submission 13*, p. 8.

36 WorkVentures Ltd, *Submission 33*, p. 6.

37 LACVI, *Submission 5*, p. 2.

density of population and the remote and less densely populated areas of Australia.³⁸

- 2.37 More than 500 000 Australians aged 60 years and over have a Facebook page.³⁹ Facebook told the Committee that:

Every day, countless seniors in Australia connect via Facebook with the friends, family, places, events and things that they care about. Social platforms such as Facebook can assist senior Australians to ‘bring the outside world in’ at a time when they may face greater challenges getting out and about in the physical world.⁴⁰

- 2.38 However, although social networking sites offer a significant opportunity for seniors to remain engaged with their community, these sites also present challenges for those who do not know how to safely use social media.⁴¹ Dr Cassandra Cross said:

Many seniors do not have an adequate knowledge of security settings on accounts, either about their existence in the first place, or the importance of changing the default setting. They believe that only their contacts can access the information that is being posted. In reality, this is not the case.⁴²

- 2.39 As with the wider community, many seniors use online dating and romance websites and some have had bad experiences, including in some cases losing significant sums of money as well as their self-confidence and self-esteem.

- 2.40 Abacus – Australian Mutuals, the Association of Building Societies and Credit Unions, told the Committee that many senior Australians are establishing friendships and relationships through online social networking and dating websites. Social networking is a very positive development for seniors, especially those who are housebound, but there are risks involved. Abacus told the Committee that romance scams are a significant and growing concern for seniors because many profiles are bogus, with criminals befriending victims in order to get them to send money in the promise of love or a relationship.⁴³

38 Telstra Corporation Ltd, *Submission 22*, p. 4.

39 South Australian Government, *Submission 37*, p. 6.

40 Facebook, *Submission 36*, p. 2.

41 South Australian Government, *Submission 37*, p. 6.

42 Dr Cassandra Cross, *Submission 49*, p. 3.

43 Abacus – Australian Mutuals, *Submission 44*, p. 2.

Seniors' use of internet for banking and e-commerce

- 2.41 ABS research from 2010 reported that among seniors who used the internet at home, using it for financial transactions was significantly less popular than using it for email and general browsing.⁴⁴
- 2.42 In 2012, the Committee's online survey found that 'banking and paying bills' was the most popular use of the internet by seniors who are online at home (see Appendix D).⁴⁵ This might indicate that seniors who are active online have become more confident about using the internet for banking in the two years since the 2010 research.
- 2.43 Again it is the housebound and isolated seniors who could benefit greatly from the ability to do banking and other financial transactions from home:
- In some cases, it may also be their only means of conducting their necessary day-to-day business [such as] banking, paying bills, online purchasing and so on.⁴⁶
- 2.44 A submission from eBay and PayPal told the Committee that both companies 'enjoy considerable patronage from the 55 year old plus age group'. Over 400 000 senior Australians use PayPal.⁴⁷

Shopping online

- 2.45 The ability to shop online offers housebound seniors and those in rural or remote places shopping opportunities which they could not have dreamed of only a few years ago.⁴⁸
- 2.46 In 2011, an NSA Productive Ageing Centre report noted that older people are increasingly shopping online with at least 10 per cent of internet users

44 Australian Bureau of Statistics (ABS), 8146.0 *Household Use of Information Technology, Australia, 2010-11*, Personal Internet Use, Table 8.

45 76.5 per cent of respondents to the Committee's online survey found that 'banking and paying bills' is the predominant reason for seniors using the internet.

46 LACVI, *Submission 5*, p. 2.

47 eBay and PayPal, *Submission 11*, p. 1.

48 The Committee's online survey found that 'shopping' was fourth placed among reasons for seniors using the internet with 54.5 per cent of respondents saying they use the internet for shopping.

who are aged 50 years and over purchasing one or more items online on a weekly basis, or more frequently.⁴⁹

- 2.47 Potential risks for seniors shopping online, such as making transactions on unsecure websites or on an unsecured computer, are discussed in the next chapter of this report.

Shift of government services to the internet

- 2.48 Increasingly, essential information about government services is provided online. Seniors (and everyone else) can access government services provided by Medicare Australia, Centrelink and Veterans Services, among others, through the *Australia.gov.au* website. The site also provides a portal for the Government to communicate with consumers, including senior Australians, who are using the internet to access government services.⁵⁰

- 2.49 The DBCDE submitted that:

The rollout of the National Broadband Network (NBN) is expected to bring substantial economic and social benefits to internet users and access to health and aged care will be improved by increased online government service delivery and greater commercial opportunities.⁵¹

- 2.50 Although government is increasingly using websites to convey important services and information, the AHRC says it is not always easy for seniors to navigate those websites and it recommends that all government departments should audit their online information to ensure it is user-friendly and accessible '... with the view to improving accessibility and extending information platforms beyond the online medium if required'.⁵² The accessibility for seniors of information on government and business websites is further discussed later in this report.

- 2.51 Mr Andrew Connor from Digital Tasmania suggested to the Committee that to provide all seniors with equal access to government websites, government could look at the feasibility of providing a low cost internet

49 NSA Productive Ageing Centre, *Older Australians and the Internet: Bridging the Digital Divide*, September 2011, p. 13.

50 DoHA, *Submission 16*, p. 4.

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

52 AHRC, *Submission 2*, p. 9.

connection to seniors for the purpose of accessing government online services and legitimate online banking sites.⁵³

Recommendation 1

That the Australian Government investigates innovative ways of providing low cost internet connection to financially disadvantaged housebound and geographically isolated seniors who request it.

Government initiatives to engage seniors with ICT

Internet kiosks for seniors

2.52 Since 2008, around 2,000 Broadband for Seniors kiosks have been established across Australia as part of the Australian Government's National Digital Economy Strategy. At these kiosks, seniors can access free, personalised training on how to use a computer and surf the internet. Kiosks are located in community centres, retirement villages, libraries, some ex-service organisations and senior citizens clubs.⁵⁴ Mrs Bosler from the ASCCA told the Committee:

[The kiosks] are a wonderful stepping stone for seniors to become used to the basic concept of using the internet. It is that fear factor of not quite knowing where to start and whether they can manage that often is the stumbling block for older people. Those kiosks are doing a good job.⁵⁵

2.53 The NSA Productive Ageing Centre noted that the free internet kiosks address the barrier of cost of access to the internet and lack of training only in the areas that benefit from these initiatives. The report states that in 2011 only 17 per cent of 'older Australians who never or rarely use the internet' were aware of the existence of internet kiosks yet they are the kiosks' target group.⁵⁶

53 Mr Andrew Connor, Spokesperson, Digital Tasmania, *Committee Hansard*, 7 August 2012, p. 9.

54 Department of Families, Housing, Community Services and Indigenous Affairs (FaHCSIA), <www.fahcsia.gov.au/our-responsibilities/seniors/programs-services/broadband-for-seniors> viewed 8 January 2013.

55 *Committee Hansard*, 23 March 2012, p. 15.

56 NSA Productive Ageing Centre, *Older Australians and the Internet: Bridging the Digital Divide*, September 2011, pp. 9–10.

- 2.54 The AHRC is also concerned about seniors' lack of awareness of the kiosks and recommended to the Committee that a publicity campaign to alert seniors to the existence of the kiosks would be useful. The campaign should target seniors clubs, magazines, newspapers, radio and television.⁵⁷
- 2.55 The Broadband for Seniors kiosks are playing an important role in education and training of seniors in cybersafety and this is discussed in some detail in Chapter 4.

Recommendation 2

That an advertising campaign targeting seniors be devised to alert seniors around the nation to the existence and location of the Broadband for Seniors kiosks.

Digital Hubs

- 2.56 The Digital Hubs program, administered by the Department of Broadband, Communications and the Digital Economy (DBCDE) encourages Australians to realise the benefits of greater digital engagement in a safe and secure way. Forty communities were selected to be the first digital hubs connected to the NBN. The program provides local residents with online training and the opportunity to experience NBN-enabled services and technology.⁵⁸ Training opportunities being offered at digital hubs are discussed in Chapter 4.
- 2.57 DBCDE told the Committee that 'digital exclusion' exacerbates 'social exclusion' and the Digital Hubs program recognises that older Australians often have concerns about online safety and security and these are addressed by the program.⁵⁹
- 2.58 ALIA's Ms Little said that public libraries are using the digital hubs to provide library users with access to services which require high bandwidth and which were not previously available. Digital hubs are becoming:

... an access point for a whole range of other services, like eHealth, access to lawyers and access to educational programs overseas.⁶⁰

57 AHRC, *Submission 2*, p. 8.

58 DBCDE, *Submission 25*, p. 11.

59 DBCDE, *Submission 25*, p. 11.

60 *Committee Hansard*, 9 May 2012, p. 8.

- 2.59 In Tasmania the Committee visited a digital hub in the Pittwater Community Centre at Midway Point and observed firsthand a computer class for seniors. Committee members talked to the participants and heard how they were using their new knowledge of the internet for various projects.

ICT and healthcare

- 2.60 In May 2011 the Government released its *National Digital Strategy* which has eight 'Digital Economy Goals', one of which is *Improved Health and Aged Care*. The goal is that by 2020, 90 per cent of high priority consumers, including older Australians, can access individual health records electronically. This will include investment in telehealth consultations to provide improved remote access to specialist services for patients in rural, remote and outer metropolitan areas.⁶¹
- 2.61 The development of the Personally Controlled Electronic Health Record (PCEHR) by the National E-Health Transition Authority (NEHTA) supports the *National Digital Strategy's* goals for eHealth in Australia. Since its launch in July 2012, PCEHR allows the 'secure sharing of health information between an individual's healthcare providers, while enabling the individual to control who can access their PCEHR'.⁶²
- 2.62 CHF's Ms Bennet said that while PCEHR creates particularly exciting opportunities, consumers of all ages need to have access to the right information and know what their rights and responsibilities are if they are going to reap the full benefits.⁶³
- 2.63 Ms Susan Ryan, Age Discrimination Commissioner from the AHRC told the Committee that the Human Rights Commission is very enthusiastic about the opportunities that eHealth services will present, but it is absolutely crucial that older people 'be given tools whereby they can take advantage of this great new investment that is being made on behalf of all Australians'.⁶⁴
- 2.64 Several groups made representations to the Committee with concerns about how PCEHR would operate, particularly in relation to online safety for seniors and about the possibility of misuse of PCEHR information by third parties, such as employers or insurers. These concerns are discussed in Chapter 3.
-

61 DoHA, *Submission 16*, p. 1.

62 National E-Health Transition Authority (NeHTA), *Submission 4*, p. 2.

63 *Committee Hansard*, 19 September 2012, p. 2.

64 *Committee Hansard*, 23 March 2012, p. 2.

Barriers to internet access for seniors

2.65 Research in 2011 by the Australian Research Council Centre of Excellence for Creative Industries and Innovation (CCI) looked at all aspects of 'Older Australians and the Internet' including barriers to access. It found the key barriers preventing seniors from using the internet were:

- they don't know how to use the internet/lack of skills (76.5 per cent)
- they are confused by the technology (73.8 per cent), and
- they have concerns about security and viruses (63.8 per cent)⁶⁵

2.66 Respondents to CCI's research placed 'cost of access to the internet' ninth in the list of reasons why they were not using it. Of those who did identify cost as the reason for non-use, one respondent said:

To the government I would just like to tell them that I am quite sure many single pensioners out there on their own haven't got a computer or the internet for the same reason as me. It is the cost factor. If the cost factor was eliminated I would get a computer and then go back to U3A.⁶⁶

2.67 COTA NSW told the Committee that it has identified 'cost' and 'lack of knowledge' as the two main barriers which prevent some people over the age of 55 years from engaging in the digital world.⁶⁷ COTA NSW said:

Knowledge includes education and application. Before this barrier can be addressed the fear factor needs to be addressed. If the fear factor is not acknowledged and the benefits outlined, older Australians will avoid the technology and justify why they should not engage in the digital world.⁶⁸

2.68 The NSA Productive Ageing Centre also identified cost as high on the list of barriers which some older people face in relation to using the internet. The barriers the NSA identified were:

- cost of access to computers and internet connection;
- geographical and/or physical constraints, illness and/or lack of transport preventing access to internet resources;

65 Creative Workforce Program, Australian Research Council Centre of Excellence for Creative Industries and Innovation (CCI), *Older Australians and the Internet*, June 2011, p. 31.

66 Creative Workforce Program, CCI, *Older Australians and the Internet*, June 2011, p. 32.

67 COTA NSW, *Submission 39*, p. 2.

68 COTA NSW, *Submission 39*, p. 2.

- limited public access to computer facilities;
- knowledge-based barriers and lack of online skills;
- concerns regarding privacy and security of internet transactions; and
- lack of ability or confusion about the internet can 'lead to a feigned lack of interest' – seniors find it less stigmatising to have 'no interest' than to be unable to use online resources.⁶⁹

2.69 The Australian Institute of Criminology (AIC) told the Committee that while seniors do not have the highest prevalence of online victimisation, many have a real fear of victimisation which prevents them from accessing government or business services or hampers online social interaction with friends and family. Dr Rick Brown, Deputy Director (Research), with the AIC said:

Fear of potential victimisation may also make it difficult for senior Australians to identify and use legitimate online resources.⁷⁰

2.70 Seniors from culturally and linguistically diverse backgrounds can face the additional barrier to internet access of language. The Federation of Ethnic Communities' Councils of Australia (FECCA) told the Committee that language barriers can 'certainly act to prevent engagement with information provided online, and can reduce confidence in engaging with new technology.'⁷¹

2.71 Dr Jenny Cartwright, AFP Co-ordinator, Strategic Initiatives, told the Committee that on the ThinkUKnow website there are fact sheets on cybersafety in several different languages including Greek, Korean, Persian, Serbian, Spanish, Turkish and Vietnamese.⁷²

2.72 Many older immigrants with culturally and linguistically diverse backgrounds are unlikely to have had significant training in the use of new technologies. Financial constraints may mean that they have limited opportunity to engage with new and emerging technologies.⁷³

2.73 However, when people with limited English are comfortable using ICT, it gives them the ability to stay in touch with friends, family and news in other places. Digital Tasmania's Mr Connor said:

69 NSA Productive Ageing Centre, *Older Australians and the Internet: Bridging the Digital Divide*, September 2011, p. 15.

70 *Committee Hansard*, 10 October 2012, p. 1.

71 Federation of Ethnic Communities' Councils of Australia (FECCA), *Submission 40*, p. 2.

72 *Committee Hansard*, 13 March 2013, p. 7.

73 FECCA, *Submission 40*, p. 3.

.... The internet provides marvellous opportunities for people for whom English is not their first language to connect with their communities ... my mother-in-law is from Poland and does not speak a lot of English. She can keep totally up to date through the computer and the news sites, even watching TV shows and news bulletins.⁷⁴

- 2.74 Asked whether any cybersafety information on the DBCDE website is available in languages other than English, Mr Abul Rizvi said that currently it is not but 'that is probably something we should look into'.⁷⁵

Recommendation 3

That the Department of Broadband, Communications and the Digital Economy prioritise including some cybersafety information on their website in languages other than English.

- 2.75 Unfortunately, it is the people who are socially isolated, whether it is because of language or for other reasons, who would probably benefit most from having the internet in their homes. Ms Danielle Walker, Community Development Officer at Hobart City Council, said:

... often social isolation is not just about health and wellbeing; there are poverty related issues that restrict access to resources such as laptops or computers or transport to get out to centres where they are available. When the costs start to add up, coming out of your home can be more difficult, and then that starts to impinge on your health and wellbeing and mental health.⁷⁶

The cost of ICT as a barrier for seniors

- 2.76 Despite the decreasing cost of purchasing a computer and internet connection, many seniors remain unable to afford the necessary hardware and software to enable connection to the internet in their home:

.... [computer] costs are compounded by the cost of software and ongoing support required to download and regularly update

74 *Committee Hansard*, 7 August 2012, p. 5.

75 *Committee Hansard*, 12 September 2012, p. 3.

76 *Committee Hansard*, 7 August 2012, p. 4.

software (such as anti-virus and security software), and to troubleshoot technical problems.⁷⁷

2.77 According to the NSA Productive Ageing Centre, those seniors who were most likely to identify 'cost' as a barrier preventing them from using the internet or improving their internet skills are:

- females
- those receiving an income of \$30 000 or less a year
- those receiving an age pension, or
- those receiving other government support.⁷⁸

2.78 LACVI suggested to the Committee that the government could subsidise the cost of security software and devices and perhaps even access to broadband services for pensioners as a way of preventing victimisation through cybercrime because:

Many seniors are likely to try to do it 'on the cheap' to avoid spending any more than necessary on their often meagre income ...we suggest that government has a role to ensure seniors are not excluded from their use simply because they cannot afford high-cost and poorly targeted services...⁷⁹

2.79 There are programs which help seniors to acquire ICT equipment at low cost. WorkVentures told the Committee about its *Connect IT program* which supplies 'refurbished computers' to low income households. Over the last three years senior Australians have become the largest customer segment of the program. People receiving the aged pension have grown from receiving 29 per cent of the program's deliveries in 2009 to 53 per cent in 2011. 'This equates to thousands of computers being supplied to senior Australians each year.'⁸⁰

2.80 When seniors receive a computer from WorkVentures, they also receive a mousepad that is attached to an information booklet which describes what the main cyber safety risks are and how seniors can protect themselves. This package is provided by the AFP as part of the ThinkUKnow program. Dr Cartwright told the Committee that the AFP has distributed approximately 500 of these mousepad/information packages each month

77 Government of Western Australia, *Submission 19*, p. 4.

78 NSA Productive Ageing Centre, *Older Australians and the Internet: Bridging the Digital Divide*, September 2011, p. 10.

79 LACVI, *Submission 5*, p. 4.

80 WorkVentures Ltd, *Submission 33*, pp. 2-3.

since July 2011. Additionally, each new computer has a ThinkUKnow sticker on it so seniors can immediately see the ThinkUKnow website address for cybersafety information.⁸¹

2.81 WorkVentures also provides free technical support throughout the life of the refurbished computer. WorkVentures receives considerable support from Centrelink in promoting this program.⁸²

2.82 On top of the cost of the hardware, internet access adds another cost which some seniors cannot meet. The Brotherhood of St Laurence believes government policy should take account of the cost of internet access at home among senior Australians:

This is especially important as increasing numbers of services become available only on line and new essential services like e-health become the norm. As this trend gathers momentum, internet connection will become an essential service equivalent to other utilities and government policy needs to embrace its affordability by all senior Australians.⁸³

2.83 The AHRC told the Committee that in 2010 and 2011, a number of European countries codified internet rights into law. For example, Finland became the first country in the world to make broadband a legal right for every citizen in 2010.⁸⁴

Concluding comments

2.84 The Committee found that the way seniors use ICT reflects their wide diversity of skills, attitudes to and uses for the technology. Some seniors are as cyber savvy as anyone, while others are non-users or very cautious users. Seniors who do go online have quite a high level of awareness of cybersafety issues. Mr Rizvi said:

They seem to be more conscious of it and they are more aware of the things they need to do to keep themselves safe online. So we have this dual situation where on the one hand a high percentage

81 *Committee Hansard*, 13 March 2013, p. 3.

82 WorkVentures Ltd, *Submission 33*, pp. 2-3.

83 Brotherhood of St Laurence, *Submission 13*, p. 8.

84 AHRC, *Submission 2*, p. 8.

of seniors are fearful about going online but, on the other hand, those who do go online appear to be more careful about it.⁸⁵

- 2.85 Younger seniors may have used ICT in their workplace before retirement so they have ICT skills and are confident of keeping themselves cybersafe. Other seniors did not use ICT in the workplace but they have embraced the new technology and are also skilled and confident. However, many seniors left the workforce before the ICT revolution and they are either non-users or tentative users because they lack knowledge and skills and/or because they are fearful of going online, knowing there are risks but not feeling confident to manage those risks.
- 2.86 The fears that many seniors have about cybersafety are reasonable. The evidence shows that seniors are being specifically targeted by scams and 'phishing' because they have access to life savings and superannuation investment funds making them primary targets for cybercrime.⁸⁶
- 2.87 Overwhelmingly, the Committee heard that the only way that seniors who are afraid to go online will overcome their fears is by providing appropriate and accessible education and training. Cybersafety education and training for seniors is discussed in Chapter 4 of this report.

85 Mr Rizvi, DBCDE, *Committee Hansard*, 12 September 2012, p. 2.

86 Mrs Karen Harfield, Executive Director, Fusion, Target Development and Performance, Australian Crime Commission, *Committee Hansard*, 15 August 2012, p. 1.

Cybersafety risks and threats for seniors

Introduction

- 3.1 The digital economy is constantly growing and diversifying: Australians are going online for business and pleasure, for social networking, to access government information or advance their education, for shopping, investment or other financial transactions.
- 3.2 As discussed in the previous chapter, there are significant financial and quality of life benefits in this for every sector of the Australian community. However, just as government and businesses embrace the internet to improve their services, so the market expands to host new generations of cyber-enabled crimes.
- 3.3 This chapter surveys the nature and extent of cybercrime before discussing the particular risks to older Australians and their perceptions of, and responses to, these risks. Finally, the chapter considers some basic measures to build the online confidence and consumer awareness of all Australians, and particularly those aged 55 plus.

The nature and prevalence of cybercrime

- 3.4 The immediacy and global nature of interaction on the internet, and its convergence with new technologies such as smartphones and portable tablets, offers senior Australians a new means of access to family and friends, education and health services, and business. These benefits are

not achieved, however, without exposing participants to an ever diversifying range of online threats and risks. The Australian Crime Commission (ACC) advised:

As the cyber-world becomes increasingly embedded in every aspect of our lives, the opportunity for cyber enabled criminal groups and entrepreneurial actors also increases. The internet in particular is being utilised by organised crime groups to commit traditional crimes such as fraud in a manner that removes many of the associated risks. Cyber-criminals can operate from a distance across a borderless cyber-environment with a degree of anonymity that has never been seen before and against a significant quantum of potential victims. [They] are interested in attaining illicit wealth, either through the theft of personal information or through fraudulent investment scams and similar activities.¹

3.5 The Australian New Zealand Policy Advisory Agency has defined cybercrime to cover:

- crime directed at computing and communications technologies themselves, such as unauthorised access to, modification or impairment of electronic communications or data; and
- crime where the use of the internet or information technology is integral to the commission of the offence, (sometimes referred to as technology enabled crime) such as online fraud (including Internet or email scams), online identity theft, online child exploitation and online intellectual property infringement.²

3.6 The 2012 *Norton Cybercrime Report* estimated the global financial cost of cybercrime over the previous year at \$110 billion. Over 556 million victims were affected with nearly half of these subject to malware or virus attacks, hacking scams, fraud and/or information theft.³

3.7 The borderless and anonymous nature of online activity, along with the versatility of organised crime, poses significant challenges to regulators internationally.⁴ Australia's accession to the *Council of Europe's Convention on Cybercrime*, and recent implementation of legislation in support of it, intends to address this by enhancing the capacity for

1 Mrs Karen Harfield, Executive Director, Fusion, Target Development and Performance, Australian Crime Commission (ACC), *Committee Hansard*, 15 August 2012, p. 1.

2 Quoted in ACC, *Submission 9*, p. 7.

3 Symantec, *2012 Norton Cybercrime Report*, 2013, pp. [2-3].

4 ACC, *Submission 9*, p. 9.

international information and data sharing and enforcement co-operation.⁵

- 3.8 The Australian Government has established a goal that Australia should be among the world's leading digital economies by 2020. Evidence to the Committee highlighted a number of emerging cyber threats that have potential to jeopardise the economic prosperity expected with this economic expansion.⁶

Emergent cyber threats

- 3.9 According to the ACC, international cybercrime is now occurring at an unprecedented rate.⁷ While the cost estimates of this to the Australian community vary, these are clearly significant: the Australian Federal Police (AFP) estimates that Australians lose in excess of \$1 billion a year to cyber criminals.⁸ The internet security company Symantec calculated the figure over 2012 was closer to \$2 billion.⁹
- 3.10 The latest statistics from the Australian Competition and Consumer Commission (ACCC), which registers complaints about online scams,¹⁰ confirms the growth in online frauds. In 2011 the ACCC received 83 150 scam related contacts from consumers and small businesses, almost double the number received in 2010, and four times that recorded in 2009.¹¹
- 3.11 Top scams reported to the ACCC over 2011 were mass marketed advance fee frauds, covering upfront payment for services, products or rewards, which accounted for half of all reports, and computer hacking which was the second most reported scam type, accounting for 23 per cent of scams. This compared with 12 per cent in 2011.¹²

5 See Chapter 5 for more detail.

6 Australian Government, # au20, *National Digital Economy Strategy: Leveraging the National Broadband Network to Drive Australia's Digital Productivity*, Department of Broadband, Communications and the Digital Economy (DBCDE), 2011, and see DBCDE, *Submission 25*, p. 2.

7 ACC, *Submission 9*, p. 7.

8 Quoted in DBCDE, *Submission 25*, p. 6.

9 Symantec, *2012 Norton Cybercrime Report*, 2013, p. [6].

10 Australian Competition and Consumer Commission (ACCC), SCAMwatch <www.scamwatch.gov.au/content/index.phtml/tag/scamAboutUs/> viewed 30 January 2013.

11 ACCC, *Targeting Scams: Report of the ACCC on Scam Activity 2011*, 2011, p. 1.

12 ACCC, *Targeting Scams: Report of the ACCC on Scam Activity 2011*, pp. 1, 7.

- 3.12 A major driver of online crime is the availability of personal information used for identity theft and system hacking. The Centre for Internet Safety (CIS), a cybercrime centre in Canberra, advised that credit card skimming and online data theft can now be taken as a given, with decreasing prices for personal information in Australia commensurate with its increased availability in a thriving black market.¹³
- 3.13 The ACC reported that some organised crime networks specialise in the sale of personal data. While rates vary, Australia often ranks as the third or fourth least expensive source country after the United States (US), the United Kingdom (UK), and Canada:
- Average prices for a single Australian credit card range between A\$7 and A\$35, depending on the amount of credit available on the card. Prices for bank logins vary according to the bank balance. It costs on average A\$100 for a login with a balance of A\$1 000; A\$200 for a login with a balance of A\$3 000 and so on. Credit card magnetic strip coding information and PINs are also available, with prices ranging between A\$70 and A\$170, depending on the location.¹⁴
- 3.14 Cybercriminals are entrepreneurial and opportunistic, continually monitoring the online environment for vulnerabilities to exploit for criminal gain.¹⁵ The ACC's Mrs Karen Harfield referred to online fraud activity during the global financial crisis:
- For example, you will remember the \$900 bonus as part of the response to the global financial crisis. We saw, within 48 hours, that people were being directly contacted for their names, dates of birth and account numbers so that the payment could be diverted away from the legitimate person who was to receive it.¹⁶
- 3.15 According to the CIS, the most successful online threats now combine social engineering, involving psychological manipulation to gain personal information, and technical attacks, to gain access to systems.

13 Mr Alastair McGibbon, Co-Director, Centre for Internet Safety (CIS), *Committee Hansard*, 14 March 2012, p. 2.

14 Prices fluctuate and vary for different countries at different times, see ACC, *Submission 9*, Case Study, p. 13.

15 ACC, *Submission 9*, p. 9.

16 *Committee Hansard*, 15 August 2012, p. 3.

Spam meanwhile continues to be an important vector for spreading malware (malicious software), 'phishing' and social engineering scams.¹⁷

- 3.16 Research conducted by the Symantec security firm over 2011 found that around 72 per cent of adult internet users in Australia had experienced cybercrime with viruses and malware, online credit card fraud and social networking profile hacking being most reported.¹⁸
- 3.17 The following sections describe the nature and impact of key threats to Australians as identified in evidence: identity theft, by 'phishing' and company-based data breaches or 'hacking'; superannuation and investment schemes; online dating schemes; money transfer and lottery and charity scams.

Identity theft by 'phishing'

- 3.18 Identity theft involves fraudulent use of personal details, such as drivers licences, tax file numbers and electronic personal identity information (computer passwords and personal identification numbers – PINs), without permission or to illegally appropriate another persons' identity for unauthorised gain.¹⁹
- 3.19 'Phishing' is the term used to describe approaches designed to capture personal information by email, often by including hotlinks to 'poisoned' web pages.²⁰ The email may purport to be from a victim's bank or another trusted source and will request account information to be verified through the linked site.²¹
- 3.20 The Australian Tax Office (ATO) submission provided examples of ATO branded 'phishing' exercises over some years showing their increasing sophistication. Appendix F shows a recent version.²² The ATO's Mr Todd Heather explained the enforcement challenges posed by these scams:

When we discovered that people were using our brand in this way we created something that we call the phishing filter, by which we would detect that a scammer was coming to our website to try to

17 CIS, *State of the Nation*, December 2011, pp. 1, 6.

18 Symantec, *Norton Cybercrime Report 2011*, Cited in ACC, *Submission 9*, p. 7.

19 CIS, *State of the Nation*, December 2011, p. 8; ACC, *Submission 9*, p. 13.

20 See CIS, *State of the Nation*, December 2011, p. 9.

21 C Budd and J Anderson 'Consumer Fraud in Australasia: Results of the Australasian Consumer Fraud Taskforce Online Australia Surveys 2008 and 2009', *Technical Background Paper 93*, AIC, March 2011, p. 21.

22 Australian Taxation Office (ATO), *Submission 43*, p. 4.

re-present our information to them. We would send a message back saying, 'This is a scam website; it is being blocked.' They got wind of that, so instead of referring directly to our website, they point to a copy they have made of our website.²³

- 3.21 Over 2010–11, the ATO recorded a 74 per cent increase on total IT security incidents, with 67 per cent being ATO branded phishing attacks.²⁴
- 3.22 Phishing scams may also involve notification of a fake lottery win, bequest or inheritance scams or requests to act as an intermediary to transfer funds from an overseas country in return for a commission (advance fee scams).²⁵ The AFP reported a recent phishing scam using its logo to lure consumers into paying money to unlock their personal computers.²⁶
- 3.23 Another trend is the prevalence of phishing scams posted on travel websites and mailing lists, with links to non-existent resorts and holiday packages used to gather booking fees and personal information.²⁷

Computer hacking

- 3.24 In addition to data theft from an individual's online activities and home computer, a major source of financial and personal information is through hacking into the computer networks and databases of institutions or businesses. As noted above, online hacking was the second most reported scam reported to the ACCC in 2011.²⁸
- 3.25 Malware can be installed on computers through phishing invitations and used to redirect users from a legitimate URL to a false website in a process known as 'pharming'.²⁹ Spyware is used to gather information

23 Mr Tod Heather, Chief Technology Officer, Strategy, Planning and Assurance, Enterprise Solutions and Technology, ATO, *Committee Hansard*, 18 May 2012, p. 25.

24 In 2012, the most prevalent ATO branded scam was a fax related scam, in which real estate agents were asked to forward a 'rental income without deduction form' to landlords to elicit information to be faxed back to a designated 'ATO' number, see ATO, *Submission 43*, p. 4–5.

25 Brotherhood of St Laurence, *Submission 13*, p. 5.

26 Commander Glen McEwen, Manager, Cyber Crime Operations, Australian Federal Police (AFP), *Committee Hansard*, 13 March 2013, p. 1

27 AVG Technologies in *Age Traveller* <www.theage.com.au/travel/dodgy-deals-are-daylight-robbery-20130201-2dop4.html#ixzz2KkF26zhj> viewed 13 February 2013.

28 ACCC, *Targeting Scams: Report of the ACCC on Scam Activity 2011*, p. 7.

29 C Budd and J Anderson 'Consumer Fraud in Australasia', *Technical Background Paper 93*, AIC, March 2011, p. 21.

by monitoring online use without otherwise disrupting a computer's function.³⁰

- 3.26 The Committee was told that few Australian Small and Medium Enterprises (SMEs) have the capacity to manage the data they hold, and even large companies are not immune to sophisticated attacks using malware.³¹ According to Abacus-Australian Mutual, the industry body for mutually owned Deposit-taking Institutions (ADIs),³² the cost to business of cybercrime was reported to be up to \$624 million in 2008 alone.³³
- 3.27 In the wake of a number of significant and well publicised hacking incidents overseas involving multinationals³⁴ and most recently in Australia against institutions and SMEs,³⁵ the Government has issued warnings and introduced legislation to better protect personal information. This is discussed in more detail in Chapter 5.

Superannuation fraud and boiler room investment schemes

- 3.28 The AFP reports that superannuation fraud is the largest earner for cybercriminals in Australia. Various means are deployed to obtain access to superannuation funds. The AFP advised:

Criminals exploit a range of techniques including phishing in order to first steal the identity of victims before transferring their superannuation into self-managed accounts or applying for hardship payments.³⁶

- 3.29 Crime experts agreed that domestic and offshore investment schemes pose an escalating threat to Australians, and especially to senior

30 See CIS, *State of the Nation*, December 2011, p. 8.

31 Professor Nigel Phair, Co-Director, CIS, *Committee Hansard*, 14 March 2012, pp. 2-3 and for detail on malicious software see CIS, *State of the Nation*, December 2011, pp. 5-6.

32 Abacus-Australian Mutuals represents 89 credit unions, seven mutual building societies and six banks, with a total of \$ 85 billion total assets and 4.5m customers. See *Submission 44*, p. 1.

33 K Richards, 'The Australian Business Assessment of Computer User Security (ABACUS): a National Survey', *AIC Research and Public Policy Series no. 102*, June 2009, Forward. Data ref. in *Abacus-Australian Mutuals, Submission 44*, p. 1.

34 The largest recorded data breach occurred in April 2011 when 77 million Sony PlayStation accounts were hacked. See CIS, *State of the Nation*, December 2011, pp. 8-9.

35 Notably, a school and medical practices in Queensland had data stolen, encrypted and held for ransom. See DBCDE, 'Ransomware Attacks Will Increase in 2013', 21 December 2012, <www.staysmartonline.gov.au/alert_service/advisories/ransomware_attacks_will_increase_in_2013> viewed 31 January 2013.

36 Australian Federal Police (AFP), *Submission 20*, p. 3.

Australians who are targeted because of their superannuation wealth.³⁷ Also known as boiler-room fraud or 'serious and organised investment fraud' (SOIF), these schemes use sophisticated techniques to solicit investment in non-existent or essentially worthless shares and other securities.³⁸

- 3.30 The CIS stated that, typically, boiler room investment schemes are 'well backstopped', utilising a range of media to ensnare their victims.³⁹ The ACC advised that victims are first identified by stored online information obtained through the personal information leads market. Operators start with a cold call or emails and high pressure sales techniques to secure investment, sometimes grooming their victims over a long period. Victims are then directed to professional-looking websites which may be operated from anywhere in the world.⁴⁰
- 3.31 Victims are usually encouraged to make a small upfront investment, with websites presenting investment growth over the long term to persuade people to invest more. Detection of loss may result in a subsequent scam for investigation at a fee, or sites simply close down and the 'investment' disappears.⁴¹
- 3.32 Explaining the success of these schemes, the ACC's Mrs Harfield said that the perpetrators of these crimes psychologically profile their victims, and the back up with phone calls, letters and faxes tends to legitimate the scheme.⁴² The CIS's Professor Phair explained that SOIF websites also appear as part of a complex series of interrelated sites, which convinces even professional investment advisers.⁴³

Online dating and romance scams

- 3.33 According to the ACCC, dating and romance scams are a major threat to Australian consumers; more money is lost through these scams by proportion than in all other scams.⁴⁴ Over 2011 dating and romance

37 AFP, *Submission 20*, p. 3; ACC, *Submission 9*, p. 17.

38 ACC, *Submission 9*, p. 17.

39 Professor Phair, CIS, *Committee Hansard*, 14 March 2012, p. 6.

40 ACC, *Submission 9*, p. 18.

41 Mrs Harfield, ACC, *Committee Hansard*, 15 August 2012, p. 2.

42 ACC, *Committee Hansard*, 15 August 2012, p. 2.

43 CIS, *Committee Hansard*, 14 March 2012, p. 6.

44 One in two people who reported a dating and romance scam lost money compared to around one in five across all types of scams. See 'ACCC Working with Industry to Target Dating and Romance Scams', *Media Release*, 29 September, 2011.

scams cost Australians more than \$21 million.⁴⁵ Almost five per cent of consumers affected by this type of scam lost in excess of \$100 000.⁴⁶

3.34 Romance and dating scams are a category of advance fee scam where a payment is made in anticipation of a reward. Dating and romance scammers use social engineering techniques to promote emotional involvement and a sense of obligation. Criminals may use bogus profiles on social networking sites to befriend victims in order to get them to send money in the promise of love or relationship.⁴⁷

3.35 The AFP notes that many victims are approached on legitimate dating websites, now a major growth industry with wide community engagement:

These scams typically involve a genuine user of an online dating site being contacted by a potential admirer who is a scammer in disguise. After forming a relationship with the victim, the scammer plays on emotional triggers to get the victim to provide money, gifts or personal details.⁴⁸

3.36 The ACCC's consumer guide *The Little Black Book of Scams* warns that romance and dating scammers are usually extremely experienced at emotional manipulation:

Even on a legitimate dating site, you might be approached by a scammer – perhaps someone who claims to have a very sick family member or who is in the depths of despair (often these scammers claim to be from Russia or Eastern Europe). After they have sent you a few messages, and maybe even a glamorous photo, you will be asked (directly or more subtly) to send them money to help their situation. Some scammers even arrange to meet with you, in the hope that you give them presents or money – and then they disappear.⁴⁹

45 ACCC, 'Safer Dating Online' <www.accc.gov.au/content/index.phtml/itemId/1047887> viewed 31 January 2013.

46 ACCC, *Targeting Scams: Report of the ACCC on Scam Activity 2011*, p. 12.

47 Abacus-Australian Mutuals, *Submission 44*, p. 2.

48 AFP, *Submission 20*, p. 4, also see 'ACCC Working with Industry to Target Dating and Romance Scams', *Media Release*, 29 September, 2011.

49 ACCC, *The Little Black Book of Scams: Your Guide to Scams, Swindles, Rorts and Rip-Offs*, 2008 (rev. 2011), p. 27.

Money transfer, lottery and charity scams

- 3.37 Money transfer, or advance fee, scams usually involves receipt of an unsolicited email promising an unexpected and significant cash payment, pending the payment of substantial 'administrative' fees by the victim to an overseas bank account.⁵⁰
- 3.38 Originally issued from Nigeria, these scams are now generated in many other nations. According to the ACC many victims, on realising losses, continue to send funds hoping for a 'successful' completion. The perpetrators profit from only a small number of victims but the use of email means pervasive impact for a minimal cost.⁵¹ Advance fee scams also include those in which the offender pretends to sell something that does not exist while taking money in advance, or provides a product of a lower standard than that which was offered for sale.⁵²
- 3.39 Lotteries and charity scams rely on users' familiarity with legitimate lottery and prize sites.⁵³ The ABS, in its first fraud survey report released in 2008, found that fake lotteries accounted for the largest number of victims (84 100) over the previous year.⁵⁴ The ACCC advises that scammers may ask for fees upfront or call premium rate numbers to claim a prize, noting:
- These premium rate calls can be very expensive, and the scammers will try to keep you on the line for a long time or ask you to call a different premium rate number.⁵⁵
- 3.40 Charity scams use online social engineering to play on human sympathies by masquerading as charities or disaster relief campaigns.⁵⁶ The CIS noted that social networking sites are a common vehicle for such scams. For example, during the Japanese earthquake, tsunami and nuclear incidents were exploited by poisoned hotlinks, social networking scams and malicious spam campaigns.⁵⁷

50 Abacus-Australian Mutuals, *Submission 44*, p. 2, and ACC, *Submission 9*, p. 12.

51 ACC, *Submission 9*, p. 12.

52 Australian Human Rights Commission (AHRC), *Submission 2*, p. 6.

53 ACCC, *The Little Black Book of Scams*, 2008 (rev. 2011), p. 7.

54 ABS, *4528.0 Personal Fraud 2007, 2008*, p. 6.

55 ACCC, *The Little Black Book of Scams*, 2008 (rev. 2011), p. 7.

56 AFP, *Submission 20*, p. 4.

57 See CIS, *State of the Nation*, December 2011, p. 6.

Are seniors more at risk?

- 3.41 Anyone can be a victim of cybercrime but, the Committee was advised, Australia's seniors, as a relatively wealthy and recently growing demographic online, are an attractive target for innovative cybercriminals both domestic and international.⁵⁸
- 3.42 Available research also suggests Australian seniors are being disproportionately targeted by, and fall victim to, certain types of online criminal activity dependent on age. The trends also reflect the uptake of online activities by older groups:
- 2008–09 research for the Australian Consumer Task Force (ACTF), found seniors aged 55–65 were most vulnerable to advance fee scams, such as Nigerian scams and 'phishing' scams, while those aged 55 to 64 years and 65 up were more likely to respond to lottery scams.⁵⁹
 - 2011 surveys by the Australian Institute of Criminology (AIC) showed seniors aged 65 plus as most vulnerable to advance fee fraud, with mid-life individuals aged 45 to 54 years most susceptible to dating scams.⁶⁰ The ASIC and ACC reported the growing victimisation of older people, 55 plus, by using cold calling to encourage investment in fake boiler room (SOIF) schemes.⁶¹
- 3.43 A range of specific factors, alone or in combination, were identified as heightening online vulnerability to these types of cybercrime which target the financial, psychological and social circumstances of senior Australians:
- financial situation – well-funded retirees wanting to invest or those with limited wealth seeking funds;
 - reluctant users – required to go online to access health information, other government information or services;
 - unfamiliarity with internet conventions – such as email management, formatting hierarchies and commercial drivers; and

58 AFP, *Submission 20*, p. 2; CIS, *Submission 26*, p. [3].

59 C Budd and J Anderson, 'Consumer Fraud in Australasia', *AIC Reports Technical and Background Paper 43*, p. 14.

60 C Ross and R Smith, 'Risk Factors for Advance Fee Fraud Victimisation', *Trends and Issues in Crime and Criminal Justice no. 420*, AIC, 2011 cited in AHRC, *Submission 2*, p. 6.

61 Australian Securities and Investments Commission (ASIC) *Submission 46*, p. 5, ACC, *Submission 9*, p. 17.

- increased social networking and technology take up, given social trends and the take up of new technologies including android phones, and the rollout of the NBN.

Wealthy or seeking wealth

- 3.44 Mr Michael O’Neill, CEO, of National Seniors Australia Ltd (NSA) informed the Committee that Australia’s seniors are increasingly ‘targets for nefarious activities’, being relatively cashed up at retirement and lacking sophistication with internet and interface technologies. It is this combination which heightens their vulnerability to unscrupulous online scammers.⁶²
- 3.45 The AFP advised that superannuation fraud and boiler room investment schemes are major online threats to midlife and senior Australians.⁶³ The deposit taking industry peak body Abacus-Australian Mutuals reported:
- Seniors have become vulnerable to investment scams particularly since the Global Financial Crisis. The need to supplement reduced incomes, or repair investment portfolios, has made seniors targets for criminals here and overseas... The victims of these scams are usually already in distressed financial circumstances.⁶⁴
- 3.46 The primary victim profile for SOIF schemes are people over 50 years with a university education or high school diploma and good financial knowledge.⁶⁵ The multi-agency Task Force Galilee, in operation since 2011, reports Australian losses to SOIF scams at \$113 million, with investments ranging from \$500 to just over \$ 1 million. The oldest victim, who was 91 years old, lost everything.⁶⁶
- 3.47 While the victims of sophisticated SOIF investment schemes tend to be well educated, financially literate and internet savvy,⁶⁷ less cyber savvy seniors are susceptible to ‘phishing’ scams via phone or email.⁶⁸
- 3.48 The Brotherhood of St Laurence advised that phishing scams trade on older people’s confidence in established institutions and can have a deleterious impact on a person’s reputation if their identity is used to

62 *Committee Hansard*, 31 October 2013, p. 1

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

64 *Abacus -Australian Mutuals, Submission 44*, p. 2.

65 *Mrs Harfield, ACC, Committee Hansard*, 15 August 2012, p. 1.

66 *Mrs Harfield, ACC, Committee Hansard*, 15 August 2012, p. 7.

67 *ACC, Submission 9*, p. 16.

68 *AHRC, Submission 2*, p. 7, *Australian Taxation Office (ATO), Submission 43*, p. 1.

commit fraudulent or illegal acts.⁶⁹ The ATO confirmed that retirees are particularly susceptible to ATO 'branded' phishing scams, especially those using phone call centres.⁷⁰

- 3.49 Research conducted by ACTF has established that people in the 55–64 and 65 plus year age groups are statistically more likely to respond to lottery scams than other age groups.⁷¹
- 3.50 Online lottery scams are particularly attractive to seniors whose incomes are finite and are hence more likely to take a 'flutter' on gambling or lottery sites to gain a fund injection. US studies indicate that people with negative life experiences, such as medical problems and financial difficulties, are most vulnerable to advance fee scams.⁷²
- 3.51 The AIC advised that seniors affected by these scams have limited potential to recover from the loss of their retirement incomes.⁷³

Reluctant and online

- 3.52 Research from Edith Cowan University in WA suggests that, in contrast to other age groups who have quickly embraced online activity, many seniors now participate in online interaction because they must.⁷⁴ Brisbane Seniors Online Association confirmed:

It is becoming increasingly difficult to obtain information without seeing the phrase "for more information go to www..." Organisations at all levels, be they governments, local councils, utilities or business of all types and sizes are gradually 'forcing' their clients to use the internet as a means of doing business by making all other mechanisms too difficult or too expensive. This particularly affects seniors who cannot easily adapt to the new technologies and are fearful of the possible consequences.⁷⁵

69 Brotherhood of St Laurence, *Submission 13*, p. 5.

70 ATO, *Submission 43*, p. 5.

71 C Budd and J Anderson, 'Consumer Fraud in Australasia', *AIC Reports Technical and Background Paper 43*, p. 14.

72 AHRC, *Submission 2*, p. 7.

73 A 2011 study of advance fee fraud victims found that of 59 per cent of respondents had sent an average of \$12 000 each overseas, and 43 per cent of them reported emotional trauma, 40 per cent loss of confidence and 12 per cent marital or relationship problems due to the victimisation. See AIC, *Submission 12*, p. 3.

74 D M Cook, P Szewczyk and K Sansurooah, 'Securing the Elderly', Edith Cowan University WA, presented at the Second International Cyber Resilience Conference, p. 21; cited in Western Australian (WA) Government, *Submission 19*, p. 1.

75 Brisbane Seniors Online Association Inc. (BSOL), *Submission 34*, p. 1.

- 3.53 NSA suggested that the 'lack of interest' reported in many surveys of seniors attitudes to the internet may be feigned to avoid stigma and mask confusion and fearfulness about the technology.⁷⁶
- 3.54 Over 2011 the Department of Broadband, Communication and the Digital Economy (DBCDE) conducted segmentation research to better target cybersafety awareness programs for Australian internet users. Seniors comprised 22 per cent of the 'fearful avoiders' group, who were most likely to report that they did not know enough to protect their privacy or personal information online.⁷⁷
- 3.55 According to the AIC, fearfulness of the internet can increase vulnerability to technology based crime, online or off.⁷⁸ Worries about online security may prompt unwary seniors to subscribe to fake IT security products which introduce viruses onto their computer to collect financial information. Offline scams such as the Do Not Call Register Hoax target seniors frustrated by cold calling, and solicit mobile numbers or other information for use in cybercrime.⁷⁹
- 3.56 The ubiquitousness of the 'Microsoft Scam', where victims are told their computer has a virus which can be rectified by giving external access to hacker, was widely cited to indicate the vulnerability of seniors to multimedia scams.⁸⁰
- 3.57 Older users may be forced onto the internet because of poor health or lack of mobility. They may be isolated or reluctant to seek help, not wanting to burden their friends or family, or fearful of breaking the computer.⁸¹ Those on a limited income may be reluctant to invest in computer upgrades and security systems necessary to keep safe. As discussed later in this chapter, cost was raised as a barrier to internet use by seniors in submissions.

76 NSA, *Submission 29*, p. 15.

77 The surveys identified four online behavioural segments: 'comfortable but weary', 'watchful transactors'; 'confident and (tech) savvy'; and 'fearful avoiders'. DBCDE, *Submission 25*, p. 7.

78 Dr Rick Brown, Deputy Director (Research), AIC, *Committee Hansard*, 10 October 2012, p. 1.

79 WA ScamNet advice to WA Government, *Submission 19*, p. 3; Stay In Touch Pty Ltd, *Submission 47*, p. 3; Dr Cassandra Cross, *Submission 49*, p. 5.

80 Moorook 8 Neighbourhood Watch, *Submission 14*; WA ScamNet advice to WA Government, *Submission 19*, p. 3; Stay In Touch Pty Ltd, *Submission 47*, p. 3, and Mr MacGibbon, CIS, *Committee Hansard*, 14 March 2012, p. 5.

81 Australian Research Council Centre of Excellence for Creative Industries and Innovation (CCI), *Older Australians and the Internet*, 2011, cited in ACMA, *Submission 24*, pp. 7-8.

Unfamiliarity with cyber 'conventions'

- 3.58 While older people can be more cautious about online risks than younger users, the Committee was told that the ease of 'surfing the net' at home tends to induce a false sense that online interaction is secure, private and confidential:

Unfortunately when people get home they are in a relaxed environment – they have a mug of Milo with them, perhaps the fluffy slippers on – feeling pretty relaxed and all of a sudden they divulge all this information which, I would contend, they normally would not in a social real-world setting.⁸²

- 3.59 The Alannah and Madeleine Foundation noted that a senior's usually 'acute judgement of character' can be disabled without visual cues.⁸³ Deprived of these cues, and the normal caution exercised during face to face business or personal interaction, seniors can fall prey to online manipulation.⁸⁴ The Consumer Health Forum Australia (CHF) advised that an older person's trust in published material may also make them less sceptical about information on the internet purporting to be factual, such as health information.⁸⁵
- 3.60 Increased opportunities for online interactions for business and shopping have also opened up new risks for trusting seniors. A West Australian (WA) Government survey found that older users are often unaware of the commercial underpinnings of much online interaction. Lengthy terms and conditions statements in the last stages of online transactions may be ignored and the informality of real estate sites may encourage ill-considered rental and retirement decisions.⁸⁶
- 3.61 DBCDE advised that seniors may be disconcerted by the 'organic' nature of internet search engines.⁸⁷ They may not realise that the top of web search lists are often advertisements,⁸⁸ that product reviews can be fabricated, or that 'pop up' offers on websites may not be verified by web managers, and can be vehicles for fraud or identity theft.⁸⁹

82 Professor Phair, CIS, *Committee Hansard*, 14 March 2012, p. 3.

83 The Alannah and Madeleine Foundation, *Submission 35*, p. 6.

84 AFP, *Submission 20*, p. 2; Professor Phair, CIS, *Committee Hansard*, 14 March 2012, p. 3.

85 Ms Carol Bennet, CEO, Consumer Health Forum of Australia (CHF), *Committee Hansard*, 19 September 2012, p. 1.

86 WA Government, *Submission 19*, p. 2.

87 Mr Abdul Rizvi, Deputy Secretary, Digital Economy and Services Group, DBCDE, *Committee Hansard*, 12 September 2012, p. 2.

88 WA Government, *Submission 19*, pp. 2–3.

89 ACC, *Submission 9*, p. 13.

- 3.62 Seniors can also lack a general awareness of the protocols of emailing, such as the risks of forwarding emails and chain mail.⁹⁰ Stay in Touch, a seniors' computer training provider, noted that they:
- ...[are] often unaware that unwanted emails can appear to be alright when it comes from family or friends when in fact a virus has gotten onto that person's computer and automatically sends an email out to everyone in those peoples' address books.⁹¹
- 3.63 The Australian Seniors Computer Clubs Association (ASCCA) advised that older people may consider they are protecting themselves by clicking on phishing emails to 'unsubscribe' before deleting.⁹²
- 3.64 The Federation of Ethnic Communities' Councils of Australia (FECCA) alerted the Committee to the vulnerabilities of Culturally and Linguistically Diverse (CALD) seniors to the growing threat of cyber racism and bullying.⁹³ The African Seniors Club advised that African seniors in Australia, many without formal education, are inclined to accept everything on the internet as factual and to tolerate abuse by scammers without complaint.⁹⁴
- 3.65 The Alannah and Madeline Foundation referred to similar risks for Aboriginal and Torres Strait Islander Elders.⁹⁵ The Committee notes the ACCC's recent alerts on Nigerian charity scams targeting remote Indigenous communities in South Australia.⁹⁶

Increased social networking

- 3.66 Social networking is becoming an increasingly important tool for communicating with friends and family, with over 10 million Australians having active accounts on the Facebook social networking site.⁹⁷
- 3.67 As the population becomes more mobile and families are dispersed, keeping in contact with family and friends through email, cheap internet

90 WA Government, *Submission 19*, p. 3; Mrs Nancy Bosler, President, ASCCA, *Committee Hansard*, 23 March 2012, p. 21.

91 Stay in Touch Pty Ltd, *Submission 47*, p. 4.

92 ASCCA, *Submission 7*, p. 6.

93 The Federation of Ethnic Communities' Councils of Australia (FECCA), *Submission 40*, pp. 2-3; 5.

94 African Seniors Club – Australia Inc., *Submission 18*, pp. 1-2.

95 Alannah and Madeline Foundation, *Submission 39*, p. 13.

96 SCAMwatch, ACCC 'Beware of Distress Emails Targeting the APY lands', Media Notice, January 2012: <www.scamwatch.gov.au/content/index.phtml/itemId/914432>

97 Facebook, *Submission 36*, p. 2.

phone calls, skyping and social networking sites is increasingly important for seniors. It also offers utility for those who live in outlying regions or who are unable to drive.⁹⁸

- 3.68 Mrs Diana Edwards, Manager of the Italian Australian Pensioners Welfare Association of Tasmania Inc. Day Centre, told the Committee of the importance of Skype to migrant Australians:

Cyberspace as I know it is really a good tool because it opens up, especially for ethnic or cosmopolitan people, a world out there that they can actually bring into their house – to pay bills, to socialise. If I could not see my two grandchildren on Skype I would be most upset, because my son lives in Brisbane.⁹⁹

- 3.69 However, the Committee also heard that older people communicating with relatives or friends on social networking sites maybe easily targeted for identity or information theft.
- 3.70 While Facebook offers users privacy controls and provides advice for people over 50 to keep safe online,¹⁰⁰ Dr Cassandra Cross's research suggested that few seniors have adequate knowledge of security settings on their accounts and believe that only their contacts can access the information.¹⁰¹ The AIC advised that offline crimes such as burglary are supported by information, about holiday plans for example, shared on these sites. Other household members or relatives can also use shared information on computers to perpetrate financial abuses.¹⁰²
- 3.71 Victims of romance and dating scams are often first identified through personal information on social networking or dating sites. While these sites are not as well patronised by seniors compared to younger age groups, many seniors are lonely, isolated and vulnerable to approaches for love or friendship.¹⁰³

98 NSA Productive Ageing Centre, *Older Australians and the Internet*, September 2011, p. 8, attachment to NSA, *Submission 29* and see Facebook, *Submission 36*, p. 2.

99 Mrs Diana Edwards, Manager of the Italian Australian Pensioners Welfare Association of Tasmania Inc. Day Centre, *Committee Hansard*, 7 August 2012, p. 2.

100 Facebook, *Submission 36*, pp. 2–3.

101 Dr Cassandra Cross, Lecturer, School of Justice, Faculty of Law, Queensland University of Technology, *Committee Hansard*, 6 February 2013, p. 9.

102 AIC, *Submission 12*, p. 2. See also Office of the Public Advocate advice to Government of WA, *Submission 19*, p. 3.

103 ACCC, *Targeting Scams: Report of the ACCC on Scam Activity 2011*, p. 12.

- 3.72 Dr Cross advised that the insidious nature of dating romance frauds is not easily counteracted by education, and compounds financial damage with a sense of perceived personal loss.¹⁰⁴

The NBN and technology take-up

- 3.73 While senior citizens are showing an increased interest in going online, there is still a 'digital divide' in the Australian community, with low rates of connection among those over 65 years, across rural populations, and among lower income groups.¹⁰⁵
- 3.74 The rollout of the National Broadband Network (NBN) into regional areas is expected to compound risks associated with low skill or confidence levels, as less cyber savvy regional seniors seek to capitalise on opportunities newly accessible on the web or are required to do so to access services long distance such as banking, telehealth, applying for licences and so on.¹⁰⁶
- 3.75 The Committee's cybersafety survey provides an indication of this potential, with the second most reported problem, malicious software installation, affecting 42.9 per cent of seniors in a rural setting and 31.3 per cent in regional areas, compared with 29.4 per cent in urban areas.¹⁰⁷ The ASCCA advised that many seniors unfamiliar with new technologies don't know how to obtain security software, how to install it or that it must be updated regularly.¹⁰⁸
- 3.76 At the same time, seniors' organisations recorded a burgeoning interest in smartphones and portable tablets which are a more intuitive technology for seniors.¹⁰⁹ Data from Telstra confirms seniors' interest in the use of new technologies such as the smartphone.¹¹⁰ However, the CIS advised that cybercriminals are increasingly adept at infecting smartphones with malware that send out SMS messages, while cross

104 Dr Cassandra Cross, *Submission 49*, p. 26.

105 The Alannah and Madeline Foundation, *Submission 35*, p. 5.

106 AFP, *Submission 20*, pp. 2-3.

107 See Appendix D.

108 ASCCA, *Submission 7*, p. 6.

109 A survey conducted of *YOURLifeChoices* magazine's subscribers over 2011 found ownership of eBook readers and Smartphones had more than doubled compared with 2010 and nearly a quarter of subscribers said that they would purchase an iPad during the next year, while slightly less than a fifth, would invest in a smartphone or e-reader. *YOURLifeChoices*, *Submission 38*, p. 4.

110 According to a June 2011 report, 46 per cent of Australian mobile phones are smart phone, with 23 per cent owned by users aged over 50. See *Telstra Smartphone Index – June 2011*, cited in DBCDE, *Submission 25*, p. 6.

platform Trojans are designed to enable a range of spamming and other criminal activities.¹¹¹

- 3.77 Access under the NBN and use of smartphones also brings into focus seniors' concerns about information security under eHealth initiatives.¹¹² A CIS study observed that eHealth is already using mobile devices (mHealth) to collect vital data and as such will be open to traditional network vulnerabilities.¹¹³

Seniors' responses to risk

- 3.78 Reluctant seniors adopt two main ploys to reduce their risk to cybercrime: avoidance; or selective use. Submissions from seniors' organisations reported that privacy and security are major concerns for older Australians, with fears about these the main reason for avoidance of the internet.¹¹⁴
- 3.79 Recent research cited by the Western Australian (WA) Government suggested that up to 40 per cent of senior Australians avoided internet use, considering themselves to be without the necessary skills, knowledge or interest given concerns about security and/or online viruses.¹¹⁵ Telstra noted that a lack of online skill fosters such fears, and that all internet users are vulnerable if they lack adequate skills.¹¹⁶
- 3.80 According to Dr Cross's research, seniors adopting selective use typically avoid online banking or other financial transactions such as online shopping, even while continuing with research or social networking activities.¹¹⁷ Online fraud victims usually withdrew from using the internet, and through shame or embarrassment kept their experiences to themselves, contributing to their stress and sense of isolation.¹¹⁸

111 CIS, *State of the Nation*, December 2011, pp. 11–12.

112 *YOURLifeChoices*, *Submission 38*, p. 4.

113 CIS, *State of the Nation*, December 2011, pp. 11–12.

114 Australian Seniors Computers Clubs Association, *Submission 7*, p. 7; Hobart Older Persons Reference Group, *Submission 8*, p. 1; Stay In Touch Pty Ltd, *Submission 47*, p. 6.

115 ABC Science survey, 8 August 2011, quoted in *Submission 19*, p. 1.

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

117 Data varies to sample: the Committee's online survey (appendix D) found that 76 per cent of respondents use the internet for banking, more than for any other activity online. See also Legacy Australia for data on 75 plus group, *Submission 10*, p. 2, and BSOL, *Submission 34*, p. 1.

118 Dr Cassandra Cross, *Submission 49*, p. 5.

- 3.81 The Australian Human Rights Commission (AHRC) held that any failure to support older Australians to engage confidently, safely and competently online would demonstrate a threat to their human rights as economies shift to online services.¹¹⁹ Referring to the ‘digital divide’ for seniors above 65, more than half of whom do not access the internet, the Australian Age Commissioner the Hon. Susan Ryan AO stated:

What that means is that those people are missing out on all of the benefits that the rest of the community is enjoying – services like shopping online, banking online, but more and more the access to essential information, including the information that the government provides to Australians on their websites. Often now you find that the information is exclusively available or the service is exclusively available on the net. So it really becomes an equity issue. If older Australians cannot get access then they are missing out on the benefits that the rest of us can enjoy.¹²⁰

- 3.82 The WA Government submission reiterated this position noting that seniors will be denied the benefits of the ‘digital democracy’, and that the digital divide may consolidate as technology use becomes even more prevalent across the general population.¹²¹

Building seniors’ confidence and safety online

- 3.83 The Australian Government and its law enforcement and consumer protection agencies are currently monitoring the prevalence and evolving nature of cybercrime threats to Australians.¹²² A cybersafety focus in policy in recent years has been on the internet safety of younger people, with children and teens being increasingly exposed to online bullying and stalking. This was the subject of the Committee’s interim report, *High Wire Act: Cyber-Safety and the Young*, tabled in Parliament in June 2011.
- 3.84 Evidence covered in this chapter suggests that senior Australians are, in some incidences, disproportionately affected by a range of consumer

119 These rights are preserved under Article 19 of *The Universal Declaration of Human Rights 1948* which states that everyone has the right to ‘seek, receive and impart information and ideas through any media regardless of frontiers’. See *Submission 2*, p. 3.

120 *Committee Hansard*, 23 March 2012, p. 1.

121 Government of WA, *Submission 19*, p. 4.

122 See Chapter 5 for an overview of Government consumer protection and enforcement measures.

fraud activities to which the broader community is also exposed and could benefit from additional assistance and advice.

- 3.85 The Committee does not, however, endorse the position that senior Australians are by definition lacking any necessary capacity to keep safe online. While there is evidence of a 'digital divide' for those above 65 years, there was also an enormous range of IT skills across senior cohorts, and evidence that the proportion of cyber savvy seniors is growing, even as the population ages.
- 3.86 Mrs Joyce Hocking (formerly Sheasby) from Toowoomba was one of those highly skilled seniors who, at 83 years, teaches other older people computer skills. She summed up the value of training to empower the less cyber savvy senior:
- They remind me of hares in the headlights of a ute when they come in, but, by the time they get to the fifth session, they are confident. It has always surprised me that you can change a person's total outlook by a little bit of knowledge.¹²³
- 3.87 In Chapter 4, the Committee covers a broad range of initiatives advanced by the Government and the private sector to improve seniors' cybersafety awareness.
- 3.88 While training and improved user competence were universally agreed as fundamental to enhancing cybersafety among all age groups, there was also a view that government and industry could do more to protect consumers from growing cyber threats.¹²⁴ These issues are discussed in more detail in Chapters 5, on government's consumer protection framework, and 6, on the role of industry.
- 3.89 At a more fundamental level, a number of basic measures were proposed to Government to improve seniors' confidence and capacity to negotiate the web safely. These were to:
- Keep it simple: key safety messages must be headlined
 - Keep it clear: intuitive web design and format
 - Keep it safe: access to security software and advice
 - Keep it easy: a single portal for reporting and advice.

123 Mrs Joyce Hocking (formerly Sheasby), *Committee Hansard*, 31 October 2012, p. 6.

124 Mr MacGibbon, CIS, *Committee Hansard*, 14 March 2012, p. 1.

Keep it simple: key messages for keeping safe

3.90 Given the range of risks to the consumer and the dynamic nature of the evolving cybercrime scene, regulators have recognised that, even with appropriate frameworks in place, online safety rests very much on the acuity of individual internet users.¹²⁵ The AFP advised:

...there must be a degree of online responsibility commensurate with care taken in the real world. It is critical that all internet users exercise a prudent degree of caution in their cyber transactions, be they social, financial or commercial.¹²⁶

3.91 The DBCDE, which is in charge of producing information for cyber awareness, has expressed confidence that older people are receptive to cybersafety messages, referring to recent consumer confidence research on computer security management and online shopping.¹²⁷ Given this receptivity, there was strong support for a new approach to cybersafety awareness: less about the types of risks and more on the real life consequences of certain behaviours.¹²⁸

3.92 Dr Cross, having conducted extensive research in this area in the UK, Canada and the US, considered the Australian approach focusses too much on the 'white noise' around fraud, that is 'the journey and not on the destination':

...We focus on the different ways in which a person can be defrauded...It does not matter how a person is approached for money or why they are approached, we need to focus our prevention message on that transfer of money.¹²⁹

3.93 The fundamental message: 'Do Not Send Money', coupled with the advice that 'if it is too good to be true, it probably is', was reiterated by the AFP, which noted the criticality of promoting these messages as the NBN expands opportunities for computer offences against less technically experienced users.¹³⁰

125 See also DBCDE, *Submission 25*, p. 8.

126 AFP, *Submission 20*, pp. 1, 3.

127 Mr Rizvi, DBCDE, *Committee Hansard*, 12 September 2012 p. 4 and see Ipsos survey conducted for 2012 National Cyber Security Awareness Week (held 12 to 15 June 2012) which recorded older people's receptiveness to online security advice and relative online caution compared with younger age groups, in DBCDE, *Supplementary submission 25.1*, p. 1.

128 Life Activities Clubs Victoria, *Submission 5*, p. 7; CIS, *Submission 26*, p. 2; AFP, *Submission 20*, p. 2.

129 *Committee Hansard*, 6 February 2013, p. 9.

130 AFP, *Submission 20*, p. 2.

- 3.94 The CIS specifically referred to the need to apply ‘real world sensibilities’ to requests for money when using dating sites, given the efficiency of modern methods of money transfer:

....Certainly do not send the money by Western Union where, once it is in the system, you cannot get it out and it is highly efficient at delivering it to the country that you are sending the money to.¹³¹

- 3.95 How these messages might better inform government awareness campaigns is discussed in more detail in Chapter 5.

Keep it clear: user friendly web design and interfaces

- 3.96 Another fundamental recommendation to assist seniors use the internet safely was to ensure that web design and content is presented in a clear and user friendly format.

- 3.97 A review of online security information conducted in 2011 found that government sites, such as the Cybersmart and Stay Smart Online sites, did not meet the needs of seniors and were deficient in terms of content and design. The researchers recommended use of simple language, ease of navigation, and graphical step-by-step tutorials to be more effective.¹³²

- 3.98 Ms Fabienne Balsamo, Senior Policy Officer, AHRC, contrasted the Broadband for Seniors website in Australia with Britain’s online access point for seniors:

...the Age UK website is...incredibly user-friendly. When you go to that website all you need to do is put your postcode in on a big front page and it tells you what services are available in your region and what supports are available. The Broadband for Seniors website has much more embedded information and is much harder to navigate. It took me a while to find where my local services were. I think they have got some really good usability stuff happening in the UK.¹³³

- 3.99 The NSA considered that government and company fora should promote awareness of the issue in a joint campaign to make accessible websites ‘normal business’. Its submission referred to developments by the

131 Mr MacGibbon, CIS, *Committee Hansard*, 14 March 2012, p. 3.

132 D M Cook, P Szewczyk and K Sansurooah, ‘Securing the Elderly’, Edith Cowan University WA, presented at the Second International Cyber Resilience Conference, 2011, p. 21; cited in Government of WA, *Submission 19*, p. 1.

133 *Committee Hansard*, 23 March 2012, p. 2.

National Institute on Ageing and the National Library of Medicine websites as good examples.¹³⁴

- 3.100 The ASCCA reiterated the demand for user friendly websites and accessible learning opportunities if the trend to internet dissemination of government information is to be viable.¹³⁵ In particular, for eHealth:

Designers must make sure that the e-health tools are designed so that they can be used with an absolute minimum of technical knowledge! Even a highly technically skilled person may not be able to use complicated equipment when in a state of wellness or trauma.¹³⁶

- 3.101 The Committee has noted that the Government introduced 'Web Content Accessibility Guidelines' for government internet sites in 2010 to ensure people with a disability are not disadvantaged online.¹³⁷ The guidelines contain mandatory requirements for accessibility including design, navigation, content and quality of presentation and searching results.¹³⁸
- 3.102 On inspection, it appeared to the Committee that the *Web Guide* is complex and technical, being broken down into many topics addressing legal requirements and obligations.¹³⁹ The Committee could see utility in the development of a supplementary web style guide to promote the user friendly design of government information portals.

Recommendation 4

That the Australian Government develops, as a supplement to its *Web Guide*, a web style guide prescribing the key elements of web design to ensure simplicity of language, visual clarity in design and logical navigation tools. This could be supported by graphical step-by-step tutorials for use where applicable.

¹³⁴ NSA, *Submission 29*, p. 29.

¹³⁵ Recommendation 4, ASCCA, *Submission 7*, p. 5.

¹³⁶ Recommendation 5, ASCCA, *Submission 7*, p. 6.

¹³⁷ The Hon. Lindsay Tanner MP (former) Minister for Finance and Deregulation and (former) Parliamentary Secretary for Disabilities and Children's Services, the Hon. Bill Shorten MP, 'Dealing with Government Online to Become Easier for Australians with Disabilities', *Joint Media Release 05/2010*, 23 February 2010.

¹³⁸ Australian Government, *Web Guide: Usability Requirements* <webguide.gov.au/accessibility-usability/usability-testing/> viewed 11 February 2013.

¹³⁹ *Web Guide* <webguide.gov.au/> viewed 23 February 2013.

- 3.103 Departments and agencies are required to report their compliance with the current guidelines to the Australian Government Information Management Office (AGIMO).¹⁴⁰

Recommendation 5

In support of the previous recommendation, the Committee also recommends that, in addition to conducting compliance audits based on the web style guide requirements, the Australian Government Information Management Office should offer an Annual Award for user friendly web design, in part based on public input on the utility of government websites.

Make it safe: access to computers and security advice

- 3.104 The 2011 report *Older Australians and the Internet* found that high costs and uncertainty about computer products and security requirements are barriers to seniors who otherwise were interested in using the internet.¹⁴¹
- 3.105 The State Library of WA observed that, despite decreasing computer costs and associated communication charges, many seniors are still unable to afford the upkeep of a computer. These costs include those for anti-virus and security software and upgrades, and to trouble shoot technical problems. The Council of Ageing WA also advised of frustration about the pace of change and the rate at which technologies became obsolete: seniors are isolated in their struggle to 'keep up'.¹⁴²
- 3.106 Other concerns were the cost and unreliability of broadband services in regional areas. The Hobart Older Persons Reference Group saw broadband cost as a major limit on seniors' online access and skills.¹⁴³ Tandara Lodge Community Care, Sheffield Tasmania, commented on lack of competition between providers in the area, and on the price of antivirus software, computer hardware, printer inks and the 'hidden costs' associated with online shopping.¹⁴⁴

140 Former Minister for Finance and Deregulation and former Parliamentary Secretary for Disabilities, 'Government Releases Website Accessibility National Transition Strategy', *Joint Media Release*, 37/2010, 30 June 2010.

141 CCI, *Older Australians and the Internet*, 2011, cited in ACMA, *Submission 24*, pp. 7-8.

142 See survey of agencies in Government of WA, *Submission 19*, p. 4.

143 The Hobart Older Persons Reference Group, *Submission 39*, p. 1.

144 Tandara Lodge Community Care, Sheffield Tasmania, *Submission 1*, pp. 1-2.

- 3.107 The Committee notes that the Government is supporting seniors by funding free secure internet access and training in libraries, through Seniors Kiosks, under Broadband for Seniors initiatives and at NBN Digital Hub trial sites. Proposals for free online access and training to seniors at these and other community centres had wide support in submissions.¹⁴⁵
- 3.108 However, the NSA contended that while:
- Free internet kiosks and digital hubs will address the barriers of cost and lack of training in those areas that benefit from these initiatives...they are unlikely to fully address the barriers of lack of transport to reach these facilities, ineffective classes and instructional materials, low awareness of the existence of these services, and the need for extra support for older people who access the internet from home.¹⁴⁶
- 3.109 As more services go online and face to face and telephone supports are reduced, the burden of upgrading to new systems and security products will be an increasing strain for seniors, especially if they are physically or mentally fragile.
- 3.110 The Government may wish to consider subsidies or a partnership with private industry to improve seniors' ability to access, apply and maintain security on their home computer or mobile systems. This is considered along with industry's costs settings for computers and security products, in Chapter 6.

Make it easy: a single portal for reporting and advice

- 3.111 A major obstacle to understanding the true extent of victimisation experienced by seniors is the low reportage rate of online crime. Factors which may contribute to this include embarrassment, lack of certainty about the illegality of an activity, or the conviction that there will be no result from reporting.¹⁴⁷
- 3.112 The Committee also heard that the lack of clear reporting avenues for the different varieties of scam and online fraud is a major deterrent to crime

145 AHRC, *Submission 2*, p. 9; Australian Library and Information Association (ALIA) and National and State Libraries Australasia (NSLA), *Submission 6*, p. 2; WA Government, *Submission 19*, p. 5; DBCDE *Submission 25*, p. 3.

146 NSA, *Submission 29*, p. 29.

147 C Budd and J Anderson, 'Consumer Fraud in Australasia', *AIC Reports Technical and Background Paper 43*, pp. 5; 13.

reportage.¹⁴⁸ The AIC's Dr Rick Brown, Deputy Director of Research, explained:

To illustrate, in Australia government agencies that may take reports of cybercrime include state or federal policing agencies, state and territory consumer protection agencies, the Australian Competition and Consumer Commission, the Australian Communications and Media Authority, the Australian Securities and Investments Commission and the Australian Taxation Office. Other organisations that may receive complaints include banks and financial institutions and online trading and auction sites, as well as social media sites. Expand this to multiple victims in multiple jurisdictions and the picture relating to just one case can become very complicated.¹⁴⁹

3.113 There was strong stakeholder support for the streamlining of reporting arrangements, with a range of proposals made for the structure and functioning of an online central reporting point for all cybercrime:

- The CIS recommended an 'online central clearing house for complaints', noting that seniors in particular are confused and distressed by current arrangements.¹⁵⁰
- The ACC also envisioned a single portal or co-ordinated gateway to direct the user to the correct information, and for help and advice.¹⁵¹
- Internet shopping site eBay and payment manager PayPal recommended a single contact point or a 'co-ordinated set of entry points' to provide all victims with guidance and support.¹⁵²
- YOURLifeChoices, the online seniors' magazine, advocated for an industry and government supported 'one-stop-shop' for seniors in particular, backed up by telephone support, with access to education and advertising of cybersafety issues.¹⁵³

148 *YOUR LifeChoices*, the seniors' online magazine conducted an online survey and received 701 individual comments on why seniors did not report a scam. 14 per cent stated they didn't know who or where to report the crime. See Mr Drew Patchell, Publisher Owner Director, *YOURLifeChoices* website, *Committee Hansard*, 18 May 2012, p. 2.

149 Dr Rick Brown, Deputy Director (Research), AIC, *Committee Hansard*, 10 October 2012, p. 2.

150 Professor Phair, CIS, *Committee Hansard*, 14 March 2012, pp. 1, 10.

151 Mrs Harfield, ACC, *Committee Hansard*, 15 August 2012, p. 3.

152 eBay and Pay Pal, *Submission 11*, Recommendation 4, p. [3].

153 *YOURLifeChoices* website, newsletters and magazine, *Submission 38*, p. 4.

- The South Australian and WA Governments suggested that the DBCDE's Stay Smart Online site be upgraded for both information and reporting of offences, with a specific seniors' tab.¹⁵⁴
- 3.114 Submitters emphasised that a user friendly format, with clear language and graphics and less embedded information, is particularly important to engage seniors.¹⁵⁵ WA ScamNet recommended its model where scam warnings appear at the top of search engine lists, noting that ACC and ASIC websites do not currently do this. An archive of online warnings could also be uploaded.¹⁵⁶
- 3.115 The site should also link to a seniors' victim support or help line for personalised, non-technical advice.¹⁵⁷ Dr Cross reported that the UK and Canada have well developed online reporting sites which also offer victim support services, delivered by charitable agencies:
- In the United Kingdom, support for victims is facilitated by having a central reporting authority. When a victim calls Action Fraud to report whatever fraudulent experience they have had, they are then asked about the impact of that fraud on their life. If they rate the impact as quite severe they are then given the opportunity to receive a follow-up call from Victim Support, which is a charitable organisation over there, and they are able to receive some follow-up counselling to help them get back on their feet. That can be through either a telephone call or face-to-face counselling. Canada has a very similar program.¹⁵⁸
- 3.116 The Committee notes that the Government has recently launched a seniors' helpline under its Broadband for Seniors initiative.¹⁵⁹ The Committee, however, believes that there would be merit in centralising reporting and support mechanisms for all cybercrime victims who need support or advice.

154 WA Government, *Submission 19*, ref. WA Department of Health and Department of Finance, p. 5; and Recommendation p. 8; SA Government, *Submission 37*, p. 11.

155 Government of WA, *Submission 19*, p. 5; Mr MacGibbon, *Committee Hansard*, 14 March 2012, p. 11; Ms Balsamo, AHRC, *Committee Hansard*, 23 March 2012, p. 2.

156 See, WA Government, *Submission 19*, p. 5.

157 WA Government, *Submission 19*, ref. Department of Communities, and Rec. p. 8.

158 *Committee Hansard*, 6 February 2013, p. 10.

159 In November 2012, see FaHCSIA, Broadband for Seniors website < www.necseniors.net.au/ > viewed 15 February 2013.

Recommendation 6

That the Australian Government develops a centralised user friendly reporting and cybersafety awareness portal for all types of cybercrime with links to relevant regulators.

The site should feature a dedicated reporting tab, a seniors tab and be backed up by a telephone service which links individuals to appropriate victim support, training and other advice.

Recommendation 7

In support of the above, the Australian Government should investigate options for the contracting of appropriate non-government organisations or private organisations to provide support and advice to victims of online and technology related crime.

- 3.117 Another strong commendation for the centralised reporting facility is the need to collect and collate data on the various types of cybercrime and its effect on different segments of the community, including seniors. The criticality of this data to target both consumer education and to fine tune legislation and enforcement measures against cybercrime was universally emphasised by stakeholders.¹⁶⁰ The role for government in progressing this initiative is discussed in Chapter 5.

Concluding comments

- 3.118 Compared with the rest of the world, Australian seniors are an attractive target for cybercriminals. Relatively new to the internet, many are also relatively affluent.
- 3.119 Australia's mandatory superannuation requirements allow a lot of Australians to retire with lump sums to invest, or operate their own self-managed funds. Others may seek to establish an income stream for retirement, or be living on part or full pensions, and be tempted by online gambling, lotteries or other windfall schemes.

¹⁶⁰ AFP, *Submission 20*, p. 5; CIS, *Submission 26*, ACMA, *Submission 24*, p. 2 and see Mr Rizvi, DBCDE, *Committee Hansard*, 12 September 2012 p. 4.

- 3.120 Given the dynamic nature of the internet and opportunism of global organised crime networks, the rollout of the NBN into regional areas, and seniors' increasing attraction of the tablet and the smartphone, it will be essential to ensure older Australians are upskilled and aware of both the risks and benefits of using digital technologies.
- 3.121 In addition to the range of cyber threats to which the community is exposed, the Committee also heard about the negative consequences of some seniors' risk averse behaviours. In the Committee's opinion, overcoming the fear of the unfamiliar will help seniors over 'the hurdle' of the digital divide.
- 3.122 In support of this, the Committee has made recommendations in this chapter to help seniors help themselves by providing for clear and more user friendly government information online, and by establishing a centralised access point for information and crime reportage, with follow up support for victims when needed.
- 3.123 In the following chapters, the Committee examines possible measures to address education and training needs, proposals for improved consumer awareness and regulatory reform, and the potential role of industry to help seniors gain confidence and remains safe online.

Cybersafety education and training for seniors

Introduction

- 4.1 Lack of knowledge about the internet and how to be cybersafe online was identified in Chapter 2 as one of the main barriers preventing many seniors from being active online. Other parts of this report examine how technical solutions can provide some degree of protection against security threats. This chapter will look at the role of education and training in preparing seniors to be safe online and keeping them cybersafe into the future.
- 4.2 The risks experienced by seniors when using the internet are not significantly different to those experienced by anyone else, however what can be seen as unique to a significant number of seniors is their lack of knowledge about the internet. Dr Cassandra Cross told the Committee that:

Having not grown up with the technology or been exposed to it in the same way as younger generations have experienced, this can impact on their ability to use the internet safely and in some cases may contribute to their victimisation. While many seniors have an in-depth understanding of the internet, there are many more who do not have such knowledge. ...a lack of knowledge [can] create

fear of the unknown and an awareness of the risks posed by online fraud tends to exaggerate this fear.¹

- 4.3 Computer literacy in itself is not enough to ensure that seniors will be safe online. Lack of knowledge about cybersecurity can make seniors vulnerable to myths and scams. Cybercriminal activities such as phishing will continue to evolve and people will continue to be one of the weakest links in attempts to secure systems and networks. Therefore, 'user awareness and education and training are critical in mitigating many types of cyber threats.'²
- 4.4 The inquiry found that there is a substantial amount of cybersafety education available in various guises but it is mostly online and for a senior who is fearful of going online it could be hard to find the help that he or she needs, if indeed they even recognise that they do need knowledge about cybersafety.
- 4.5 Across Australia various groups have taken on the task of providing cybersafety education and training to seniors and the Committee is impressed by their efforts. From state and public libraries all around the nation, to Universities of the Third Age (U3As), computer groups, seniors' clubs and church groups, the Committee found a dedication, often by seniors themselves, to bringing all seniors 'up to speed' so they can safely enjoy the benefits of participating in the digital age.

How seniors prefer to learn

- 4.6 The Committee took a lot of evidence that seniors who are hesitant to go online prefer to learn about computers and cybersafety from their peers.
- 4.7 In most cases, where cybersafety education is offered by seniors' groups, it is delivered by seniors. Those who are learning see that others of their own age have succeeded in learning to use the technology safely, giving them confidence that they too can learn to be cybersafe:

If people have concerns like, 'Is it safe?' or, 'I'm old; I can't do it,' and all those sorts of things, if the person who is teaching them is a

1 Dr Cassandra Cross, *Submission 49*, p. 5.

2 Australian Securities and Investments Commission (ASIC), *Submission 46*, p. 6.

peer and has had those concerns and has overcome them, there is a level of comfort and identification with the person.³

- 4.8 The Committee heard that when seniors teach seniors they do so at a pace which works. Several witnesses said that when younger people teach seniors cybersafety, the pace is often too fast. Mrs Nancy Bosler, President of the Australian Seniors Computer Clubs Association (ASCCA), told the Committee that 'if a senior is motivated to use technology and can learn at their own pace, they are likely to succeed'.⁴ Once seniors are active online, then they are usually comfortable asking their children or grandchildren to solve their internet problems, but 'seniors who are not online appear to prefer to learn from a peer'.⁵
- 4.9 ASCCA estimates that more than 150 000 seniors have learned how to use a computer through its peer-assisted learning programs.⁶
- 4.10 At U3As around the nation senior volunteers tutor seniors in a variety of courses, including computer courses with cybersafety components. Seniors who attend U3A computer classes are often not initially confident that they can learn the technology but 'once they realise they are being taught by someone in their age group...they seem to relax'.⁷
- 4.11 The Communications Law Centre at the University of Technology in Sydney (CLC) said that senior Australians who are savvy internet users have an important role to play in creating a safer online environment for other seniors. Seniors who have years of experience online are well placed to engage with other seniors to give advice on how to navigate the internet and how to access online services, as well as providing advice on cybersafety. CLC said that many seniors are currently helping other seniors in this way.⁸

DBCDE / COTA NSW Peer Education Program

- 4.12 In recognition that many seniors prefer to be trained by their peers, the Department of Broadband, Communications and the Digital Economy

3 Ms Bonnie Simons, Senior Research Officer, Retirement and Ageing, Research and Policy Centre, Brotherhood of St Laurence, *Committee Hansard*, 18 May 2012, p. 22.

4 *Committee Hansard*, 23 March 2012, p. 18.

5 Mr Abul Rizvi, Deputy Secretary, Digital Economy and Services Group, Department of Broadband, Communications and the Digital Economy (DBCDE), *Committee Hansard*, 12 September 2012, p. 3.

6 ASCCA, *Submission 7*, p. 26.

7 Mrs Joyce Hocking (formerly Sheasby), *Committee Hansard*, 31 October 2012, p. 7.

8 The Communications Law Centre (CLC), University of Technology in Sydney, *Submission 31*, p. 3.

(DBCDE) recently provided funding to the Council on the Ageing in NSW (COTA NSW) to develop a peer education program. Called *Internet Safety: Be Confident Online*, the program trains seniors to deliver cybersafety education sessions to other seniors in a relaxed and informal setting. Mr Abdul Rizvi from DBCDE said that it is not so much about how to use the internet, but rather the program aims to alleviate the fears that make seniors avoid using the internet:

...[It] can be delivered with or without a computer wherever seniors meet – such as the local library, community hall or at regular group meetings. This gives the program a broad reach into the community allowing it to engage seniors who might not have a digital hub nearby.⁹

- 4.13 COTA NSW told the Committee that the Internet Safety: Be Confident Online program has three major objectives, which are:

...to collect older people's ideas and concerns in relation to cybersecurity, generate discussion to address any barriers and myths and to then introduce the older people to practices that increase security.¹⁰

- 4.14 COTA Tasmania is working with COTA NSW and has successfully trained peer educators in Tasmania using Internet Safety: Be Confident Online. COTA Tasmania's CEO Mrs Sue Leitch said:

COTA has been using the peer education model for a while now and it is very successful. It is where volunteers of the same age as the target groups are trained in a particular subject and then that goes out to regular groups of people that meet normally, so it is a safe environment for people to learn in.¹¹

Inter-generational cybersafety help

- 4.15 In addition to peer education, there is a role for young people to help seniors with cybersafety. The Australian Communications and Media Authority (ACMA) told the Committee:

[We] encourage young Australians to pass on their user knowledge and practices to older members of their family to ensure safety of their parents and grandparents in online environments. This not only affirms positive online practices and

9 Mr Rizvi, DBCDE, *Committee Hansard*, 12 September 2012, p. 2.

10 Council on the Ageing NSW (COTA NSW), *Submission 39*, pp. 1-2.

11 *Committee Hansard*, 7 August 2012, p. 3.

experiences of senior community members, but strengthens a young person's own knowledge (through the necessity for clear communication skills and reinforcement of their digital citizenship skills) and incidentally promotes close and respectful inter-generational family relationships.¹²

- 4.16 Young people might also play a role as cybersafety mentors to seniors and again, such a relationship could be beneficial to both parties. Dr Judith Slocombe CEO of the Alannah and Madeline Foundation said that:

Children from an eSmart school have the knowledge to become mentors to older Australians in the skills of using technology and already some eSmart schools are linking young people with seniors. Young people are often experts in the smart use of technology and even know how to use privacy and safety settings but sometimes lack the wisdom that makes them behave responsibly. Grandparents and other seniors in a child's life can play an important role here.¹³

Cybersafety education for the most vulnerable

- 4.17 The Committee heard from several witnesses that if all Australians are to have equal access to the opportunities of the internet, educational initiatives must reach those who are most vulnerable.¹⁴

- 4.18 In its submission to the inquiry, the Australian Federal Police (AFP) questioned whether the Government's messages about cybersafety are reaching the most vulnerable in the community, saying some of the cybersafety campaigns are now in their second or third iteration and, therefore:

We should question whether awareness is reaching across the entire community through all socio-economic and culturally and linguistically diverse aspects and age groups and therefore reaching the most vulnerable.¹⁵

12 Australian Communications and Media Authority (ACMA), *Submission 24*, p. 10.

13 *Committee Hansard*, 18 May 2012, p. 36.

14 See, for example, the CLC, *Submission 31*, p. 2.

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

- 4.19 Commander Glen McEwen from the AFP told the Committee that the AFP 'plays a pivotal role in addressing cybercrime operationally and ensuring senior Australians have confidence in continued online engagement.'¹⁶
- 4.20 The South Australian Government expressed concern about vulnerable groups, such as Aboriginal people, older people from culturally and linguistically diverse backgrounds and older people living in rural and remote areas, not being able to keep up-to-date with new technology and ultimately becoming socially isolated from friends and family. It is, therefore, important that all seniors 'are provided the opportunity to develop the knowledge and confidence needed to use the internet effectively'.¹⁷

Cybersafety education for life

- 4.21 Everyone needs to continuously update their awareness of cybersafety practice. This means that everyone, including seniors, needs to be able to access up-to-date information and education on cybersafety, even if it is quite informal updating. Mr Alastair MacGibbon from the Centre for Internet Safety said cybersafety education 'needs to be generational, consistent and sustained'.¹⁸
- 4.22 Or, as Ms Andree Wright from ACMA put it:
- We are increasingly focusing on the notion of cybersafety education as something you need to equip you from the cradle to the grave in this day and age.¹⁹
- 4.23 Mrs Karen Harfield from the Australian Crime Commission (ACC) told the Committee that the next generation of seniors should reach that stage of their life fully confident about current technology so that they can use it to enhance their quality of life.²⁰

16 Commander Glen McEwen, Manager, Cyber Crime Operations, AFP, *Committee Hansard*, 13 March 2013, p. 2.

17 South Australian Government, *Submission 37*, pp. 3–4.

18 Mr Alastair MacGibbon, Co-Director, Centre for Internet Safety (CIS), University of Canberra, *Committee Hansard*, 14 March 2012, p. 8.

19 Ms Andree Wright, General Manager, Digital Economy Division, ACMA, *Committee Hansard*, 23 March 2012, p. 37.

20 Mrs Karen Harfield, Executive Director, Fusion, Target Development and Performance, Australian Crime Commission (ACC), *Committee Hansard*, 15 August 2012, p. 1.

Cybersafety education currently available for seniors

- 4.24 Most cybersafety education is currently being delivered as a component part of a 'computer course' or via one of the various government websites which offer cybersafety information and advice (see Appendix E).
- 4.25 As mentioned above, computer courses with cybersafety as a component are being delivered by a variety of organisations. Courses where cybersafety is the sole topic are few but they do exist, for example, the U3A in Toowoomba has recently added a cybersafety awareness short course to its program.²¹
- 4.26 Many seniors receive cybersafety training informally when receiving help from library assistants or friends, etc. Every day around the nation public libraries are offering practical help with:
- ...setting up email accounts, online banking, setting up mobile phones, completing government forms, accessing e-government information, applying for Centrelink benefits, etc...[while] passing on cybersafety training as they are doing so.²²
- 4.27 Libraries also provide one-on-one and group sessions on cybersafety for seniors but they are limited in what they can offer seniors by the amount of available resources.²³
- 4.28 Some of those seniors' groups, organisations and clubs around the nation which offer members cybersafety training and updates in various ways include:
- National Seniors Australia (NSA) which uses its national magazine to inform its members about scams and its 'IT column' educates its members about new technology.²⁴
 - Brisbane Seniors Online Association (BSOL) which offers its members training in the home on the learner's own computer, including a basic security assessment of the computer, 'for a reasonable and cost-effective annual membership fee'. BSOL has over 1,000 active members and no paid staff. Trainers are volunteers.²⁵

21 Mrs Hocking, *Committee Hansard*, 31 October 2012, p. 6.

22 Australian Library and Information Association and National & State Libraries Australasia (ALIA and NSLA), *Submission 6*, pp. 2, 4.

23 ALIA and NSLA, *Submission 6*, p. 3.

24 Ms Saunders, General Manager, Public Affairs, National Seniors Australia Ltd (NSA), *Committee Hansard*, 31 October 2012, p. 5.

25 Brisbane Seniors Online Association Inc.(BSOL), *Submission 34*, p. 1.

- The YOURLifeChoices website for seniors has over 61,500 subscribers to its e-newsletters and e-magazine which continuously update members with new information about technology and cybersafety.²⁶
 - ASCCA, in partnership with the AFP, delivers sessions to seniors who are active online about how they can protect their personal and financial information, use secure online banking and secure their wireless connections.²⁷
- 4.29 In Victoria, seniors who can afford it can have cybersafety training in their own home as part of an overall package to get them online. A Melbourne-based company assists seniors with a range of services including help to purchase affordable hardware and appropriate internet (and phone) plans, set-up in their home, ensuring the technology is secure and virus-free, providing one-on-one tutoring including cybersafety information, and ongoing IT support.²⁸ Ms Joanne Lambie told the Committee that:
- ... the best medium for teaching seniors, and ensuring knowledge retention and implementation is through one-on-one tutoring.²⁹
- 4.30 The Department of Veterans' Affairs has used its newsletter Vetaffairs on several occasions to publish articles to raise awareness in the veteran community of scams targeted at its clients.³⁰
- 4.31 Telstra runs the Telstra Connected Seniors program which helps seniors to learn more about technology, and how to engage more safely and securely online. Telstra says the program offers individual self-teach guides, fun interactive workshops, and also offers 'eligible community groups with the opportunity of funding to run successful training courses around technology'.³¹ The Telstra Connected Seniors website receives approximately 5000 unique visits each month.³²
- 4.32 The Telstra Connected Seniors program is, according to the South Australian Government, one of the few initiatives which provides training for seniors in using new technology, such as tablets and smartphones, to access the internet. Participants are provided with access to an iPad and instructional materials at sessions which are held across Australia. In
-

26 YOURLifeChoices website, e-newsletters and magazine, *Submission 38*, p. 4.

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

28 Ms Joanne Lambie, *Stay In Touch Pty Ltd, Submission 47*, p. 1.

29 *Stay In Touch, Submission 47*, p. 7.

30 Department of Veterans' Affairs, *Submission 30*, p. 2.

31 Telstra Corporation Ltd, *Submission 22*, p. 3.

32 Telstra Corporation Ltd, *Submission 22.1*, p. 2.

South Australia such sessions have been held in aged care facilities, among other venues.³³

- 4.33 In Queensland, the Carindale Police Citizens Youth Club launched its Seniors Online Security Project, which is a training package targeted specifically at seniors about online security issues. Five separate modules were developed on the topics of computer security, identity crime, social networking, fraudulent emails and internet banking. The key message in each module is that ‘no-one should send you an email asking for personal details’ and each module encourages people to think through the consequences of sending information or money. Rather than focusing on the ways in which a person can be targeted to send personal information or money, the training materials specifically focus on the sending of personal data or the transferral of money.³⁴
- 4.34 The Seniors Online Security Project is available to anyone and includes Powerpoint presentations. Dr Cassandra Cross told the Committee that feedback from seniors groups about the training material has been overwhelmingly positive, especially in terms of the content and how it is presented to seniors.³⁵
- 4.35 Government departments also play a significant role in helping seniors become cybersafe, offering – for those who are confident enough to use the internet – online training and cybersafety advice. For those not active on the internet, there are other government cybersafety initiatives. The various Australian Government cyber safety education and training initiatives are discussed later in this chapter.

Off-line cybersafety education for seniors

- 4.36 For those seniors who are not yet online information about cybersafety must be delivered using off-line methods. The Australian Human Rights Commission (AHRC) noted that:

Information about cyber safety needs to be extended to offline media platforms in order to reach older Australians who are not yet online and may have concerns about going online due to safety issues. Older Australians are still very loyal to traditional media platforms such as TV, radio and print.³⁶

33 South Australian Government, *Submission 37*, p. 12.

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

35 Dr Cassandra Cross, *Submission 49*, p. 8.

36 The Australian Human Rights Commission (AHRC), *Submission 2.1*, p. 3.

- 4.37 The Committee heard that given the shift to providing almost all information via government and commercial websites, the Government has a responsibility to educate everyone about the benefits of using information technologies extensively and ‘this education should balance the benefits against the risks, without unduly emphasising risk’.³⁷
- 4.38 When current affairs programs on television air reports highlighting scams and other cybersafety problems, these can help to raise awareness of cybersafety among seniors and ‘heighten their sense of caution’.³⁸ However, the Committee took evidence that there is a fine line between raising awareness and frightening seniors so that they fear the internet and refuse to learn how to use it.³⁹ Many witnesses said that positive messages along the lines of ‘you can learn how to be safe online’ are more productive.
- 4.39 It was suggested to the Committee that if short, targeted messages about cybersafety were shown as commercials on free-to-air television during ‘the soaps’ those messages would reach a large proportion of seniors who are not yet online.⁴⁰
- 4.40 Life Activities Clubs Victoria told the Committee that educational campaigns using traditional media to explain the benefits of the internet and to encourage people to use the available technologies:
- ... must preclude scaremongering. [They] must also emphasise the simplicity (and safety) of using these technologies and provide information on where basic skills can be acquired ... quite a few opportunities already exist, but are poorly promoted and consequently under-utilised.⁴¹

Incidental cybersafety education for seniors

- 4.41 Incidental learning can play an important role in helping seniors to become familiar and competent internet users. Dr Helen Kimberley from the Brotherhood of St Laurence said that this sort of learning would be

37 Life Activities Clubs Victoria Inc. (LACVI), *Submission 5*, p. 3.

38 WorkVentures Ltd, *Submission 33*, p. 4.

39 See, for example, Mr Lindsay Doig, President, LACVI, *Committee Hansard*, 18 May 2012, p. 14; Mrs Diana Edwards, Italian Australian Pensioners Welfare Association of Tasmania Inc. Day Centre, *Committee Hansard*, 7 August 2012, p. 2; COTA NSW, *Submission 39*, p. 1.

40 Mrs Hocking, *Committee Hansard*, 31 October 2012, p. 7.

41 LACVI, *Submission 5*, p. 2.

helped by 'an expansion of social inclusion programs that support people and assist them to come together'.⁴²

- 4.42 Seniors' groups which meet for purposes other than cybersafety education can be an important builder of ICT competence. Ms Bonnie Simons from the Brotherhood of St Laurence told the Committee that social venues such as craft groups, Men's Sheds or Neighbourhood Houses often offer activities which use the internet for information, techniques or technical patterns, so incidental cybersafety learning occurs as participants use the internet to take part in the activity.⁴³
- 4.43 The Brotherhood of St Laurence believes that while government support for skills development is very important, support and funding for social engagement opportunities is equally important to ensure that seniors have access to spaces where they can meet to discuss and share tips and advice about safe internet use.⁴⁴

Government cybersafety training initiatives

- 4.44 The Australian Government's cybersafety initiative is part of a whole-of-government initiative involving DBCDE, ACMA, the Commonwealth Director of Public Prosecutions (DPP) and the AFP. The current initiative is a continuation of the former government's 'Protecting Australian Families Online' initiative which was implemented in 2007-2008. Funding for the Cybersafety initiative was \$49 million over the four years 2009-2012.
- 4.45 Several Australian Government departments and agencies host informative cybersafety for seniors pages on their websites as do various State and Territory departments. The presentation and accessibility of websites with cybersafety information aimed at seniors was discussed in the previous chapter. This chapter is looking at what is available for seniors seeking cybersafety information.
- 4.46 DBCDE and the Department of Families, Housing, Community Services and Indigenous Affairs (FaHSCIA) both have a vast amount of information about cybersafety on their websites.
- 4.47 ACMA also has a vast amount of cybersafety information, although none of it is targeted specifically at seniors.

42 Dr Helen Kimberley, Principal Researcher, Research and Policy Centre, Brotherhood of St Laurence, *Committee Hansard*, 18 May 2012, p. 17.

43 Ms Simons, Brotherhood of St Laurence, *Committee Hansard*, 18 May 2012, p. 19.

44 Brotherhood of St Laurence, *Submission 13*, p. 8.

- 4.48 Additionally, government organisations such as the Australian Competition and Consumer Commission (ACCC) have informative publications about cybersafety on their websites.
- 4.49 The obvious problem is that if seniors are not online then they will not see, and are probably unaware of, the wealth of available information and where to find it.
- 4.50 While all Governments have made a concerted effort to educate young Australians about cybersafety, reaching seniors who are not active online to educate them about cybersafety has been less ubiquitous and presents particular problems:
- The use of State education resources and popular internet programs makes the dissemination of information [to young people] relatively easy compared to doing so for senior Australians. The difficulty is that to gain access to useful information about cybersafety one has to use the internet so it becomes a “chicken and egg” situation.⁴⁵
- 4.51 Specific government cybersafety training initiatives are discussed below.

DBCDE's cybersafety training

- 4.52 DBCDE is the lead department in cybersafety education for all Australians. It hosts the Stay Smart Online website which is the Government's cyber security website designed to help everyone understand cyber security risks and to educate home and small business users on the simple steps they can take to protect their personal and financial information online.⁴⁶
- 4.53 National Cyber Security Awareness Week is one of DBCDE's key awareness-raising initiatives. Each year the week is held in partnership with industry, consumer and community groups and all levels of government. Mr Rizvi said that DBCDE works closely with ASCCA during the week to ensure it has a focus on senior Australians.⁴⁷
- 4.54 Additionally, DBCDE uses Seniors Week to promote messages to seniors on the Stay Smart Online website, as well as through a range of articles, promotional material and other activities.⁴⁸

45 Legacy, *Submission 10*, p. 2.

46 DBCDE, <www.staysmartonline.gov.au/about> viewed 5 February 2013.

47 Mr Rizvi, DBCDE, *Committee Hansard*, 12 September 2012, p. 1.

48 Mr Rizvi, DBCDE, *Committee Hansard*, 12 September 2012, p. 1.

- 4.55 DBCDE's Digital Hubs program (see Chapter 2) helps local communities gain the skills needed to maximise the expected benefits provided by the National Broadband Network. The program is providing local residents with training in digital literacy skills, including cybersafety and security. The hubs have a focus on people who have yet to engage online and seniors are one of the target groups for the program.
- 4.56 A new website called Internet Basics has been developed to assist the digital hubs deliver the training. It provides introductory information and training for people with little or no experience with the internet to enable them to engage online safely and securely. A number of senior Australians helped to develop the website.⁴⁹
- 4.57 At the digital hubs, a DBCDE staff member will sit with any senior who has never used a computer and help them to get started in a 'very hands-on way'. Mr Rizvi told the Committee:
- Once seniors are familiar with the basics of getting online they can then participate in seminars on specific online topics at these hubs. Each of these seminars generally has a component on cybersafety and security. For example, if they are attending a seminar on online shopping they will have as a dimension of that seminar how to remain safe whilst they shop online.⁵⁰
- 4.58 DBCDE told the Committee it has received very positive feedback from seniors who have used the Internet Basics website and participated in the training to develop digital literacy skills.⁵¹
- 4.59 The Cybersafety Help Button on DBCDE's website is focussed on children and young people but has information for everyone, providing internet users with easy online access to a range of cybersafety and security information and assistance.
- 4.60 The Easy Guide to Socialising Online can be accessed using the Cybersafety Help Button. It provides cybersafety information about social networking sites, search engines and online games and gives instructions on how to report cyberbullying, abuse and inappropriate content on sites, as well as clear information on how to adjust privacy settings and tips on how to stay safe when using a social media site.⁵²

49 Mr Rizvi, DBCDE, *Committee Hansard*, 12 September 2012, p. 1.

50 Mr Rizvi, DBCDE, *Committee Hansard*, 12 September 2012, p. 1.

51 Mr Rizvi, DBCDE, *Committee Hansard*, 12 September 2012, p. 1.

52 Mr Rizvi, DBCDE, *Committee Hansard*, 12 September 2012, p. 2.

Broadband for Seniors Initiative

- 4.61 In 2008 the Australian Government committed \$15 million to its Broadband for Seniors Initiative, which is run by FaHSCIA. The initiative set-up 2,000 free internet kiosks across Australia in community centres, retirement villages, ex-service organisations and various seniors clubs. In 2011 a further \$10.4 million over four years was committed to support the kiosks and to assist seniors to develop skills in technology.
- 4.62 Trainers and tutors are available at the kiosks to assist people over 50 to develop computer and internet skills so they become comfortable using the internet and sending emails. All seniors are welcome to use the kiosks to improve their computer skills whether or not they are connected to the internet at home.⁵³
- 4.63 At the kiosks, seniors receive access to training materials including an online development course so that they can learn at their own pace, particularly on their computers at home. Training courses were designed with the unique learning needs of seniors in mind and are easy to use – even for those who have never used a computer before.⁵⁴
- 4.64 Guidance and on-going support is provided in a friendly face-to-face environment by volunteer tutors on topics such as how to email and surf the internet, how to use Skype, and how to stay safe online. However, volunteers are not permitted to teach how to access internet banking, complete online shopping, or any other activity where the participant needs to disclose personal or financial information.⁵⁵
- 4.65 If volunteer tutors are not permitted to provide financial training, seniors may be left with a gap in their knowledge, for example, they need to learn what information is safe to provide on the internet, which organisations should be provided with personal and private information and in which context this information should be provided. The South Australian Government suggested that other avenues, such as external facilitators, could be pursued to provide this training at the kiosks in a safe manner.⁵⁶
- 4.66 Feedback to FaHSCIA about the kiosks has been extremely positive. Seniors who have been trained at the kiosks have told FaHSCIA:
-

53 Department of Families, Housing, Community Services and Indigenous Affairs (FaHSCIA), <www.fahcsia.gov.au/our-responsibilities/seniors/programs-services/broadband-for-seniors> viewed 8 January 2013.

54 FaHSCIA, <www.fahcsia.gov.au/our-responsibilities/seniors/programs-services/broadband-for-seniors> viewed 8 January 2013.

55 South Australian Government, *Submission 37*, p. 13.

56 South Australian Government, *Submission 37*, p. 13.

... [they] now having the confidence to chat to family online, surf the internet, send emails and even join social media sites such as Facebook and Twitter.⁵⁷

- 4.67 In late 2012 FaHSCIA launched the Broadband for Seniors website which provides many resources including, as noted in the previous chapter, a telephone helpline number for seniors who want to speak to a person about cyber safety concerns or to report a cybercrime. The need for a telephone helpline number for seniors who want to speak to a person about cyber safety concerns was raised during the course of the inquiry by several witnesses.⁵⁸
- 4.68 On the Broadband for Seniors website there is a direct link to the DBCDE Cyber Safety Help Button and links to other cybersafety resources, as well as free online training and a list of organisations that currently host a Broadband for Seniors kiosk.

ACMA's Cyber[smart] website

- 4.69 ACMA hosts an informative website called Cyber[smart] on which cybersafety information specifically targets 'Young kids', 'Kids', 'Teens', 'Parents', 'Libraries' and 'Schools'. While not specifically targeting 'Seniors', they can find a lot of useful information about cybersafety on the website.
- 4.70 ACMA has been researching cyber issues and delivering cyber-related education programs for more than 10 years. Cyber[smart] provides critical information on risks including online scams, malware, hacking and identity theft. This information gives practical steps to take with privacy, reporting mechanisms, passwords and security software, to assist in recognising and minimising online risks (see next chapter for more about ACMA).⁵⁹

SCAMwatch

- 4.71 SCAMwatch is a website run by the ACCC (see next chapter for more about the ACCC). SCAMwatch provides information to consumers and small businesses about how to recognise, avoid and report scams.

57 FaHCSIA, <www.fahcsia.gov.au/seniors/news/2012/new-broadband-for-seniors-website-now-live> viewed 29 January 2013.

58 See for example: YOURLifeChoices website, newsletters and magazine, *Submission 38*, p. 4.

59 ACMA, *Submission 24*, p. 10.

- 4.72 The SCAMwatch website notes that many scams originate overseas or take place over the internet, which makes them very difficult to track down and prosecute. The ACCC warns that if people lose money to a scam, it is unlikely that they will be able to recover the loss. The ACCC publishes the website to help consumers recognise and prevent scams.⁶⁰

MoneySmart

- 4.73 MoneySmart is hosted by the Australian Securities & Investments Commission (ASIC). MoneySmart provides, among other information, information on scams and bad value investments. The MoneySmart consumer website has a section dedicated to 'people over 55'.⁶¹
- 4.74 ASIC has a statutory mandate to promote the confident and informed participation of investors and consumers in the financial system (see next chapter for more about ASIC).
- 4.75 The information on the MoneySmart website can also be accessed for free by calling ASIC's 'infoline' number (1300 300 630). Infoline staff will assist people by talking through any general issues and will also post (free of charge) MoneySmart information if requested.⁶²

Suggestions for future cybersafety education and training

- 4.76 The Committee heard from various stakeholders about the key elements of effective cybersafety education. While each group's key elements are worded in different ways, basically they each have come to similar conclusions about cybersafety education for seniors.
- 4.77 Through its Connected Seniors program Telstra has identified that seniors have the following preferences for learning about cybersafety:
- they require programs that practically demonstrate the relevance of using the internet;
 - that training and demonstrations need to be kept simple and straightforward;
 - they prefer to be trained in smaller groups, with lots of opportunity to practice – and then return for more follow-up training;
 - they are concerned about cybersafety and consequently are reluctant to transact online; and

60 Australian Competition and Consumer Commission (ACCC), <www.scamwatch.gov.au/content/index.phtml/itemId/693900> viewed 5 February 2013.

61 ASIC, *Submission 46*, p. 3.

62 ASIC, *Submission 46*, p. 3.

- viruses and scams are an increasing concern.⁶³
- 4.78 ASCCA told the Committee that it has identified the four key elements for effective seniors' cybersafety education as:
- informing people but not by terrifying them;
 - funding community learning;
 - providing information at the point of purchase for computers;
 - making sure that learning is available without it having to be formal or obvious.⁶⁴
- 4.79 COTA NSW said the following three learning stages will help seniors to become cybersafe:
- a community awareness program to reduce fear and showcase benefits;
 - support provided to access computers and the internet; and
 - further education programs to increase knowledge and skill.⁶⁵
- 4.80 When seniors are first venturing into the cyber world, they need cybersafety training which starts right at the beginning. Ms Lambie said that many seniors who are not active online do not even know that they should have a password on their computer, or:
- ... those that do have a password do not know what a strong password is, are unaware that you should have different passwords and that you should change your passwords on a regular basis. ... Seniors who have never used a computer before do not know this and leave themselves exposed.⁶⁶
- 4.81 The South Australian Government noted that most cybersafety training is quite narrowly focussed on training seniors to be safe and secure on the internet for limited purposes such as general browsing and checking email, whereas broader training could encourage more seniors 'to use more complex online services, such as e-banking and potentially e-health'.⁶⁷
- 4.82 The Committee received many suggestions about additional cybersafety training and education needs, especially about the need for a 'one-stop shop' to be created between government and industry, 'where all Australians, including those of mature age can feel confident and

63 Telstra Corporation Ltd, *Submission 22.1*, p. 2.

64 ASCCA, *Submission 7*, p. 9.

65 COTA NSW, *Submission 39*, p. 6.

66 Ms Lambie, Stay In Touch Pty Ltd, *Submission 47*, p. 4.

67 South Australian Government, *Submission 37*, p. 2.

comfortable about both reporting cybercrime and asking questions related to Cybersafety'.⁶⁸

- 4.83 This 'Cybersafety Centre' would need both an online presence and a widely promoted telephone number:

...with phones manned by trained specialists sympathetic [to] and aware of the needs of older Australians. An exclusive use of methods of reporting which require internet expertise will miss significant sections of the target audience. Basic education and general advertising on cybersafety also needs to be provided through this centre.⁶⁹

- 4.84 The Centre for Internet Safety (CIS) said that an amalgamation of the cybersafety efforts of ACMA, DBCDE and the ACCC under one Office of Cyber Security would be a positive step for cybersafety education.⁷⁰

- 4.85 Legacy suggested that a dedicated phone number for seniors to use if they have cybersafety concerns is needed:

... a national Australian based telephone call centre to assist senior Australians understand the nature of the risks and threats in accessing information and communications technology would be of advantage.⁷¹

- 4.86 As mentioned above, in late November FaHSCIA launched its Broadband for Seniors website which includes a dedicated cybersafety telephone number which seniors can phone to ask any questions about cybersafety. It has been reported to the Committee that the helpline has been busy since its introduction, receiving at least 20 phone calls a day and the number of calls has been much higher on many days.⁷²

- 4.87 The Committee heard from many witnesses that more advertising on traditional media is needed to alert seniors to cybersafety awareness. Legacy said that government programs on cybersafety aimed at seniors are effective and informative for those seniors who have the confidence and knowledge to use the internet to access the information:

However, what is required is a clear broad-based campaign in both print media and national TV to inform senior Australians of

68 See, for example, YOURLifeChoices website, newsletters and magazine, *Submission 38*, p. 4; Legacy, *Submission 10*, p. 2.

69 YOURLifeChoices website, newsletters and magazine, *Submission 38*, p. 4.

70 Centre for Internet Safety (CIS), *Submission 26*, pp. 7-8.

71 Legacy, *Submission 10*, p. 2.

72 Pers. Comm. with Broadband for Seniors Helpline Operator, 13 February 2013.

both the advantages of internet use and the resources available to them and how best to use these resources to ensure cyber safety.⁷³

- 4.88 The National People with Disabilities and Carer Council emphasised the need to include older people with disability in future cyber education initiatives.⁷⁴
- 4.89 The Federation of Ethnic Communities' Councils of Australia said government must put in place clear strategies for digital literacy training and digital access opportunities for seniors from culturally and linguistically diverse backgrounds.⁷⁵
- 4.90 Telstra said that there is need for a coordinated public education campaign that will enable seniors to better identify the risks of undertaking online transactions.⁷⁶ A taskforce approach, according to Telstra, is needed to help drive a campaign of cybersafety education and awareness amongst seniors. This 'would be an essential element of any effective strategy to improve the nation's ability to manage cybersafety'.⁷⁷
- 4.91 Ms Catherine Walpole from the U3A (Hobart) said that while most training is aimed at people being online on personal computers, more and more people are online using iPads, tablets, smartphones and other devices and this should be reflected when designing training programs.⁷⁸
- 4.92 Ms Carol Bennet from the Consumers Health Forum of Australia suggested that in addition to providing education about scams, education should also include general guidance to seniors about how to consider the credibility of the information that seniors find online.⁷⁹
- 4.93 Ms Wright from ACMA believes 'people do not want a wealth of theoretical information. They want some helpful tools that ensure positive behaviour and good results'.⁸⁰
- 4.94 NSA recommended that a website designed specifically for older people, along the lines of ACMA's Cyber[smart] site, be created in tandem with a telephone hotline for those not yet confident in using web-based

73 Legacy, *Submission 10*, p. 2.

74 National People with Disabilities and Carer Council, *Submission 27*, p. 2.

75 Federation of Ethnic Communities' Councils of Australia, *Submission 40*, p. 3.

76 Telstra Corporation Ltd, *Submission 22*, p. 3.

77 Telstra Corporation Ltd, *Submission 22*, p. 3.

78 Ms Catherine Walpole, Database Officer, University of the Third Age, U3A (Hobart), *Committee Hansard*, 7 August 2012, p. 13.

79 Ms Carol Bennet, CEO, Consumers Health Forum of Australia, *Committee Hansard*, 19 September 2012, p. 1.

80 Ms Wright, ACMA, *Committee Hansard*, 23 March 2012, p. 37.

information.⁸¹ The Committee believes this recommendation has been satisfied by the introduction of the Broadband for Seniors website.

Recommendation 8

That the Australian Government advertise the Broadband for Seniors initiative widely, including:

- **launching a campaign publicising the internet kiosks using seniors clubs, magazines, newspapers, radio and television; and**
- **widely advertising the new cybersafety telephone helpline, including on all government websites which host cybersafety information.**

Research into appropriate cybersafety education

4.95 There has been a limited amount of research done by various bodies on how best to train seniors for cybersafety. Some departments and other bodies have conducted surveys about different aspects of being online, including questions relating to awareness of cybersafety.⁸²

4.96 Dr Rick Brown from the Australian Institute of Criminology (AIC) told the Committee that the AIC is committed to conducting high-quality research in relation to cybercrime:

Where cybersafety for senior Australians is concerned, the AIC recognises the need for research to ensure that prevention activities are suitably targeted to specific age groups. Prevention activities should also be rigorously evaluated in order to develop best practice, ensure resources are being used appropriately and determine that activities are meeting their intended goals. In addition, research that identifies the nature and extent of cybercrime can be used to inform resource allocation, compile intelligence, raise awareness and identify trends. To achieve this,

81 NSA, *Submission 29*, p. 2.

82 See for example: ACMA's *Australia's progress in the digital economy: Participation, trust and confidence*, <www.acma.gov.au/WEB/STANDARD/pc=PC_600063> viewed 11 February 2013.

the AIC has proposed in its submission to the committee a national cybersecurity monitoring program.⁸³

- 4.97 Dr Cross from the Queensland University of Technology conducted extensive research focused on the problem of online fraud victimisation, particularly as it relates to seniors, while she worked with the Queensland Police Service. As a result of her years of research on this topic, Dr Cross makes some clear suggestions about where the focus of cybersafety education should be. She believes that the focus of cybersafety education should be on how to avoid becoming a victim rather than on describing every possible scam. This is further discussed under 'Overseas cybersafety education initiatives' below.⁸⁴
- 4.98 A comprehensive report funded by the Department of Health and Ageing about rural seniors and technology was published recently by the Murray Mallee Aged Care Group and the University of Adelaide. Called 'Linking Rural Older People to Community through Technology', the project was a three year, five phase project, which included two pilot projects that utilised laptops and iPads to strengthen community connections for older people in the rural Murray Land regions of South Australia.⁸⁵ While this report is not about cybersafety *per se*, it has a lot of information about attitudes to technology, methods of learning and uses for new technology including social networking, specifically as these relate to seniors in rural areas.
- 4.99 ACMA told the Committee that there remains a need for a detailed exploration and identification of the online risks and threats to seniors including which, if any, specific groups of senior Australians may be particularly vulnerable. Such research would be an important element in developing successful cyber education campaigns aimed at senior Australians and critically, it would provide an understanding of how and where to target awareness and education initiatives for senior Australians.⁸⁶

83 Dr Rick Brown, Deputy Director (Research), Australian Institute of Criminology (AIC), *Committee Hansard*, 10 October 2012, p. 2.

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

85 Murray Mallee Aged Care Group Inc. and University of Adelaide, *Linking Rural Older People to Community through Technology*, August 2012, <www.murraymallee.org.au/pages/special-projects/linking-rural-older-people-to-community-through-technology.php> viewed 1 December 2012.

86 ACMA, *Submission 24*, p. 8.

Targeting cybersafety training appropriately

4.100 The Committee took a lot of evidence about the need to target cybersafety messages appropriately. The AHRC said that senior Australians who are not active online or who are hesitant about using the internet need targeted and effective opportunities to become confident internet users:

Access to computers and internet training is only the first part of ensuring cybersafety for older Australians. The second is to ensure that users are aware of potential cyber risks and can take action to maintain their security online. ... Evidence suggests that more targeted initiatives are required to engage segments of the aged population that do not respond to current programs.⁸⁷

4.101 Mr Michael O'Neill from NSA said that there is a lot of material produced for older Australians about cybersafety but the emphasis seems to be on large glossy booklets and publications. While these are useful, many seniors will not read such detailed publications but they would be likely to respond to brief, targeted simple messages about cybersafety.⁸⁸

4.102 Mr O'Neill went on to say that the bulk of material being published about cybersafety does 'not focus enough on vulnerable consumers' nor does it resonate with older people who have not grown up with the technology.⁸⁹

4.103 Evidence taken throughout the inquiry indicates there is a need for appropriately targeted cybersafety education programs for all seniors but particularly for vulnerable seniors, such as Aboriginal seniors, seniors from culturally and linguistically diverse backgrounds and seniors living in rural and remote areas.⁹⁰

Overseas cybersafety training initiatives

4.104 ACMA told the Committee that internet safety measures overseas to date have generally been targeted at the needs of children and adults with a comparatively limited number of cyber education initiatives targeted specifically at seniors – as has been the situation in Australia.⁹¹

87 AHRC, *Submission 2*, pp. 4, 8, 11.

88 Mr Michael O'Neill, CEO, NSA, *Committee Hansard*, 31 October 2012, p. 2.

89 Mr O'Neill, *Committee Hansard*, 31 October 2012, p. 4.

90 See for example: South Australian Government, *Submission 37*, pp. 3-4; and AFP, *Submission 20*, p. 5.

91 ACMA, *Submission 24*, p. 9.

4.105 A recent study commissioned by ACMA surveyed cybersecurity awareness-raising and educational initiatives in 11 international jurisdictions. None of the 68 international campaigns which were examined in the study focused solely on seniors and only eight campaigns (or 12 per cent) included information tailored for senior consumers. ACMA found a deliberate focus overseas by government and industry on the cybersafety needs of children, their families and schools.⁹² Key findings included:

- The dominant tools used in most campaigns were basic websites and publications. The proportion of campaigns employing interactive tools such as games and quizzes was quite low. The proportion of campaigns that included a reporting or counselling service was very low.
- Government organisations (either departments or regulators) were the dominant ‘host’ of the campaigns, although consortiums that included the private sector were also common. A smaller number of campaigns were hosted by the community sector.
- The topics covered in the campaigns were quite diverse – no single topic appeared in a majority of campaigns.⁹³

4.106 The Committee took evidence about cybersafety prevention messages in Canada where the focus is on ‘what [potential victims] do in that moment, when asked to send money or personal details’⁹⁴ rather than the traditional focus on the many ways in which fraud can occur, as is mostly the case in Australia:

Currently, our prevention messages around fraud and online security in general ... are primarily concerned with the large variety of ways in which a person can be approached. The problem with this method is that there are an infinite number of ways in which a potential victim can be targeted. Prevention messages and awareness campaigns will struggle to remain current and relevant, as criminals modify and refine their approach methods on a daily basis.⁹⁵

92 ACMA, *Submission 24*, p. 9.

93 *An Overview of International Cyber-Security Awareness Raising and Educational Initiatives. Research Report commissioned by the Australian Communications and Media Authority*, <www.acma.gov.au/webwr/_assets/main/lib310665/galexia_report-overview_intnl_cybersecurity_awareness.pdf> viewed 6 February 2013.

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

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

4.107 Dr Cross told the Committee that central to every online fraud is the transfer of money or the sending of personal information. What the potential victim does when asked to send money or personal details is crucial and the effectiveness of all prevention messages and awareness campaigns culminate in that moment. Therefore, it is how to act when requested to transfer money or send personal details that should be the focus of future prevention messages about online fraud.⁹⁶

The cost of training

4.108 There are two aspects to the cost of training which were presented to the Committee. One is that many seniors cannot afford to pay for cybersafety training and the second is that the public libraries and the many voluntary groups that teach cybersafety at no cost, are all constrained in what they can offer by their available funds.

4.109 The Committee heard that many seniors are likely to avoid spending any more than necessary if they seek out cybersafety training:

There is a clear need for [cybersafety training] and government has a role to ensure seniors are not excluded from [available training] simply because they cannot afford high-cost ... services.⁹⁷

4.110 During the course of the inquiry many voluntary providers of cybersafety training to seniors said that education delivered by voluntary groups costs money. Mrs Hocking told the Committee:

Education directed at such a large number of Australians requires money If government considers providing funds to allow the voluntary groups to expand, they are generally only looking at capital expenditure for the group as all tutors and committee members are volunteers. ... funds could be used to develop courses in cyber safety and related topics for Australian seniors.⁹⁸

4.111 The public and State libraries associations told the Committee that they are 'in a unique position to ... assist seniors with internet and cybersafety training' but although they are experiencing an ever-increasing demand for the help they offer seniors, they struggle to fund the services and are limited in what they can offer by the funds they have available.⁹⁹

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

97 LACVI, *Submission 5*, p. 4.

98 Mrs Hocking, *Submission 45*, p. 2.

99 ALIA and NSLA, *Submission 6*, p. 3.

4.112 ASCCA told the Committee that increased funding is also needed by community groups which teach computer literacy for daily living skills:

There is a considerable role for governments – particularly the Federal Government – to provide direct funding to community groups outside the vocational area for computer literacy for daily living skills. With all business and community sectors relying more heavily than ever on ICT for disseminating and seeking information, daily living skills, business transactions and even socialisation of those who are not computer literate will be severely affected.¹⁰⁰

4.113 BSOL strongly supports the ASCCA recommendation for the provision of funding to seniors' computer clubs. BSOL said that while seniors helping seniors is a most effective medium, most community groups struggle to provide up-to-date training facilities.¹⁰¹

4.114 The Committee notes that many seniors groups around the country are playing an important role in training seniors in cybersafety. Governments may wish to consider new and innovative measures to support the valuable work of these voluntary groups.

Recommendation 9

That the Australian Government work with the States and Territories to support public libraries or community resource centres where no public library exists, for the purpose of meeting the demand for cybersafety training for seniors.

Concluding comments

4.115 The Committee found that across the nation there are numerous community groups doing a heroic job teaching seniors how to be cybersafe. These groups are usually staffed by volunteers who are often seniors themselves. The courses help seniors to gain the necessary skills and to become confident enough to enjoy being active online.

¹⁰⁰ ASCCA, *Submission 7*, p. 8.

¹⁰¹ BSOL, *Submission 34*, p. 2.

- 4.116 Seniors' groups are also playing an important role keeping their members who are already active online up-to-date about cybersafety issues.
- 4.117 Public and State libraries around the nation are also doing an excellent job providing internet assistance and training for seniors across a range of technologies while providing both formal and informal cybersafety training.
- 4.118 Libraries and many of the volunteer groups which teach cybersafety as a part of computer classes demonstrated to the Committee their need for increased funding to allow them to continue the work they are doing and to meet the ever-increasing demand by seniors for cybersafety education.
- 4.119 The Committee recognises that various government departments, particularly DBCDE, are increasingly providing online cybersafety information for seniors and the Committee was pleased to see the launch of the FaHSCIA cybersafety telephone helpline for seniors because the need for a helpline service was spoken about by many stakeholders during the inquiry.
- 4.120 The Committee found that the free internet kiosks supported across Australia by FaHSCIA in community centres, retirement villages, ex-service organisations and various seniors clubs are providing a popular and valuable internet and cybersafety training service to seniors.
- 4.121 The last word about the value of educating seniors to be confident, cybersafe internet users goes to Mrs Bosler from the ASCCA:

Once a person can really start using the internet and feel confident in using it, the world opens up for them. It is really amazing.¹⁰²

102 *Committee Hansard*, 23 March 2012, p. 17.

Consumer protection, regulation and enforcement

Introduction

- 5.1 The Australian Government has recognised that digital technologies are now so embedded in daily life of Australians that they must be considered as a normal part of the activities of every community sector:¹

The internet has changed the world – there is no way to go back. A digital revolution is transforming every part of the economy and individuals, businesses and governments have no choice but to adapt or be left behind.²

- 5.2 Given the centrality of online interactions to the future prosperity of the Australian community and its economy, the Government is instigating legislative reform and developing new strategies to build community confidence in the online environment. Some of these measures specifically target senior Australians; others are aimed at fostering the broader health of the cyber environment.
- 5.3 This chapter outlines the responsibilities of the various government agencies in Australia's cybersafety consumer protection framework before

1 Australian Government, *Connecting with Confidence: Optimising Australia's Digital Future. A Public Discussion Paper*, Department of Prime Minister and Cabinet (PM&C), 2011, p. 6.

2 Department of Broadband, Communications and the Digital Economy (DBCDE), 'Boosting Australia's Productivity Performance through Broadband, Communications and the Digital Economy', [n.d], p. 1, <www.dbcde.gov.au/__data/assets/pdf_file/0011/156566/Productivity-measures-of-DBCDE.pdf> viewed 21 January 2012.

reviewing recent relevant legislative changes and evidence related to them.

- 5.4 The chapter also covers concerns raised in relation to the protection of personal information under eHealth, in particular the Personally Controlled Electronic Health Record (PCEHR), before canvassing some measures to improve seniors' awareness of cybersafety and help target government programs to protect consumers and contain cyber threats.

Australia's cybersafety framework

- 5.5 Australia's cybersafety framework is supported by key agencies responsible for developing, administering and enforcing our consumer protection framework. The fundamentals of this engagement were set out in May 2008, when the Australian Government committed \$125.8 million over four years to a comprehensive Cybersafety Plan.³
- 5.6 A whole-of-government initiative, the Cybersafety Plan aims to combat online risks and raise community awareness to those risks.⁴ The Plan is a continuation of the former Government's 'Protecting Australian Families Online' initiative implemented over 2007-08.⁵
- 5.7 A range of federal departments and agencies develop the policy and the regulatory architecture in support of the Cybersafety Plan. Others monitor and implement enforcement actions against cybercriminals. These agencies work with State and Territory partners to promote the cybersafety agenda.

Federal agencies

- 5.8 Key federal agencies involved in the delivery of Australia's cybersafety framework, with a brief description of their functions, are set out in alphabetical order below.

3 DBCDE, Cybersafety Plan < www.dbcde.gov.au/online_safety_and_security/cybersafety_plan > viewed 21 January 2012.

4 DBCDE, Cybersafety Plan < www.dbcde.gov.au/online_safety_and_security/cybersafety_plan > viewed 21 January 2012.

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

Attorney-General's Department

- 5.9 The Attorney-General's (A-G's) Department was formerly co-ordinator of the Government's whole-of-government cyber security policy. Responsibility for this moved to the Department of the Prime Minister and Cabinet (PM&C) from 14 December 2011.⁶
- 5.10 The Department now works to address cyber threats and vulnerabilities to Australia's telecommunication infrastructure through DBCDE, and with the NBN Co. on national security issues in the design and operation of the National Broadband Network (NBN).⁷
- 5.11 The Australian National Computer Emergency Response Team (CERT Australia) operates under the auspices of the A-G's Department. CERT Australia's primary responsibility is to inform the private sector about cyber security threats and vulnerabilities and to assist domestic and international CERT partners during cyber security incidents.⁸

Australian Competition and Consumer Commission

- 5.12 The Australian Competition and Consumer Commission (ACCC) is an independent Commonwealth statutory authority formed in 1995 to administer the *Trade Practices Act 1974*. Since 1 January 2011, the ACCC also administers the national Australian Consumer Law (ACL) under the *Competition and Consumer Act 2010*.⁹
- 5.13 The ACCC's primary responsibility is to administer the Commonwealth's competition, fair trading and consumer protection laws. It also promotes and safeguards competition and fair trade policy and regulates national infrastructure industries. As part of this brief, the ACCC's SCAMwatch website provides advice and registers consumer fraud complaints for both online and offline fraud. In February 2012 the ACCC issued its *Best*

6 Attorney-General's (A-Gs) Department, 'Chapter 2: 2011-2012 Snapshot', *Annual Report 2011-2012* <www.ag.gov.au/Publications/AnnualReports/AnnualReport201112/Pages/default.aspx> viewed 21 December 2012.

7 A-G's Department, 'Chapter 2: 2011-2012 Snapshot', *Annual Report 2011-2012*, viewed 21 December 2012.

8 CERT Australia website <www.ag.gov.au/RightsAndProtections/CERT/Pages/default.aspx> viewed 13 February 2013.

9 The Australian Consumer Law (ACL) replaced previous Commonwealth, state and territory consumer protection legislation. See SCAMwatch, 'About the ACCC' <www.scamwatch.gov.au/content/index.phtml/itemId/694363> viewed January, 2013.

Practice Guidelines for Online Dating to provide guidance to the convenors of romance and dating websites and to their clients.¹⁰

- 5.14 The ACCC also works with State and Territory fair trading agencies and other government agencies to promote general awareness in the community about scams. In 2005 the ACCC and these other agencies formed the Australasian Consumer Fraud Taskforce (ACFT) to co-ordinate this work.

Australian Communications and Media Authority

- 5.15 The Australian Communications and Media Authority (ACMA) is the federal agency responsible for the regulation of broadcasting, the internet, radio communications and telecommunications.¹¹
- 5.16 ACMA researches cyber issues and delivers cyber-related education programs under the remit of the Online Content Scheme (OCS), established under the *Broadcasting Services Act 1992*, as well as reporting on matters affecting consumers or proposed consumers of carriage services under the ACMA Act 2005.¹² Under the OSC, the ACMA also receives and investigates complaints about prohibited online content and facilitates a co-regulatory approach with the internet industry by developing and enforcing industry codes of practice.¹³
- 5.17 The Authority's educational services include the Cybersmart website, the interactive shared learning schools programs offered at schools, Internet Safety Awareness presentations, DVDs and brochures. ACMA's research into online services use led to the Digital Media Literacy Research program.¹⁴

Australian Federal Police

- 5.18 The Australian Federal Police (AFP) has a commitment to preventing online crime, considering that: 'Cyber-safety requires a multi-faceted

10 See Australian Competition and Consumer Commission (ACCC) <www.accc.gov.au/content/index.phtml/tag/DatingSiteGuidelines/> viewed January, 2013.

11 Australian Communications and Media Authority (ACMA) website <www.acma.gov.au/WEB/STANDARD/pc=ACMA_ROLE_OVIEW> viewed 13 February 2013.

12 Section 8 (d). *Broadcasting Services Act 1992*, Section 94 Schedule 5 in ACMA Digital Economy Series, <www.acma.gov.au/WEB/STANDARD/pc=PC_311655> viewed 13 February 2013.

13 ACMA, *Submission 24*, p. 2.

14 ACMA, *Submission 24*, p. 2, and see Appendix A for ACMA's outreach programs.

approach; law enforcement; policy and legislation; education and some level of user vigilance'.¹⁵

- 5.19 The AFP works in partnership with the A-G's Department and other agencies to 'evolve effective law, policy and practices to address cybercrime threats to Australia's domestic and national security'. Its High Tech Crime Operations unit identifies emerging technology challenges for law enforcement and works to address these with domestic and foreign law enforcement agencies, governments, industry and academic partners.
- 5.20 The AFP has a strategic alliance with the Australian and New Zealand Policy Advisory Agency, works globally through the International Liaison Officer Network and also partners with State and Territory counterparts to combat cybercrime.
- 5.21 The AFP regards consumer education as important to prevent online crime. It has partnered with the Australian Seniors Computer Clubs Association (ASCCA) to deliver sessions to seniors on how they can protect their personal and financial information, secure online banking and wireless connections.¹⁶

Australian Securities and Investments Commission

- 5.22 The Australian Securities and Investments Commission (ASIC) has a statutory mandate to promote the confident and informed participation of investors and consumers in the financial system.¹⁷
- 5.23 As such, ASIC has a consumer protection role at a Federal level in relation to financial products and services. ASIC's regulatory role covers financial services, disclosure requirements on financial products, enforcement on misleading or deceptive conduct cases, as well as the licensing and monitoring of licensed financial services providers.
- 5.24 ASIC also advances the National Financial Literacy Strategy and on its MoneySmart Consumer website. Senior Australians are represented on its Consumer Advisory Panel which informs and directs ASIC's consumer research and education projects.

15 Information in this section from Australian Federal Police (AFP), *Submission 20*, pp. 1, 5 and 8.

16 See also Commander Glen McEwen, Manager, Cyber Crime Operations, and Dr Jenny Cartwright, Co-ordinator, Strategic Initiatives, AFP, *Committee Hansard*, 13 March 2013, pp. 1-2.

17 Section 1 (2)(b) ASIC Act 2001, see Australian Securities and Investments Commission (ASIC), *Submission 46*, p. 1.

- 5.25 The Commission is a member of the ACFT and also participates in Taskforce Galilee, the multi-agency, multi-jurisdiction taskforce, which works to address serious and organised investment frauds (SOIF).¹⁸

Australian Taxation Office

- 5.26 As Australia's collector of tax revenue, the Australian Taxation Office (ATO) has extensive interaction with the community which, for the most part, readily complies with ATO requests. This level of compliance attracts cyber criminals who exploit the tax office brand to legitimate a range of scam activities such as 'phishing' scams.¹⁹
- 5.27 The ATO provides a 24 hour/seven day a week Security Incident Response (SIR) service with reporting, response and monitoring capability. The Security Analysis Toolkit (SAT), which manages and processes information and data, assists the SIR to identify anomalous activity, such as bogus websites purporting to be the ATO.
- 5.28 The ATO's Vulnerability Management and Research (VMR) team refers advice to CERT Australia to initiate take-downs of scam sites. In incidents of identity theft, such as compromised use of a tax file number, the ATO follows up by contacting individuals, or a tax agent intermediary. Future abuse is prevented by reissuing a new tax file number and transferring all data.²⁰
- 5.29 The ATO also maintains a developed community awareness and education campaign to alert people to evolving risks using media releases, website, TV interviews and seminars. Consumer awareness material is also translated into multiple languages.²¹

Commonwealth Director of Public Prosecutions

- 5.30 The Commonwealth Director of Public Prosecutions (CDPP) was established as an independent prosecuting agency under the *Director of Public Prosecutions Act 1983* (DPP Act) and began operations in 1984.²²
- 5.31 The CDPP is responsible for prosecution of criminal offences against the laws of the Commonwealth, and conducts confiscation of the proceeds of
-

18 See ASIC, *Submission 46*, pp. 3-4.

19 Information in this section largely drawn from ATO, *Submission 43*, pp. 1-3.

20 ATO, *Submission 43*, pp. 1-2; Mr Bill Gibson, Chief Information Officer, *Committee Hansard*, 18 May 2012, pp. 25-26.

21 Mr Gibson, *Committee Hansard*, 18 May 2012, pp. 24, 26.

22 Commonwealth Director of Public Prosecutions (CDPP), <www.cdpp.gov.au/> viewed 13 February 2013.

crimes committed against the Commonwealth. The CDPP is within the portfolio of the Commonwealth A-G, but operates independently. State and Territory Directors of Public Prosecutions are responsible for the prosecution of alleged offences against State and Territory laws.²³

Department of Broadband, Communications and the Digital Economy

- 5.32 As discussed in Chapter 4, the Department of Broadband, Communications and the Digital Economy (DBCDE) has charge of the consumer education and awareness programs for the Government's Cybersafety plan. The Department's mandate is to improve awareness of cybersafety and cyber security risks among individuals and small and medium businesses in support of the Government's National Digital Economy strategy, as facilitated by the NBN at Digital Hubs.²⁴
- 5.33 Another key mechanism carried by the DBCDE to improve the level of cybersafety awareness in the community is the cybersafety Stay Smart Online website which has links to the Cybersafety Help Button and the ACCC's SCAMwatch site.²⁵
- 5.34 In October 2012, DBCDE also took over joint responsibility for a rebranded Cyber White Paper with the Department of Prime Minister and Cabinet.²⁶

Department of Families, Community Service, Housing and Indigenous Affairs

- 5.35 The Department of Families, Community Service, Housing and Indigenous Affairs (FaHCSIA) hosts the Broadband for Seniors initiative, the Government's main computer support program for senior Australians. The initiative provides free access to computers and the internet, as well as training in basic computing skills.²⁷
- 5.36 The Australian Government committed \$25.4 million to Broadband for Seniors over seven years to 2015, which involves establishing 2 000 internet kiosks in community centres, libraries, retirement villages and clubs. The initiative is delivered by NEC Australia Pty Ltd in partnership with Adult Learning Australia, the Australian Senior Computer Clubs

23 Information in this section from Commonwealth Director of Public Prosecutions (CDPP) website <www.cdpp.gov.au/> viewed 13 February 2013.

24 Department of Broadband, Communications and the Digital Economy (DBCDE), *Submission 25*, p. 2.

25 DBCDE, *Submission 25*, p. 9, and see StaySmartOnline, <www.staysmartonline.gov.au/> viewed 15 February 2013.

26 See section on PM&C below.

27 For this section, see DBCDE, *Submission 25*, p. 12 and see *Broadband for Seniors* <www.necseniors.net.au/about-bfs/> viewed 15 February 2013.

Association (ASCCA) and University of the Third Age Online.²⁸ Further details are in Chapter 4.

Department of Prime Minister and Cabinet

- 5.37 As already mentioned, responsibility for whole-of-government cyber security policy co-ordination was transferred from the A-G's Department to the Department of PM&C in late 2011.
- 5.38 Responsibility for the strategic leadership and co-ordination of cyber policy, including cyber security policy within PM&C is carried by the National Security and International Policy Group (NSIPC) and led by the Cyber Policy Co-ordinator.
- 5.39 In June 2011, the Government announced that the NSIPC would prepare the Cyber White Paper, a whole-of-government cyber security strategy. The strategy would build on the Government's 2008 Cybersafety Plan and its 2009 Cyber Security Strategy, and the establishment of the Cyber Security Operations Centre (CSOC), CERT Australia, and the Digital Economy Strategy.²⁹
- 5.40 A discussion paper *Connecting with Confidence: Optimising Australia's Digital Future* was launched for public comment in the second half of 2011, with the expectation that the Cyber White Paper would be released by mid-2012.³⁰ However, in October 2012, the Prime Minister suggested that the Cyber White paper should focus on the digital economy to cover the opportunities of cloud technology.³¹
- 5.41 The PM&C later advised that the new Digital Economy White Paper will be written by an inter-departmental taskforce, comprising staff from the PM&C and the DBCDE, with DBCDE as the lead agency. The taskforce would also draw on relevant expertise from other agencies.³²

28 Broadband for Seniors < www.necseniors.net.au/about-bfs/ > viewed 15 February 2013.

29 Former A-G, the Hon. Robert McClelland MP, former Minister for Defence the Hon. Stephen Smith MP, and the Hon. Senator Stephen Conroy Minister for Broadband, Communications and the Digital Economy, Cyber White Paper, *Media Release*, 3 June 2011 <www.minister.dbcde.gov.au/media/media_releases/2011/198> viewed 15 February 2013.

30 Australian Government, *Connecting with Confidence: Optimising Australia's Digital Future. A Public Discussion Paper*, PM&C, 2011, p. 5.

31 Prime Minister, the Hon. Julia Gillard, MP, 'Closing Remarks of the Digital Economy Forum' Sydney 5 October 2012 <[//www.pm.gov.au/press-office/closing-remarks-digital-economy-forum](http://www.pm.gov.au/press-office/closing-remarks-digital-economy-forum)> viewed 15 February 2013.

32 That is: the Treasury; A-G's Department; the Department of Education, Employment and Workplace Relations; the Department of Regional Australia, Local Government, Arts and Sport; and the Department of Industry, Innovation, Science, Research and Tertiary Education, see *Answers to Questions on Notice*, no. 34, Additional Estimates, Senate Finance and Public

State and Territory consumer protection activities

- 5.42 As noted above, on 1 January 2011 the commencement of the Commonwealth *Competition and Consumer Act 2010* introduced a single national Australian Consumer Law (ACL). The ACL replaced provisions set out in 20 existing national, State and Territory laws with a single national consumer law, creating a national enforcement regime with consistent enforcement powers for Australia's consumer protection agencies.³³
- 5.43 State and Territory consumer protection agencies jointly regulate the law with the ACCC and ASIC.³⁴ At hearings, Directors of the Centre for Internet Safety (CIS) identified the Western Australia (WA) Government and Queensland Police Service's Fraud and Corporate Crime Group as national leaders in consumer awareness and protection activities.³⁵
- 5.44 The CIS referred for example to the WA Department of Commerce's promotion on Youtube of actual victim accounts of being scammed by mortgage schemes.³⁶ This work fits within the WA Government's work on reducing the 'shame' of being a victim to promote awareness and reporting.³⁷
- 5.45 Dr Cassandra Cross, Lecturer at Law at the Queensland University of Technology, detailed her extensive research sponsored by the Queensland Police and under a Churchill Fellowship in the United Kingdom (UK), Canada and the United States (US). This work informed the work of the Queensland Police leading to a web-based training package for seniors, implemented in Australia and New Zealand, and recommendations for review of national cybercrime awareness campaigns to target high risk behaviours online.³⁸
- 5.46 The Committee also heard from the South Australian Government which outlined initiatives undertaken by the Consumer and Business Division of the State's A-G's Department. These included the Department's 'Scam

Administration Legislation Committee, Supplementary Budget Estimates 15–18 October 2012.

33 The Australian Consumer law <www.consumerlaw.gov.au/content/Content.aspx?doc=the_acl.htm> viewed 13 February 2013.

34 The ACL replaced previous Commonwealth, state and territory consumer protection legislation. See SCAMwatch, 'About the ACCC', <www.scamwatch.gov.au/content/index.phtml/itemId/694363> viewed January, 2013.

35 Professor Nigel Phair and Mr Alastair McGibbon, Co-Directors, Centre for Internet Safety (CIS), *Committee Hansard*, 14 March 2012, p. 11.

36 Mr McGibbon, *Committee Hansard*, 14 March 2012, p. 11.

37 Western Australia (WA) Government, *Submission 19*, p. 6.

38 See *Submission 49, passim*, and Dr Cross, *Committee Hansard*, 6 February 2013, pp. 7–10.

Alert' page, somewhat similar to the ACCC's SCAMwatch, and the *Savvy Seniors* guide which provides consumer rights advice and practical cybersafety tips in an easy to read format.³⁹

Updating the law

- 5.47 Regulation of cybercrime in Australia is largely the preserve of the State and Territory jurisdictions, which carry substantive criminal offences for many forms of computer crime. Commonwealth law also contains a growing body of legislation relating to computer technology, in particular, telecommunications systems. These laws operate along with general criminal laws which affect cybercrime, including those for intellectual property rights, classification of publications, terrorism and national security.⁴⁰
- 5.48 In addition to the introduction of national consumer protection law, recent amendments to the *Crimes Act 1914* have given specific powers to the Commonwealth for the examination and seizure of computers. Cybercrime may also be investigated under the Commonwealth *Telecommunications (Interception and Access) Act 1979*, and controlled by undercover operations under the *Crimes Act 1914*.⁴¹
- 5.49 In late 2012, the Parliament enacted a number of important new amendments to national legislation to better co-ordinate international efforts to regulate and enforce against cybercrime and to protect personal data. These include:
- the *Cybercrime Legislation Amendment Act 2012*, to implement laws for Australia's accession to the *Council of Europe's Convention on Cybercrime*;
 - the *Privacy Amendment (Financing Privacy Protection) Act 2012*, to provide for a new set of Australia Privacy Principles (AAPs) applying to both the public and private sector; and
 - the *Crimes Legislation Amendment (Serious Drugs, Identity Crime and Other Measures) Act 2012* which, among other things, imposes new penalties for identity theft using a mobile phone and the internet for criminal purposes.

39 South Australian (SA) Government, *Submission 37*, pp. 5–8.

40 Australian Institute of Criminology (AIC), G Urbas and K-K R Choo, 'Resource Materials on Technology-enabled Crime', *Technical and Background Paper No. 28*, 2008, p. 25.

41 AFP, *Submission 20*, pp. 7–8.

International co-operation and law enforcement

- 5.50 The Cybercrime Legislation Amendment Bill 2011 amended the *Mutual Assistance in Criminal Matters Act 1987*, the *Criminal Code Act 1995* and telecommunications law to implement the *Council of Europe's Convention on Cybercrime*. The Bill passed into law on 12 September 2012 as the *Cybercrime Legislation Amendment Act 2012*.⁴²
- 5.51 The *Council of Europe's Convention on Cybercrime* is the first international treaty seeking to address cybercrime by harmonising national laws, improving investigative techniques and increasing co-operation among nations. It contains procedures to make investigations more efficient and provides systems to facilitate international co-operation, including by:
- helping authorities from one country to collect data in another country
 - empowering authorities to request the disclosure of specific computer data
 - allowing authorities to collect or record traffic data in real-time
 - establishing a 24/7 network to provide immediate help to investigators
 - facilitating extradition and the exchange of information.⁴³
- 5.52 The Convention also contains a series of powers and procedures relating to accessing important evidence of cybercrimes, including by way of mutual assistance.⁴⁴
- 5.53 Reforms to telecommunications legislation in support of the Convention have been controversial, in particular in relation to the accessing and retention of personal data.⁴⁵ These concerns were foreshadowed in the Committee's *Review of the Cybercrime Legislation Bill 2011*, tabled in August 2011.⁴⁶

42 The *Telecommunications (Interception and Access) Act 1979* and the *Telecommunications Act 1997*. See *Comlaw*, Act No. 120, 2012.

43 Cited AFP, *Submission 20*, p. 7.

44 Cited AFP, *Submission 20*, p. 7.

45 See for example, *National Times*, Editorial, 'Long Memories May Haunt Us All in Hunt for Cyber Criminals' 12 February 2013, <www.smh.com.au/opinion/editorial/long-memories-may-haunt-us-all-in-hunt-for-cyber-criminals-20130211-2e8w5.html#ixzz2KIUGrMG8> viewed 13 February 2013.

46 See also Joint Standing Committee on Treaties (JSCOT) review of Australia's proposed ratification of the Convention on Cybercrime, *JSCOT Report 116*, pp. 86-92.

Protection of personal information

- 5.54 The *Privacy Amendment (Enhancing Privacy Protection) Act 2012* amends the *Privacy Act 1988* to implement the Government's first stage response to the Australian Law Reform Commission's (ALRC) 2008 report *For Your Information: Australian Privacy Law and Practice*.⁴⁷ The legislation was made into law on 12 December 2012 and will be fully implemented by 14 March 2014.⁴⁸
- 5.55 The new amendments introduce major modifications to the Privacy Act to regulate how both public and private sector organisations collect, use and disclose personal information, including to:
- create the Australian Privacy Principles (APPs), a single set of privacy principles applying to both Commonwealth agencies and private sector organisations
 - re-write the credit reporting provisions and introduce more comprehensive credit reporting
 - introduce new provisions on privacy codes and the credit reporting code and
 - clarify and strengthen the functions and powers of the Privacy Commissioner.⁴⁹
- 5.56 The APPs, which deal with the collection, storage, security, use, disclosure access and collection of personal information, will put in place stricter rules about transferal of such data overseas. These encourage Australian companies to require overseas recipients not to breach the principles. The APPs will also require a higher standard of protection for sensitive information such as health data.⁵⁰
- 5.57 As noted the Bill is the first part of the Government's response to the ALRC's report, which contained 295 recommendations to improve privacy

47 House of Representatives, *Privacy Amendment (Enhancing Privacy Protection) Bill 2012, Explanatory Memorandum*, 2012, and see Australian Law Reform Commission's (ALRC) 'For Your Information: Australian Privacy Law and Practice', *ALRC Report Number 108*, August 2008.

48 See Comlaw, Act 167, 2012.

49 The Bill also makes consequential amendments to 55 Acts. See Bills Summary, Bills Lists, Privacy Amendment (Enhancing Privacy Protection) Bill 2012 and Australian Parliamentary Library Information Service, 'Privacy Amendment (Enhancing Privacy Protection) Bill 2012,' *Bills Digest no. 20, 2012-13*, 7 November 2012, p. 1.

50 The Hon. Nicola Roxon MP, (former) Attorney-General, Second Reading Speech, *House Hansard*, 23 May 2012, p. 5210.

protection in Australia. One of these recommended the introduction of a data breach notification scheme, which was not addressed in the bill.⁵¹

- 5.58 Amendments introduced under the *Crimes Legislation Amendment (Serious Drugs, Identity Crime and Other Measures) Act 2012* propose to close various gaps in the operation of specific Commonwealth offences under the *Criminal Code Act 1995* (Criminal Code).⁵²
- 5.59 Under identity crime reforms, the Act expands the scope of existing identity crime offences as well as enacting new offences for the use of a carriage service, such as mobile phone or by the internet, with the purpose of obtaining personal information to commit another offence. The legislation also criminalises the use of identity information with intent to commit a foreign offence. The Act provides for a penalty of five years imprisonment.⁵³
- 5.60 This legislation responds to the Government's National Identity Security Strategy (NISS), an agreement between Australian governments ratified in 2007. The NISS was reviewed in 2012, to ensure the Commonwealth can better respond to the impact of digital transactions using a mobile or the internet for identity documentation between the public and private sector.⁵⁴ The Act passed into law on 28 November 2012.⁵⁵

Support for enhanced protections

- 5.61 Consumer awareness is important for the cybersafety of individuals and businesses. There was also recognition that more must be done to ensure cybercrime activities are disrupted. The ACC advised:

The overarching solution for attacking cybercrime needs a framework that is similar to that of the public health care system,

51 Australian Parliamentary Library Information Service, 'Privacy Amendment (Enhancing Privacy Protection) Bill 2012', *Bills Digest no. 20, 2012-13*, 7 November 2012, pp. 6-7, 55.

52 The Bill amends the *Australian Federal Police Act 1979*, *Crimes Act 1914*, *Crimes (Superannuation Benefits) Act 1989*, *Criminal Code Act 1995*, *Customs Act 1901*, and *Law Enforcement Integrity Commissioner Act 2006*, see *Crimes Legislation Amendment (Serious Drugs, Identity Crime and Other Measures) Bill 2012, Explanatory Memorandum*, p. 1; and Australian Parliamentary Library Research Service, *Bills Digest no. 46, 1012-13*, 19 November 2012.

53 See *Crimes Legislation Amendment (Serious Drugs, Identity Crime and Other Measures) Bill 2012, Explanatory Memorandum*, p. 1, and the Hon. Nicola Roxon MP, (former) Attorney-General, Second Reading Speech, *House Hansard*, 10 October 2012, p. 11764.

54 Council of Australian Governments (COAG), *Report to COAG - Review of the National Identity Security Strategy 2012* <www.coag.gov.au/node/480> viewed 23 February 2013.

55 See *Comlaw*, Act 197, 2012.

as it is a complex issue requiring a co-ordinated multi-dimensional approach.⁵⁶

- 5.62 This includes having a flexible but robust framework of law which encourages compliance with cyber security requirements, and promotes sharing of information between government agencies on a national and on a global basis.

Cross-jurisdictional collaboration

- 5.63 Cybercrime crosses multiple jurisdictions and imposes challenges for regulators and enforcers which have been investigated in great depth in other reports.⁵⁷ In the context of this inquiry, the Committee has noted that Australia's move to ratify the *Convention on Cybercrime* has highlighted some weakness in current protections for cybercrime victims, and hence senior Australians who are disproportionately affected.
- 5.64 Commenting on the regulatory amendments to support Australia's accession to the Cybercrime Convention, the AFP and CIS commended changes to the *Mutual Assistance in Criminal Matters Act 1987* (MACMA), which will support information sharing between Australian and foreign law enforcement agencies. Both organisations remarked the cumbersome nature of former arrangements, which were not suited to the online environment.⁵⁸
- 5.65 The Committee also heard that the 'borderless' nature of crimes facilitated by the internet creates significant challenges for regulators and enforcers.
- 5.66 The ACC observed that cybercrime organisations may not commit crimes in their location country, even while having heavy impacts in other jurisdictions. Even where Australian law enforcers work successfully with partners offshore, victims of these crimes have no tangible redress. In illustration of this, the ACC advised that no funds sent overseas to scammers have been recovered, despite the enormous losses recorded.⁵⁹
- 5.67 The AIC explained that small value high volume frauds are harder for law enforcers to investigate, with smaller proceeds easier to launder across a number of jurisdictions.⁶⁰ The CIS, however, argued that the Government

56 ACC, *Submission 9*, p. 7.

57 See in particular, the (former) House of Representatives Committee on Communications report, *Hackers, Fraudsters and Botnets: Tackling the Problem of Cyber Crime*, June 2010.

58 AFP, *Submission 20*, p. 7; Mr MacGibbon, CIS, *Committee Hansard*, 14 March 2012, pp. 7-8.

59 Mrs Harfield, ACC, *Committee Hansard*, 15 August 2012, p. 6.

60 Dr Rick Brown, Deputy Director (Research), AIC, *Committee Hansard*, 10 October 2012, pp. 1-2.

should deploy Australia's strong extraterritorial powers in terms of search warrants for cybercrime, as used for international drug transactions.⁶¹

- 5.68 The Directors of CIS referred, by example, to successes over the last ten years in closing down Pacific 'safe havens', and identified a need to undertake cyber security capacity building in developing IT hot spots, such as the Pacific Islands and South East Asia.⁶²
- 5.69 Asked about this at hearings, AFP representatives advised that the AFP currently delivers enforcer awareness training in the Pacific region under its Cyber Safety Pacifica program. The AFP also has an extensive International Liaison Officer network, operating in over 30 countries, with 100 officers active offshore.⁶³ Commander Glen McEwen reported in particular on the recent successes of Operation Lino, where the AFP, international, and State and Territory law enforcers disrupted a major foreign data theft network targeting Australia from Romania.⁶⁴
- 5.70 Another suggestion was that government should be more proactive in strengthening regulations and enforcing existing domestic laws and requirements to protect consumers. For example, foreign-based companies providing online services in Australia should be obliged to comply with domestic obligations, and ISPs, banks and money transfer agencies could monitor for scamming and other activities.⁶⁵
- 5.71 Dr Cross referred to a further impediment for cybercrime victims in Australia, the limited opportunity for legal or financial restitution offered for frauds under domestic laws:⁶⁶
- Victims of online fraud are excluded from all current victim initiatives within the criminal justice system, based solely on the type of offence which has been perpetrated against them. This directly contravenes many of the fundamental principles of justice which are argued to exist for victims of crime in Queensland.⁶⁷
- 5.72 The AIC confirmed that, at a federal level, there is only voluntary reporting to the Privacy Commissioner or Ombudsman of fraud cases, and no requirement to report criminal offences except in some specific cases.

61 Mr MacGibbon, CIS, *Committee Hansard*, 14 March 2012, p. 7.

62 Professor Phair and Mr MacGibbon, CIS, *Committee Hansard*, 14 March 2012, p. 12.

63 Dr Cartwright and Commander McEwen, AFP, *Committee Hansard*, 13 March 2013, pp. 7, 5.

64 *Committee Hansard*, 13 March 2013, p. 4.

65 Professor Phair and Mr MacGibbon, CIS, *Committee Hansard*, 14 March 2012, pp. 7-8, 12.

66 Dr Cross, *Submission 49*, p. 9.

67 Dr Cross, *Submission 49*, p. 9.

As a consequence, reporting on fraud, including cyber-based fraud, is relatively low.⁶⁸

- 5.73 The AFP, however, reported positively on recent reforms to the Commonwealth Criminal Code, which afforded extensive powers to enforcers to address cybercrime.⁶⁹

Mandatory reporting of data breaches

- 5.74 An area of strong agreement among cybercrime experts was the need for domestic legislation to require organisations to report and contain data breaches. There was, however, also recognition that this proposal raises questions about the market sensitivity of information, and related practical enforcement issues.
- 5.75 One of the recommendations made by the Australian Law Reform Commission's review of the operation of the *Privacy Act 1988* was for the introduction of a mandatory data breach notification scheme, to impose a legal requirement on entities to notify a victim and the relevant regulator about any breaches of personal information. In October 2012 the Government released a discussion paper on the proposal for privacy breach notification for public commentary by 23 November 2012.⁷⁰
- 5.76 Submitters referred to data indicating the disparity between the very high level of losses and the low reportage of data breaches. Abacus-Australian Mutuals, for example, cited 2008 AIC research indicating that Australian small and medium businesses (SMEs) had estimated the cost of computer security incidents to their business at around \$600 million, but only eight per cent of affected businesses had reported these breaches.⁷¹ Other research indicated that 73 per cent of SMEs had experienced at least one data breach in 2010.⁷²
- 5.77 The AIC confirmed that there are no current requirements for data breaches to be reported, being voluntary as for other crime reportage. The AIC representatives referred to the massive financial impacts on business

68 AIC, *Submission 12*, p. 3.

69 Commander McEwen, *Committee Hansard*, 13 March 2013, p. 3.

70 Australian Government, *Discussion Paper: Australian Privacy Breach Notification*, Commonwealth A-G's Department, October 2012.

71 K Richards, 'The Australian Business Assessment of Computer User Security (ABACUS): a National Survey', *Australian Institute of Criminology Research and Public Policy Series no. 102*, June 2009, Forward. Data ref. in Abacus Australian Mutual, *Submission 44*, p. 1.

72 Ponemon Institute LLC, *2010 Annual Study: Australian Costs of Data Breach*, 2010, cited in eBay and PayPal, *Submission 11*, p. [2].

of data theft and also the effects of accidental data loss on victims. Given the scale of current losses, and the potential market disincentives to report them, the AIC recommended a mandatory scheme.⁷³

- 5.78 The CIS agreed that market disincentives to reportage require corrective action, advocating a ‘carrot-and-stick’ approach incorporating mandatory data breach notification:⁷⁴

Our economy would be healthier if consumer confidence was based on a more transparent knowledge of the threat environment and of the security incidents that occur.⁷⁵

- 5.79 Industry respondents maintained that market forces do compel attention to data protection but also acknowledged that the level of compliance is patchy. The eBay and PayPal supported mandatory measures but emphasised they must not be a ‘one size fits all’ module, which may stifle small business, noting:

...the delivery of breach notifications must be consistent with the way each organisation regularly communicates, and notification needs to be actionable.⁷⁶

- 5.80 The Australian Information Security Association (AISA), a peak body for information security professionals, reported that security of information is currently a low budget priority in most industries and asked for regulations like those for the Paycard industry in the US. AISA also recommended that ‘any data breach notification scheme be part of a broader and “more responsive” regulatory approach supporting information security’.⁷⁷
- 5.81 The Committee discusses other obligations and supports for industry’s increased security awareness in Chapter 6.

Secure government information systems — PCEHR

- 5.82 The anticipated release of the Government’s PCEHR system in July 2012 brought into focus fears about personal privacy and information security

73 Dr Brown, Ms Alice Hutchings, Senior Research Analyst, Global, Economic and Electronic Crime (GEEC) Program, and Dr Russell Smith, Principal Criminologist and Manager, CEEC Program, AIC, *Committee Hansard*, 10 October 2012, pp. 3–4.

74 Mr MacGibbon and Professor Phair, *Committee Hansard*, 14 March 2012, pp. 1–2; 10.

75 CIS, *Submission 26*, pp. 6–7.

76 eBay and PayPal, *Submission 11*, p. [3].

77 AISA, *Submission 32*, p. 8.

posed by centralised government databases. National Seniors Australia (NSA) told the Committee:

Privacy and security are 'make or break' issues for older Australians in relation to PCEHR. [It] will only be able to deliver the anticipated benefits for patients, healthcare providers and the healthcare system if all parties have a high level of trust and confidence in the entire system.⁷⁸

5.83 Protections provided under the PCEHR legislation and amendments to the Privacy Act to support the system include:

- the ability for a consumer to control which healthcare provider organisations can access their information;
- closely defined limits on the reasons that information can be accessed outside of those controls;
- the ability to view an audit trail of all access to a consumer's PCEHR;
- penalties and other sanctions for unauthorised viewing of and access to records; and
- requirements to report data breaches.⁷⁹

5.84 The Department of Health and Ageing (DoHA) manages cyber risks under the PCEHR, along with Government funded tele-health initiatives including those under the NBN.⁸⁰ The National E-Health Transition Authority (NEHTA) is DoHA's managing agent for the design and contract management for the PCEHR.⁸¹

Concerns about personal privacy—the audit trail

5.85 DoHA's submission advised that 'the design of the PCEHR system, and the legal framework provided by the proposed legislation, enables security and privacy breaches to be detected and prosecuted.'⁸²

5.86 However, during the inquiry concerns were expressed about the privacy and security of senior Australians, given their relatively limited computer skills, and possible health or mental incapacity. In particular:

- Seniors, although a priority client group, maybe exposed to online risks due to unduly complex interfaces and have private data hacked.⁸³

78 NSA, *Submission 29*, p. 2.

79 DoHA, *Submission 16*, p. 3.

80 DoHA, *Submission 16*, p. 3.

81 Mr Paul Madden, Chief Information and Knowledge Officer, DoHA, *Committee Hansard*, 21 March 2012, p. 4.

82 DoHA, *Submission 16*, p. 3.

- A robust and independent complaints mechanism is required and an independent review function, such as by the Office of the Australian Information Commissioner (OAIC), should be funded.⁸⁴
 - The audit trail for PCEHR records should provide consumers with genuine privacy controls, information on all individual health practitioners who have accessed their records and notification of all PCEHR system breaches affecting their record.⁸⁵
 - There is potential for abuse under 'nominated authority' arrangements, but there is also the need to ensure access by carers, and to allow for the risk a client will pass away without sharing security passwords with spouses or family.⁸⁶
- 5.87 Departmental responses resolved a number of concerns about review mechanisms, and the internal probity and security of the PCEHR interface, which, NEHTA told the Committee, had attracted international interest for its innovative personal control features.⁸⁷
- 5.88 However, at hearings in September 2012, the Consumers Health Forum of Australia (CHF) expressed concerns that the system as introduced did not address privacy requirements, particularly in the sharing of data between agencies and on individual access:
- Some of the examples that we were given were things like people did not want their sexual history being accessible by their physiotherapist or their mental health history being accessible by their dentist, for instance. So the controls need to be very specific around which practitioners you are giving access to particular parts of your records to.⁸⁸
- 5.89 The Committee notes that the introduction of the new AAPs under amendments to the Privacy Act could require more secure handling of sensitive health information and may impact on current arrangements.

83 Consumers e-Health Alliance (CeHA), *Submission 41*, pp. 1-2.

84 (CeHA), *Submission 41*, pp. 1-2.

85 Consumers Health Forum of Australia (CHF), *Submission 15*, pp. 2-3.

86 AIC, *Submission 12*, p. 2 and see Mrs Nancy Bosler, President, Australian Seniors Computer Clubs Association (ASCCA), *Committee Hansard* 23 March 2012, p. 17.

87 Dr Mukesh Haikerwal, Head of Clinical Leadership Engagement and Safety, National e-Health Transition Authority (NEHTA), *Committee Hansard*, 23 March 2012, p. 12.

88 Ms Anna Greenwood, Deputy Chief Executive Officer, CHF, *Committee Hansard*, 19 September 2012, p. 4.

Data security for health service providers

- 5.90 Another concern related to the security of PCEHR records at medical practices and health services providers. City Clinic reported on the impact of information theft on a Sydney medical practice, and noted the lack of formal recourse for charging someone for information theft in Australia. This compares poorly with the US and UK which provide victim compensation and penalty of imprisonment for information theft.⁸⁹
- 5.91 The NEHTA advised that the National Health and Security Access Framework will provide guidance to health care providers on information security, and the National Authentication Service for Health will ensure that e-Health transactions are private, traceable and conducted by known entities.⁹⁰
- 5.92 DoHA explained that to participate in the NBN pilot program, service provider applicants will also be required to provide plans for emergency procedures, security, safety and confidentiality. Suitable patients for the trial must also be identified.⁹¹
- 5.93 The SA Government observed that all jurisdictions will need to ensure protections for the privacy and the security of personal information conveyed by the NBN. The submission also referred to the need for subsidised training for seniors to use the NBN safely and securely.⁹²
- 5.94 The CHF welcomed proposals for data breach notification to improve protections for consumers.⁹³ The Committee has discussed legislative developments on the protection of personal information and data breaches for SMEs above.

Consumer awareness measures

- 5.95 As discussed in Chapter 3, it was recommended to the Committee that the Government's consumer awareness campaigns for cybersafety should target risky behaviours that result in victimisation, rather than focus on the daunting number and range of risks. The Committee was told that for many seniors:

89 City Clinic, Sydney, *Submission 48*.

90 NEHTA, *Submission 4*, pp. 3-4.

91 Department of Health and Ageing (DoHA), *Submission 16*, Overview.

92 SA Government, *Submission 37*, p. 7.

93 Ms Carol Bennett, CEO, CHF, *Committee Hansard*, 19 September 2012, p. 8.

...a lack of knowledge creates a fear of the unknown and an awareness of the risks posed by online fraud tends to exaggerate this fear.⁹⁴

- 5.96 Accordingly, submitters advocated for a combination of computer education and strong practical messages to inform seniors. Dr Cross's research suggested that simple messages (such as 'no one should send you an email asking for personal details' and 'you should be very wary if someone asks you to send money') help consumers take control of the situation, and think through their online behaviour and its consequences.⁹⁵
- 5.97 There was strong agreement that messages like these, succinct and clear, should headline any cybersafety advertising. There was also some support for a dedicated campaign targeting seniors.
- 5.98 The SA Government, for example, expressed concern that the Australian Government's focus on cybersafety for the young and their parents, on the ACMA website and elsewhere, has left the needs of older people unaddressed.⁹⁶ The ACMA in its submission maintained that seniors are included as part of this extended family focus.⁹⁷
- 5.99 DBCDE advised that it views cybersafety as a matter of behaviour rather than age, noting research has found that seniors, once skilled, are not more at-risk than other community sectors. Seniors' internet access was, however, lower than other groups and hence the Department has new initiatives to help seniors go online.⁹⁸
- 5.100 Life Activities Clubs Victoria Inc. (LACVI) agreed with this view of seniors but considered that a dedicated cybersafety awareness platform for older Australians is necessary to overturn negative associations and fears. This should be promulgated by online and traditional media, with advice about the benefits of going online safely and the key safety messages featured.⁹⁹

94 Dr Cross, *Submission 49*, p. 5.

95 Referring to a training booklet she had prepared for the Carindale Police Citizens Youth Club's Seniors Online Security Project. *Submission 49*, p. 7.

96 The submission observed that much of the Cybersafety Plan, ACMA's work and that of the Cybersafety Consultative Working Group, while generic in some instances, focusses on the young and their families and couches its advice in those terms. The Cybersmart website for instance provides information for 'young kids', 'kids', 'teens', 'teachers', 'parents' and 'libraries'. See SA Government, *Submission 37*, p. 8.

97 ACMA, *Submission 24*, p. 9.

98 DBCDE, *Submission 25*, pp. 10-11, 13.

99 LACVI, *Submission 5*, p. 2.

- 5.101 While others agreed that a traditional media campaign is important to reach offline seniors, there was nevertheless scepticism about relying too much on glossy booklets and publications. The NSA recommended circulating alerts, like those issued by the ACCC's SCAMwatch, with key messages such as the: 'higher the return, the higher the risk'.¹⁰⁰
- 5.102 Mrs Joyce Hocking (formerly Sheasby) recommended these messages be conveyed as 60 second advertisements on television 'soapies' and cookery shows, to reach the many seniors who are unskilled and isolated.¹⁰¹ Legacy Australia supported the use of television, radio, and the print media to reach seniors.¹⁰²
- 5.103 Stakeholders also wanted a more co-ordinated and streamlined approach to promote cybersafety awareness. The CIS, for example, recommended a universal and centrally managed national education and outreach program, considering the current approach to be 'piecemeal'.¹⁰³
- 5.104 The Communications Law Centre (CLC) emphasised that, in promotion of any campaign, 'real world links' are essential.¹⁰⁴ The Australian Library and Information Association (ALIA) recommended taking a 'lifelong learning approach' to cybersafety and funding libraries to provide more services to seniors. There was strong support for this from other stakeholders with older clients.¹⁰⁵ The Committee has recommended in Chapter 4 for funding to libraries for seniors' IT training and cyber education.
- 5.105 Evidence also suggests that cybersafety campaigns for seniors should be delivered with brevity, with alerts clearly headlined. It is also important to preserve a positive message in the promulgation of cybersafety warnings: as Mrs Hocking told the Committee a little 'fun' in a campaign will retain seniors' interest.¹⁰⁶ The barrage of information currently available is evidently confusing to seniors, and is acting as a deterrent to their adaptation to online activities.

100 Mr Michael O'Neill, CEO, National Seniors Australia (NSA), *Committee Hansard*, 31 October 2012, pp. 1-2.

101 Mrs Joyce Hocking, *Committee Hansard*, 31 October 2012, pp. 7-8.

102 Legacy Australia, *Submission 10*, p. 2.

103 Mr MacGibbon, CIS, *Committee Hansard*, 14 March 2012, p. 1.

104 See Communications Law Centre (CLC), University of Technology Sydney (UTS), *Submission 31*, p. 4.

105 See for example AHRC, *Submission 2*, Recommendation 2, p. 3; ASCCA, *Submission 7*, p. 4; Brotherhood of St Laurence, *Submission 13*, pp. 3, 7; Ms Vanessa Kaye, Australian Library and Information Association (ALIA), *Committee Hansard*, 9 May 2012, p. 7.

106 See CLC, UTS, *Submission 31*, p. 4

- 5.106 The Committee has made recommendations in this report for a single clearinghouse or site for scam news, reporting and education, with telephone advice. One benefit of this will be to bring all cybersafety information – the plethora of scam alerts issued on the ACCC’s SCAMwatch, CERT Australia, ATO and Stay Smart Online websites – to a single accessible point.¹⁰⁷

Recommendation 10

That Australian Government’s cyber awareness campaigns should headline clear and practical messages for cybersafety on the central reporting and awareness portal, and appear up front of all published cyber awareness material for the general community.

Central collection and analysis of data

- 5.107 During the inquiry, the Committee was referred to advances made in the UK, the US and Canada which have centralised internet fraud reporting with support services offered to senior victims.¹⁰⁸
- 5.108 The Committee heard that a centralised reporting arrangement provides two major advantages: it is less confusing and bureaucratic so increases the rate of reportage; and it allows for collation of more reliable data about the actual impacts of cybercrime on different community segments.
- 5.109 The lack of reliable data on cybercrime was widely cited by stakeholders as an obstacle to the disruption of cybercrime and effective policy development for that purpose. Dr Cross advised on motivations for central reportage overseas:

...There was a shared belief amongst the UK, USA and Canadian agencies that the ultimate form of fraud prevention lies in the disruption of fraud activity, and it is this belief that should drive further work in this area.¹⁰⁹

107 DBCDE, *Submission 25*, p. 3, ATO, *Submission 43*, p. 11.

108 These are the ActionFraud in the UK, the Internet Crime Complaint Centre in the USA and the Canadian Anti-Fraud Centre in Canada, see Dr Cassandra Cross, *Submission 49*, p. 12.

109 Dr Cross, *Submission 49*, p. 13.

5.110 The ASIC confirmed that the low rate of self-reportage by Australians on cybercrime means that the Commission 'has relatively limited information about the impact of online fraud effecting Australians and an older Australians specifically'.¹¹⁰ The Australian Institute of Crime (AIC) advised that the reportage of cybercrimes to different agencies makes it 'difficult to assess impact and where it falls'.¹¹¹

5.111 The AIC's Dr Rick Brown explained that the consequence of disparate collection is a lack of consistency in studies being conducted by various agencies. He described the process as one of trying to compare 'apples and pears':

Part of the problem is the multiple points by which reports can be made...we have recently been looking at one area, identity misuse, and finding that there are wide differences just among federal agencies in the definitions that are used, the way that data is stored and so on. It makes it very difficult to get a handle on that as an area. It means we really have no monitoring basis for understanding how trends are changing, apart from the large-scale surveys that the ABS, for example, do on a sporadic basis.¹¹²

5.112 To rectify this, the CIS recommended that the reporting tab on the central cybercrime reporting portal should be designed both for user facility and for efficient automated data matching. Mr MacGibbon suggested this could be achieved by tabulating no more than 20 or 30 questions specifically for each type of reported offence, under the basic formula of 'the who, what, where, when, why and how of that particular type of offence'.¹¹³

5.113 The CIS and the CLC also emphasised that the definition of cybercrime for crime reportage must be broad, and not limited to malicious code, if the measure is to be effective.¹¹⁴ The ACFT, which prepares annual surveys of computer use and the impact of cybercrime on consumers, observed:

With a more extensive understanding of who is victimised and why, more effective scam prevention measures can be enacted.¹¹⁵

110 ASIC, *Submission 46*, p. 6.

111 AIC, *Submission 12*, p. 2.

112 Dr Rick Brown, AIC, *Committee Hansard*, 10 October 2012, pp. 4-5.

113 Mr MacGibbon, CIS, *Committee Hansard*, 14 March 2012, p. 7.

114 CLC, *Submission 31*, p. 4.

115 The ACFT hold an annual consumer fraud survey to assess the public's exposure to consumer scams, to assess their impact, to determine how victims respond and to identify any emerging typologies and issues. C Budd and J Anderson, 'Consumer Fraud in Australasia: Results of the ACFT Online Australia surveys 2008 and 2009', *AIC Reports Technical and Background Paper 43*, p. 14.

- 5.114 The AIC advocated establishing a National Cyber Security Monitoring Program for this task, which the AIC would be well positioned to lead. This program would also conduct annual surveys to identify the extent and impact of cyber security incidents on individuals, businesses, organisations of national interest and government.¹¹⁶
- 5.115 The ACMA and DBCDE recognised the importance of having such data to inform their work. The ACMA stated that:
- ...limited availability of specific, credible and detailed research into online risks and threats unique to older Australians [inhibits] consideration of the best methods to manage these risks and the most appropriate channels to inform, educate and empower senior Australians'.¹¹⁷
- 5.116 The AFP observed:
- Cyber-safety prevention and awareness raising campaigns need to be underpinned by sound research and longitudinal research however such research can take years. That is one of the challenges associated with requiring an evidence based approach to cyber-safety that the AFP would like addressed.¹¹⁸

Recommendation 11

That the cybercrime reporting tab on the central reporting and awareness portal be designed for ease of access to users and to facilitate data collation and assessment. The system should be supported by simple online instructions and accessible to the visually and aurally impaired, and for print in hard copy.

Concluding comments

- 5.117 The Committee's inquiry proceeds at a time of review and reform of Australia's laws to meet an enormous growth in the use of electronic communications and information storage by governments and businesses. The commensurate crime developments impose new obligations on regulators to provide a framework of laws that are robust but flexible.

¹¹⁶ AIC, *Submission 12*, p. 6.

¹¹⁷ ACMA, *Submission 24*, p. 4 and See DBCDE, *Submission 25*, p. 13.

¹¹⁸ AFP, *Submission 20*, p. 5.

- 5.118 The Committee's review in this chapter covers some key aspects of reform recently implemented, and providing platforms for others to be made in the future. The Committee did not receive submissions to this inquiry from key policy agencies managing these reforms – the Department of PM&C or the Attorney-General's Department, nor from the ACCC which manages SCAMwatch the reportage site for fraud.
- 5.119 The task of this inquiry was to review the risks and threats to senior Australians, and many submitters made comment on what they saw as too incremental and piecemeal an approach to consumer protection.
- 5.120 The Committee also heard concerns about privacy under the PCEHR, and about the protection of data in private practices. These matters will warrant continual monitoring in the first phases of eHealth implementation. There may also be implications for review under the new AAPs and potential data breach legislation.
- 5.121 The Committee has made recommendations based on the evidence it has received and on the available statistical data which, in the Committee's opinion, compels government to focus on the protections owing vulnerable Australians. This means progressive review of relevant laws, as well as the communication of key cybersafety messages in a campaign targeting seniors, many of whom are new to the internet as are the young.
- 5.122 The Committee believes that the compilation of accurate data to quantify and understand the actual threats and risks to which Australians aged 55 plus are exposed will be fundamental to any effective senior targeted or community-wide campaign. The next chapter considers what role industry might take with government in this regard.

The role of industry

Introduction

- 6.1 The internet has done more than change the means and speed of global communication. According to the Department of Prime Minister and Cabinet's (PM&C) cyber discussion paper, it has changed 'the ground rules of social and economic interaction'.¹ Where governments once decided the terms of a citizens' engagement with the outside world, the digital economy is now under management of the private sector and may bypass domestic obligations and laws.
- 6.2 Given the centrality of the digital economy to Australia's future economic prosperity, it has been argued that Internet Service Providers (ISPs) and web-based vendors should carry more responsibility for keeping their clients safe online. Another view maintains that a co-regulatory approach best preserves the balance between regulation and the market incentives necessary to grow business online.
- 6.3 This chapter reviews the effectiveness of current national industry standards and codes to regulate online safety and, more broadly, considers what role the private sector does and could play to better inform and protect seniors from online threats.

¹ Australian Government, *Connecting with Confidence: Optimising Australia's Digital Future. A Public Discussion Paper*, Department of Prime Minister and Cabinet (PM&C), 2011, p. 8.

Building productive capacity under a digital economy

- 6.4 Digital technologies have enormous potential to drive productivity and growth in the Australian economy.² However, while Australians have high levels of internet use compared with other countries, studies have found that Australian businesses are lagging behind in delivery of online services.³
- 6.5 The Department of Broadband, Communications and the Digital Economy (DBCDE) has identified the following national priorities to address the problem:
- (a) build Australia's communications critical infrastructure to provide a world class platform for online activity
 - (b) reform communications markets for fixed-line broadband, wireless spectrum and content to make these markets competitive, open, transparent and fair
 - (c) train Australian consumers, workers and small businesses to have the online skills to compete globally, stay safe and participate online
 - (d) assist Australian businesses and governments to adapt to the online environment so they can innovate and develop new products, services and business models.⁴
- 6.6 The Government has recognised that if Australia's consumers, including its older members, are to go online confidently then our marketplace and our businesses must prepare to manage the risks to reap the rewards.⁵
- 6.7 This view was strongly endorsed by respondents to this inquiry. Many also considered that the best way to ensure Australian ISPs and businesses see online safety and security as core-business is to ensure there is a correct balance between market and regulatory incentives in the online business environment.

2 Research suggests a 10 per cent increase in internet connections would grow Australia's GDP by 0.44 per cent, that is by an estimated \$5.6 billion. See Australian Government, *Connecting with Confidence: Optimising Australia's Digital Future*, PM&C, 2011, p. 12.

3 Australian Bureau of Statistics (ABS), *Household Use of Information Technology 2008–09*, Cat. No. 8146.0, ABS, 2009, and see Department of Broadband, Communications and the Digital Economy (DBCDE), *Boosting Australia's Productivity Performance through Broadband, Communications and the Digital Economy*, [n.d], pp. 1–2. <www.dbcde.gov.au/__data/assets/pdf_file/0011/156566/Productivity-measures-of-DBCDE.pdf> viewed 21 January 2013.

4 DBCDE, *Boosting Australia's Productivity Performance through Broadband, Communications and the Digital Economy* [n.d.], p. 1, viewed 21 January 2013.

5 DBCDE, *Boosting Australia's Productivity Performance through Broadband, Communications and the Digital Economy* [n.d.], p. 1, viewed 21 January 2013.

Industry security and consumer protection codes

- 6.8 There are a number of industry codes and standards which apply to ISPs and businesses participating in ecommerce. To preserve the independence of the industry these codes are voluntary, the assumption being that market forces will provide price incentives to comply.⁶
- 6.9 Under this self-regulatory model, both industry and consumers have incentives to self-protect but are not compelled by law to do so. The DBCDE submission stated:
- 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, ultimately it is businesses and individuals who must take responsibility for their own safety and security online. This means being aware of the potential risks and taking the necessary steps to protect themselves. Businesses should develop safe practices to protect both themselves and their customers, and promptly report incidents when they occur. Individuals should ensure that they take appropriate measures to protect themselves online.⁷
- 6.10 Asked whether the law might be strengthened to ensure compliance with best practice standards and safeguards, DBCDE representatives advised that education and awareness raising are the better means to protect seniors online.⁸ However, many stakeholders maintained that Government could do more to encourage ISPs and businesses to protect personal information and limit tolerance of criminality on their websites.⁹
- 6.11 In this line of argument, the effectiveness of the current codes and standards was not the issue but instead widespread failure, on the part of industries, to comply. Various codes and guidelines apply to online and credit card interactions, some of which are listed below.

6 Part 6 of the *Telecommunications Act 1997 (the Act)* outlines how industry self-regulation is to be achieved through industry initiated and developed codes of practice. See Australian Communications and Media Authority (ACMA), 'About Industry Codes and Standards', <www.acma.gov.au/WEB/STANDARD/pc=PC_2080> viewed 20 February 2013.

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

8 Mr Abul Rizvi, Deputy Secretary, Digital Economy and Services Group, DBCDE, *Committee Hansard*, 12 September 2012, p. 2.

9 For instance, eBay and PayPal, *Submission 11, passim*; Centre for Internet Safety (CIS), *Submission 26*, p. 1; Communications Law Centre (CLC), University of Technology Sydney, *Submission 31*, p. 2; Australian Information Security Association (AISA), *Submission 32*, p. 2.

Payment Card Industry Data Security Standards

- 6.12 Payment card industry security standards are upheld by a range of voluntary codes, including the Data Security Standard (PCI DSS), Payment Application Data Security Standard (PA-DSS), and PIN Transaction Security (PTS) requirements.¹⁰
- 6.13 The PCI DSS is the main instrument regulating merchant processes for payment card security, covering data storage, security settings and networks, monitoring and response to breaches. The PCI Security Standards Council, a global forum established in 2006, provides an online assessment tool and registration tool for PCI DSS. The Council is also responsible for the development, management, education, and awareness of security standards.
- 6.14 Founding members of the PCI SS Council are American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. which incorporate the PCI DSS as the technical requirements of each of their data security compliance programs.

E Payments Code

- 6.15 The Australian Securities and Investments Commission (ASIC) monitors the ePayments code as part of its responsibilities for regulation of electronic payments, including ATM, EFTPOS and credit card transactions, online payments, internet and mobile banking and BPAY.¹¹
- 6.16 The ePayments Code, formerly known as the Electronic Funds Transfer Code of Conduct, has existed since 1986.¹² ASIC advises that the Code:
- requires subscribers to give consumers terms and conditions, information about changes to terms and conditions (such as fee increases), receipts and statements,
 - establishes a consumer protection liability allocation regime for unauthorised payments including on-line payments,
 - establishes a regime for recovering mistaken internet payments.¹³

10 For information in this section see PCI Security Standards Council website <www.pcisecuritystandards.org/organization_info/index.php> viewed 19 February 2013.

11 ASIC, *Submission 46*, pp. 3–4.

12 ASIC, *Submission 46*, p. 5.

13 ASIC, *Submission 46*, p. 6.

The iCode

- 6.17 In June 2010 the Internet Industry Association of Australia (IIA) launched a voluntary ISP code of practice, the 'iCode', to promote a 'security culture' across the internet industry and reduce the number of compromised computers in Australia. This standard is designed to provide a consistent approach for Australian ISPs to help inform, educate and protect their customers in relation to cyber security risks.¹⁴
- 6.18 The iCode encourages ISPs to monitor their networks for malicious 'botnet' activity and, under the ACMA's Australian Internet Security Initiative (AISI), to notify customers if their computers become compromised, and to assist in rehabilitating compromised computers.¹⁵
- 6.19 Representatives from DBCDE advised that the iCode is the first of its kind and has attracted international attention since it commenced operation. Currently there are 34 ISPs signed up to the code, covering up to 90 per cent of users.¹⁶

Best Practice Guidelines for dating websites

- 6.20 On 13 February 2012 the ACCC issued the *Best Practice Guidelines for Online Dating*. The guidelines were developed by a working group chaired by the ACCC and comprising representatives from a number of dating websites.¹⁷
- 6.21 The guidelines are voluntary and, according to the ACCC, are intended to promote 'best practice' to dating websites, and to help users avoid romance and dating scams. While compliant websites may advertise this, the ACCC does not endorse individual websites, nor vet their compliance with the guidelines.¹⁸

14 See ACMA, Australian Internet Security Initiative (AISI), <www.acma.gov.au/WEB/STANDARD/pc=PC_310317> viewed 22 February 2013.

15 Botnets or drones are terms for a computer co-opted by malware for hosting fake websites or distributing spam and phishing attacks. See ACMA, AISI, viewed 22 February 2013.

16 Mr Rizvi and Mr Chris Drew, Acting Assistant Secretary, National Security and International Branch, Digital Strategy Division, DBCDE, *Committee Hansard*, 12 September 2012, p. 4.

17 See ACCC, *Best Practice Guidelines for Online Dating*. <www.accc.gov.au/content/index.phtml/tag/DatingSiteGuidelines/> viewed January, 2013.

18 ACCC, Scamwatch, <www.scamwatch.gov.au/content/index.phtml/itemId/694363> viewed 12 February 2013.

Mandatory codes for industry?

- 6.22 As discussed in the previous chapter, the Government is currently investigating the feasibility of introducing a mandatory data breach notification scheme. Possible justifications for introduction of such a scheme are that it would promote awareness among industry and consumers about the requirements for their cyber security, and hence enhance the security of interactions within the digital economy.¹⁹
- 6.23 The ACMA advised that regulation of the cyber sphere should be the joint responsibility of government and industry as ‘co-regulators’. The Authority referred to voluntary codes such as the iCode, introduced under the AISI, as an illustration of the growing number of ‘incentives’ for industry compliance.²⁰
- 6.24 However, the Centre for Internet Safety (CIS) told the Committee that, in reality, few small and medium enterprises (SMEs) comply with industry codes given the lack of time, resources and financial incentives to do so.²¹
- 6.25 In relation to the PCI DSS, the CIS stated that there are few tangible penalties to the merchant for non-compliance and market incentives are isolated: it is the consumer who experiences financial loss after a data breach on a credit card interaction, and often for many years after the event.²² Referring to requirements for online warnings and monitoring under the ACCC’s dating guidelines, the CIS further observed that the most effective deterrents to criminal activity, such as defensive design and data monitoring, are more expensive to implement and hence less likely to be adopted.²³
- 6.26 The iCode, however, was greeted positively as progress towards a more robust security environment. The Communications Law Centre (CLC) stated:

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.²⁴

19 Australian Government, *Discussion Paper: Australian Privacy Breach Notification*, Commonwealth A-G’s Department, October 2012.

20 Ms Andree Wright, General Manager, Digital Economy Division, Australian Communications and Media Authority (ACMA) *Committee Hansard*, 23 March 2012, p. 39.

21 Mr Alastair MacGibbon, Co-Director, CIS, *Committee Hansard*, 14 March 2012, pp. 2–3.

22 Professor Nigel Phair, Co-Director, CIS, *Committee Hansard*, 14 March 2012, pp. 2–3.

23 See discussion on defensive web design below for more detail. CIS, *Submission 26*, p. 8.

24 CLC, UTS, *Submission 5*, p. 31.

- 6.27 Asked about the potential to make iCode compliance mandatory, DBCDE's Mr Abdul Rizvi advised that, in his view, the measure would be precipitant, although it could be considered under the current review (September 2012):
- ...I think pressing too quickly to move down the mandatory path in that regard may not be giving sufficient credit to the industry which is, indeed, the only industry in the world that has been prepared to go down this path. I think they deserve some recognition for that.²⁵
- 6.28 As noted above, according to the DCBDE, roughly a third of ISPs subscribe to the iCode, protecting an estimated 90 per cent of users.²⁶
- 6.29 This supported the view among some stakeholders that the iCode would be a good platform to leverage ISPs into a more proactive intervention role. In turn, this would support the broader program of 'structures and standards' necessary to ensure the long term health and productive evolution of the digital economy.²⁷
- 6.30 At the time of writing the results of the iCode review underway in 2012 had not been released.²⁸

Self-regulation and data monitoring

- 6.31 Industry's uneven response to privacy and cyber security requirements to date has been acknowledged as an issue by the Government in developing its cybersafety and security policy. In relation to social networking, a PM&C cyber discussion paper stated, for example, that:

Social networking sites are almost entirely facilitated by the private sector. Although many of the larger sites have some capacity to monitor and limit abusive behaviour, some others do not.²⁹

25 *Committee Hansard*, 12 September 2012, p. 4.

26 Mr Rizvi and Mr Chris Drew, Acting Assistant Secretary, National Security and International Branch, Digital Strategy Division, DBCDE, *Committee Hansard*, 12 September 2012, p. 4.

27 CIS, *Submission 26*, p. 3, Professor Michael Fraser, Director, CLC, *Committee Hansard*, 23 March 2012, p. 32, and see Australian Crime Commission (ACC), *Submission 9*, p. 22.

28 DBCDE, *Cyber Security: Internet Service Provider Voluntary Code of Practice*: <www.dbcde.gov.au/online_safety_and_security/cyber_security> viewed 25 February 2013.

29 K Harvey, *Submission 42: PM&C, Cyber White Paper Discussion Paper, Digital Citizenship in a Networked Society*, 2011, p. 3.

- 6.32 Given seniors' assumptions that social networking sites, online journals, and information sites are subject to monitoring, it was argued that the internet industry and other businesses, which stand to profit greatly by seniors' increased participation online, should be more vigilant in protecting these vulnerable clients.³⁰
- 6.33 A number of proposals were explored in evidence to the inquiry, including the mandatory application of iCode data monitoring for ISPs, the utility of 'walled gardens' and the potential of private networks to improve the data security of businesses. Recommendations were also made for enhanced security and consumer awareness measures to be adopted by banks and money transfer agencies.

ISPs, data monitoring and 'walled gardens'

- 6.34 As mentioned, the Government's AISI promotes a voluntary arrangement for data sharing between ACMA and internet services to support online security. The iCode provides the compliance standard for this process.
- 6.35 Ms Andree Wright, General Manager, Digital Economy Division, ACMA explained the function of the AISI, whereby the Authority:
- ... [is] able to pass on reports of compromised computers to particular industry participants who then check them out and they contact their users to inform them that their computers are compromised, and they work with them to address that. We have initiated that in Australia and it is regarded as an international first and best practice, and it has been emulated by other countries.³¹
- 6.36 The Australian Information Security Association (AISA), the peak body for security professionals, approved this partnership between industry and Government to keep pace with elevating threat levels as the digital economy expands:
- The increasing threats to home users, associated with the compromise of their computers, cannot be solved solely by the current strategies and technologies (education and anti-virus) and a new approach is required. This may involve upstream mitigation

30 For example, Professor Michael Fraser, Director, CLC, *Committee Hansard*, 23 March 2012, p. 32.

31 *Committee Hansard*, 23 March 2012, p. 39.

(for example at the ISP level), revised education or partnership with software providers...³²

- 6.37 However, it was also thought that current requirements do not provide adequate certainty to consumers given the degree and range of threats evolving in the cyber environment.
- 6.38 The CIS's Professor Nigel Phair described ISPs as the 'gateway or funnel point for malicious software or content – packets of information'.³³ The CIS believed that 'safe harbour' type provisions, like those which exempt postal services for delivering illegal goods, had not facilitated the development of successful internet security measures by ISPs in Australia.³⁴
- 6.39 Professor Michael Fraser, Director of CLC, argued that ISPs should not be allowed to continue in this manner as 'mere conduits' for illegal activity:³⁵
- I do not agree with arguments that these people are like public carriers and that, like the post office, they should not be looking into the mail. Of course there are privacy issues that need to be managed, but I think much more could be done by the ISPs, for example, in managing and creating a secure environment for their customers.³⁶
- 6.40 The AISA maintained that where 'the costs corresponding to poor security practices are externalised, there is a role for the Government to set or co-ordinate the establishment of benchmarks of acceptable practices'.³⁷
- 6.41 One area of concern was the iCode's lack of prescribed industry responses should a system infection be identified.³⁸ The CIS recommended the imposition of 'network access control' and of 'walled gardens' until remediation occurs. This would make it mandatory for ISPs to identify, close down and isolate infected systems. The CIS noted that a number of

32 AISA, *Submission 32*, p. 10.

33 *Committee Hansard*, 14 March 2012, p. 4.

34 Mr MacGibbon, CIS, *Committee Hansard*, 14 March 2012, p. 4, and see CIS, *Submission 26*, p. [4].

35 CLC, UTS, *Submission 31*, p. 5.

36 *Committee Hansard*, 23 March 2012, p. 32.

37 AISA, *Submission 32*, p. 10.

38 At present an ISP's response can range from strong – putting a 'walled garden' around a compromised computer, effectively a temporary block by the ISP; to weak – writing a letter to the consumer months after the problem has been identified. Mr MacGibbon, CIS, *Committee Hansard*, 14 March 2012, p. 4.

websites use this approach for compromised computers, but ISPs have not done so to date.³⁹

6.42 The Committee explored possible objections to these proposals, being practical: the monitoring capability of ISPs; and ethical: on invasion of privacy grounds.

6.43 The CIS Co-Director Mr Alastair MacGibbon insisted that user activities are currently completely transparent to ISPs, given billing monitoring: 'The ISP knows what the average user does and can identify huge spikes in traffic and other behaviour'. In this view, there is an onus on the Government to specify exactly what is required of ISPs in relation to management of the knowledge they have in defence of the user.⁴⁰

6.44 Professor Fraser of CLC discussed related privacy concerns about the use of personal information by social networking sites and ISPs for commercial purposes, observing that the access of the private sector to this information is unprecedented, and merits government regulation. He considered that industry codes can be effective to meet evolving threats, but legislation must provide the overarching framework.⁴¹

6.45 The Committee asked Telstra Corporation Ltd, which has subscribed to the iCode, about its current commitments and activities:

On the operations side, our security people are constantly looking at the traffic coming on the network and whether there are any vectors of attack, as they call them, where people are trying to do malicious things on the network. We remove a considerable amount of spam that comes onto the network before it even gets to the users, and when we do become aware of scams that have actually got through to users we do attempt to educate them and inform them about that.⁴²

6.46 Telstra otherwise considered that education of the consumer, rather than increased regulatory controls, is the best means to protect the consumer from online risks.⁴³

39 Mr MacGibbon, CIS, *Committee Hansard*, 14 March 2012, pp. 4, 9.

40 *Committee Hansard*, 14 March 2012, pp. 8, 9.

41 *Committee Hansard* 23 March 2012, pp. 34, 33.

42 Mr Darren Kane, Director of Government Relations, Telstra Corporation Ltd, *Committee Hansard*, 23 March 2012, p. 23.

43 Mr Kane, Telstra Corporation Ltd, *Committee Hansard*, 23 March 2012, p. 24.

Private networks

6.47 Private networks are commonly used by government agencies and the corporate sphere to protect data and preserve system integrity. Virtual private networks may be defined as:

A network that is established via the use of public wires, such as telephone or broadband internet wires. These networks use encryption, digital certificates and other security tools to protect them against unauthorised access.⁴⁴

6.48 There was some support for the promotion of secure safe social networks, which fall within the rubric of private networks, especially for seniors. Mrs Nancy Bosler, President of the Australian Seniors Computers Clubs Australia (ASCCA), alerted the Committee to the United Kingdom's 'afinerday.com' site, a secure social networking site for seniors to safely communicate with family.⁴⁵ The African Seniors Club believed these protected sites could assist seniors in the refugee community.⁴⁶

6.49 An ABACUS (Australian Business Assessment of Computer User Security) survey of corporate networks indicated that 13 per cent used virtual private networks, while 46 per cent had a local area network and 12 per cent a wide area network. A far greater proportion of larger corporates deployed a range of IT security measures, including virtual private networks.⁴⁷

6.50 Asked about the utility of private networks to address seniors' security concerns, CLC's Professor Fraser maintained that, while large corporates may deploy these effectively, the Government has a responsibility to the broader community to regulate the cyber sphere:

... what I do not want to see is a digital divide open up so that if you are dealing in a commercial space you can operate inside these walled-fortress webs, but you are otherwise left to protect yourself. So if you are in John Wayne's town you are all right, but past that is the badlands. That will lead to a digital divide where underprivileged members of the community do not have the same

44 G Challice, *The Australian Business Assessment of Computer User Security (ABACUS) Survey: Methodology Report*, Australian Institute of Criminology (AIC) 2009, p. 63.

45 *Committee Hansard* 23 March 2012, p. 19.

46 African Seniors Club – Australia Inc. *Submission 18*, p. 2.

47 K Richards, 'The ABACUS: a National Survey', *AIC Research and Public Policy Series no. 102*, pp. 32–33.

security, unless they are doing certain kinds of commercial transactions which are within these fortresses.⁴⁸

- 6.51 The CLC recommended building technical standards into the iCode to keep pace with evolving criminal activity.⁴⁹ The AISA took another view, considering that technical specification cannot keep up with change. It preferred an ‘outcomes’ based approach of co-regulation, with more specific requirements set out for industry:

The Government should work with industry to provide guidance on what is meant by “reasonable security”, particularly with regard to new and emerging technologies. This guidance should extend not just to the organisation’s own data and systems but should also have regard to its role as a participant in the broader online world, which supports the economic prosperity and security of all Australians. It may include, for example, reference to accepted international standards as well as more specific guidance.⁵⁰

- 6.52 The AISA referred the Committee to work being done in the European Commission to develop this.⁵¹

Regulating online transactions and money transfer

- 6.53 As previously recorded in this report, advance fee frauds currently account for the largest number of victims of cybercrime, with seniors disproportionately affected by some types of scamming activities such as investment fraud and Nigerian scams. It was suggested in evidence that banks, ISPs and money transfer agencies could all be more active in disrupting these activities.

The obligations of banks

- 6.54 During the inquiry, the Committee heard of scam victims who sent all of their savings to ‘Nigerian’ scammers overseas, or who borrowed money to

48 *Committee Hansard*, 23 March 2012, p. 34.

49 Professor Fraser, CLC, *Committee Hansard*, 23 March 2012, p. 35.

50 AISA, *Submission 32*, pp. 6, 7.

51 D Korff and I Brown, *New Challenges to Data Protection: Final Report*, European Commission, 20 January 2010, in AISA, *Submission 32*, p. 6.

invest in serious and organised investment fraud (SOIF) schemes.⁵² Submitters explored options for banks to address this, such as by monitoring withdrawal and throughput in accounts.

- 6.55 In its submission to the Committee, the Australian Federal Police (AFP) expressed concerns about weaknesses under investment and banking sector rules, such as identity rules around self-managed funds and hardship payments. For instance, bank accounts receiving stolen or defrauded funds may be held in multiple names and are not checked.⁵³
- 6.56 The Brotherhood of St Laurence recommended that further obligations be placed on banks and service providers to protect customers from phishing. It suggested they participate in the Domain-based Message Authentication, Reporting and Conformance (DMARC) system, a partnership of 15 major technology and finance companies in the USA, including Google and Facebook.⁵⁴
- 6.57 The Australian Crime Commission (ACC) suggested that an additional control on SOIF schemes could be the use of early warning mechanisms on internet banking and other relevant sites. It considered that this measure, combined with an effective public awareness campaign, could significantly reduce the number of Australian victims of these scams. The ACC advised that it is currently discussing these measures with industry partners.⁵⁵
- 6.58 The Committee notes that, under recent reforms to the credit reporting regime, banks and financial institutions will have greater access to review the types of accounts held by individuals, their current credit limits and access to repayment history. These amendments should provide greater transparency and may allow for the monitoring of unusual transactions and decrease risks to consumers.⁵⁶

52 See for example, MW, *Submission 17*, JA, *Submission 21* and Case Study, ACC, *Submission 9*, p. 19.

53 Australian Federal Police (AFP), *Submission 20*, p. 3.

54 Brotherhood of St Laurence, *Submission 13*, p. 8.

55 Mrs Karen Harfield, Executive Director, Fusion, Target Development and Performance, Australian Crime Commission (ACC), *Committee Hansard*, 15 August 2012, p. 1.

56 Attorney-General, the Hon. Nicola Roxon MP, *Privacy Amendment (Enhancing Privacy Protection) Bill 2012*, Second Reading Speech, *House Hansard*, 23 May 2012, p. 5210, and see Chapter 5.

Online shopping and money transfer

- 6.59 A number of proposals were also made to make online shopping transactions and the commercial payment environment safer.
- 6.60 The eBay and Paypal approved 2011 amendments to the *Privacy Act 1988*, which enabled the use and disclosure of credit reporting information for electronic identity verification.⁵⁷ The submission recommended extending these reforms to allow for verification of State held electronic licences to make the online commerce and payments environment more secure.⁵⁸
- 6.61 The South Australian (SA) Government reported advances on electronic verification of identity under the National Document Verification Service, a key component of the NISS. The submission advised that the SA Births, Deaths and Marriages Registration Office is currently participating in trials of the scheme, which will then be progressively implemented to government agencies, and potentially to the private sector.⁵⁹
- 6.62 Other proposals were made to ensure money transfer agencies took greater responsibility for their involvement in fraudulent transactions.⁶⁰
- 6.63 Dr Cross cited enforcement trends in the action by the US Police against MoneyGram, a US based money transfer agency, which was charged with a laundering offence. She recommended that government work with money transfer agencies to better understand business obligations, given many advance fee frauds are enabled by their efficient transfer services.⁶¹
- 6.64 The West Australian (WA) Government suggested the Australian Government could also play a more active role in disrupting fraud activities by stationing officers at post offices to monitor suspicious wire transfers, for escalation to consumer protection agencies.⁶²

Industry's cybersafety services to seniors

- 6.65 In addition to requests for government to tighten obligations on industry to protect consumers against cyber threats, the Committee also heard from
-

57 Under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*.

58 See eBay and Paypal, *Submission 11*, p. [2].

59 South Australian (SA) Government, *Submission 37*, p. 16.

60 CIS, *Committee Hansard*, 14 March 2012, p. 5; Dr Cassandra Cross, *Submission 49*, p. 8.

61 The company had allegedly facilitated fraudulent transactions between victims and offenders. See *Committee Hansard*, 6 February 2013, p. 7.

62 Western Australia (WA) Government, *Submission 19*, pp. 5–8.

key industry players about the measures they currently deploy to safeguard the security and amenity of their clients, and senior Australians in particular.

6.66 Telstra Corporation Ltd, Australia's largest ISP, and Facebook, a social network provider to over 10 million Australians, made submissions to the Committee outlining their commitments to the concept of 'digital citizenship' and to empowering seniors to participate actively and confidently in the online community.⁶³

6.67 Facebook and Telstra's submissions made clear the potent market incentives they have to ensure their clients have the best online experience, which includes ensuring high standards of safety and security. Telstra's Mr Darren Kane stated at hearings:

I firmly believe that Telstra wants to ensure that all our customers have the very best online experience. We sell access – that is how we make a profit. We sell services and products that connect people and individuals. If we were to sell a service or product or network access that did not deliver a good online experience, people would not connect with us. Therefore, it is absolutely in our interests to ensure that all of our customers understand the potential online risks. It is also important to understand the positives around the digital world.⁶⁴

6.68 The Committee explored a number of aspects raised as important to seniors' online confidence and the quality of their experience with these and other inquiry participants.

Privacy and security advice

6.69 In previous chapters, the Committee has outlined seniors' online vulnerabilities due to a combined lack of skills and lack of familiarity with internet conventions on social network sites.

6.70 Dr Cassandra Cross, for example, observed:

With seniors in particular, who are somewhat new to the social networking aspect, there is this myth on the part of seniors that things on the internet are true, that there is some sort of filter and that if you read it on the internet then it has to have gone through some sort of accountability or quality control, which we know is

63 Facebook, *Submission 36*, pp. 1–2, Telstra Corporation Ltd, *Submission 22*, pp. 3–4.

64 Mr Darren Kane, Director of Government Relations, Telstra Corporation Ltd, *Committee Hansard*, 23 March 2012, p. 24.

not true at all. There is also this idea that if I am posting something on my social networking site, then only the people I want to see it can see it. Seniors do not necessarily realise that, depending on their security settings, anyone can view the material that they are putting up online.⁶⁵

6.71 In its submission Facebook emphasised its utility to seniors who are using the online network to catch up with family and to seek out friends and information. The submission also set out the range of privacy controls offered by Facebook to empower seniors to enjoy the benefits of social networking safely. These included:

- a Data Use Policy available at sign-up, with new clear format 'sign-up' button and more prominent text and link to the policy;
- a Privacy Control to set restrictions on who can see specific types of information, and interactive tools to learn more about how a user's information appears to others;
- clear links to the Privacy Policy and to the Help Centre, which provides user-friendly, non-legal explanations about privacy; and
- education and partnerships to promote awareness of the importance of the privacy and privacy tools and controls.⁶⁶

6.72 Telstra representatives informed the Committee of recent commitments under its Telstra Connected Seniors initiative, including:

- 30 large-scale training events nationally, aligned to coincide with each State's seniors week;
- cybersafety educational material, self-teach videos and other collateral for the Telstra Connected Seniors website; and,
- production of 'Connected Seniors' DVD Workshop One, and *Mobile Phones Made Easy* and *Life's More Fun When You are Connected* booklets.⁶⁷

6.73 Seniors organisations the ASCCA and Life Activities Clubs Victoria Inc. (LACVI) suggested ISPs could do more to ensure older Australians better understand the range of products and plans, and the security

65 *Committee Hansard*, 6 February 2013, p. 9.

66 Facebook, *Submission 36*, pp. 3–4.

67 Mr Kane, Telstra Corporation Ltd, *Committee Hansard*, 23 March 2012, p. 23.

requirements associated with their use, by providing leaflets on cybersafety advice at sale point.⁶⁸

- 6.74 In Telstra's view, ISPs provide adequate advice on their services to ensure market success, but more education about risks is needed:⁶⁹

I think there needs to be a balanced approach. I do think that there is sufficient information available at point of sale for all users to better understand the online risks. I do think that ISPs and telecommunications providers do provide sufficient information based on my evidence here at Telstra. I also think more can be done to ensure our customers understand why they need to educate themselves to these online risks.⁷⁰

- 6.75 But the CLC maintained that ISPs should be more transparent about costs, product services and risk, providing information at sale and on billing. Telcos should also advise consumers about their rights of complaint to the Telecommunications Industry Ombudsman (TIO) in product information and statements.⁷¹

- 6.76 The Committee notes that the Communications Alliance report *Building Consumer Confidence in the Communications Industry* (2008) observed that the TIO:

... suggests that best practice in respect of providing advice to consumers who query high usage charges should involve discussing different types of usage, such as browsing, file sharing, uploading and downloading, and the effects these can have on a bill, rather than simply asserting that the bill is correct and needs to be paid.⁷²

Defensive web design

- 6.77 Defensive web design aims to reduce the negative experiences of online users to encourage their continued patronage of a website. This involves ensuring content is informative and accessible for its audience but also addresses the technical limitations of a site such as recurring error pages,

68 Australian Seniors Computer Clubs Association (ASCCA), *Submission 7*, p. 5; Life Activities Clubs Victoria Inc. (LACVI), *Submission 5*, p. 2.

69 Mr Kane, Telstra Corporation Ltd, *Committee Hansard*, 23 March 2012, p. 24.

70 Mr Kane, Telstra Corporation Ltd, *Committee Hansard*, 23 March 2012, p. 24.

71 Professor Fraser, CLC, *Committee Hansard*, 23 March 2012, p. 34.

72 Dr E Lally *et al*, *Building Consumer Confidence in the Communications Industry Preparing for the Broadband World*, Report for the Communications Alliance, Centre for Cultural Research, University of Western Sydney, 2008, p. 11.

timing out, broken links and other threats to a user's online ease and enjoyment.⁷³

- 6.78 In Chapter 3, the Committee discussed proposals to improve government services and information portals through web design that is more intuitive to use, and hence protective for seniors.
- 6.79 Seniors' organisations also advised the Committee that online interactions can be frustrating and more risky because of technical design features, such as embedded information, early timing out and a general lack of recognition that different client groups may have different needs.⁷⁴
- 6.80 The Committee heard, for example, that websites with timed access can make senior users rush and make mistakes, or data entered will be lost when the screen suddenly closes.⁷⁵ Seniors could also fall into the trap of making ill-considered commercial, investment or real estate decisions if lengthy terms and conditions were buried within the website, or other key information written in small print.⁷⁶
- 6.81 Increasingly, defensive web design also involves the designing and monitoring of a website to maintain the online safety of its users.⁷⁷
- 6.82 Facebook's submission recounted features of its online infrastructure which are designed to help seniors have a positive and safe online experience. These included a new more user friendly Accounts Settings page, privacy controls, a user authentication policy, a Statement of Rights and Responsibilities, an abuse reporting infrastructure, and an online security framework which detects and blocks malicious activity.⁷⁸
- 6.83 Facebook also advised of its follow up procedure in the event of a client's computer being compromised:

If we detect an account has been compromised because of various factors including suspicious activity or content, the account is automatically reset, the bad content deleted from across Facebook, and the user put in a remediation process. The process includes a McAfee virus scan of the user's machine.⁷⁹

73 Mint Leaf Web Design: Defensive Web Design <www.mintleafstudio.com.au/blog/web-design/item/2011/09/19/what-is-defensive-web-design-and-how-can-you-use-it-> viewed 25 February 2013.

74 CIS, *Submission 26*, p. [5].

75 The Frankston City Ageing Positively Reference Group, *Submission 3*, p. [2].

76 WA Government, *Submission 19*, p. 2.

77 See discussion on defensive web design below for more detail. *Submission 26*, p. 8.

78 Facebook, *Submission 36*, pp. 1, 7.

79 Facebook, *Submission 36*, p. 7.

Product training and technical support

- 6.84 ISPs have recognised there are very significant market opportunities if senior Australians embrace technology in the same measure as younger age groups. This recognition provides tangible incentives to assist older clients with the advice, training and technical support needed to engage confidently with internet enabled devices and services.
- 6.85 Facebook referred to its commitment to introduce senior Australians to the benefits of online social networking. Facebook provides training and advice useful to seniors both online and through education outreach and partnerships. In 2011, Facebook also published a guide for older users *The Facebook Guide for People Over 50*.⁸⁰
- 6.86 Telstra advised that the Telstra Connected Seniors program reflects the corporation's commitment to work with its clients, as Mr Kane stated, 'from cradle to grave'.⁸¹ Mr Kane told of significant achievements under this program to date, with more than 62 000 seniors offered face-to-face training over 2010-11, and 22 000 seniors nationally during 2011-12, featuring cybersafety as a key topic.⁸²
- 6.87 The Committee has referred to research indicating that a growing number of seniors feel more confident using iPads/tablets and smartphones than standard PCs. This may provide a significant impetus for online usage among those aged 55 plus.⁸³
- 6.88 Telstra reported that it has targeted this market in development of a senior friendly mobile phone, the Telstra 'Easy Touch Discovery' phone, which was designed in consultations with senior and disability organisations.⁸⁴ Mr Kane described the features of the phone and its attraction to seniors:

[Easy Touch Phones] have a larger number pad, are more easily explained...We have a touch screen that our assistants in our T-shop retailers will walk through so that seniors understand, if it is their first phone, what the merits of this product are and the services that are available...As they become more confident, we will provide them with other services and products which suit their competence on the net.⁸⁵

80 *Submission 36*, pp. 1 and 2.

81 Mr Kane, Telstra Corporation Ltd, *Committee Hansard*, 23 March 2012, p. 24.

82 Mr Kane, Telstra Corporation Ltd, *Committee Hansard*, 23 March 2013, pp. 26-27.

83 *YOURLifeChoices*, *Submission 38*, p. 4; DBCDE, *Submission 25*, p. 6.

84 Telstra Corporation Ltd, *Submission 22*, p. 8.

85 Mr Kane, Telstra Corporation Ltd, *Committee Hansard*, 23 March 2013, p. 27.

- 6.89 Mr Kane said that seniors are usually offered a basic \$15 plan to cover emergency calls, which is the initial interest for most seniors.⁸⁶
- 6.90 The SA Government observed that the Telstra Connected Seniors program is also one of few initiatives for older people providing training in using new technology, such as iPads, to access the internet.⁸⁷

Computer and security product costs

- 6.91 The Committee has already noted that costs and uncertainty about internet products and security requirements pose significant barriers to seniors who are otherwise interested in using the internet.⁸⁸
- 6.92 Mrs Bosler of ASCCA reported that questions asked by seniors when they come to her computer classes show that fears about costs, and confusion about the range of service providers and service options, are at the forefront of their minds:
- ‘I’d like to use the internet, but I don’t quite know what to do first. What is an ISP? What ISP can I trust? What is going to happen? How am I going to manage paying for it? I have a limited fixed income. I am scared that, if I start using the internet, I might run up bills that I can’t cope with.’⁸⁹
- 6.93 One proposal to help make security products more affordable and reduce uncertainty was that all internet enabled devices, including second hand products, should be sold with security software pre-installed.⁹⁰ The ASCCA suggested these systems should have a default start-up or installation information supplied, or provided at sale point.⁹¹ The LACVI considered that the costs of such protection should be subsidised by the Government to ensure it is maintained and updated as required.⁹²
- 6.94 Other observations were: where costs were prohibitive to security, seniors could potentially benefit by provision of free software from banks;⁹³ market dynamics might be expected to drive down the costs of access and
-

86 Mr Kane, Telstra Corporation Ltd, *Committee Hansard*, 23 March 2013, p. 27.

87 South Australian Government, *Submission 37*, p. 12.

88 See Chapter 5, and for ref: Australian Research Council Centre of Excellence for Creative Industries and Innovation (CCI) *Older Australians and the Internet*, 2011, cited in ACMA, *Submission 24*, pp. 7–8.

89 *Committee Hansard*, 23 March 2012, p. 17.

90 ASCCA, *Submission 7*, p. 5; LACVI, *Submission 5*, p. 2.

91 ASCCA, *Submission 7*, p. 5.

92 LACVI, *Submission 5*, p. 2.

93 AISA, *Submission 32*, p. 10.

security products for seniors;⁹⁴ and the Government could support websites providing free or low cost security software and promote free Cloud data storage available through Google.⁹⁵ The Committee also heard about working public/private partnerships providing second hand computers to seniors with free troubleshooting and maintenance.⁹⁶

- 6.95 The question of cost was not raised with industry during the current inquiry, but the Committee is aware that the House of Representatives Committee on Infrastructure and Communications is currently conducting an inquiry into the costs of IT hardware and security software in Australia compared with overseas.⁹⁷
- 6.96 In referring the inquiry to that Committee, Senator the Hon. Stephen Conroy, Minister for Broadband, Communications and the Digital Economy, noted that consumer advocate Choice had identified a range of products for which prices were approximately 50 per cent higher in Australia than they were elsewhere. Other products cost 90 per cent more in Australia than similar ones in the US.⁹⁸
- 6.97 The Committee looks forward to the results of the inquiry and asks that, in light of its findings, the Government should consider whether price caps or incentives to industry, or subsidies to seniors purchasing IT hard or software, may be warranted to help seniors meet the costs of technology change with confidence.

Raising industry's cybersafety and security awareness

- 6.98 In the previous chapter, the Committee noted that, in 2010, 73 per cent of SMEs had recorded a data breach in the previous year.⁹⁹ That same year, other research found that IT enabled small businesses were twice as likely

94 COTA NSW (Council on the Ageing [NSW] Inc.), *Submission 39*, p. 2.

95 Keith Harvey, *Submission 42*, pp. 5–9.

96 WorkVentures, *Submission 33*, p. 2.

97 *House Hansard*, 29 October 2012, p. 12172; and Inquiry into IT Pricing, House Standing Committee on Infrastructure and Communications, referred 24 May 2012. <www.aph.gov.au/itpricing>viewed 25 January 2013.

98 See *House Hansard*, 29 October 2012, p. 12172.

99 Ponemon Institute LLC: *2010 Annual Study: Australian Costs of Data Breach*, 2010, cited in eBay and PayPal, *Submission 11*, p. [2].

as medium or large businesses to operate without using computer security tools.¹⁰⁰

6.99 As a consequence, the CIS reported that most data loss occurs within SMEs, further noting: 'The majority of SMEs do not have the capacity or capability to really cope with all data they collect'.¹⁰¹

6.100 AISA advised that the problem is not, however, limited to SMEs as many large corporations are not adequately prepared either.¹⁰² The AISA recommended, as a priority, that tertiary educators integrate security principles and skills into their IT courses and subject units to ensure they are seen as core business and not optional:

Security should be an integral part of all information systems procurement, design and development and not perceived purely as a separate discipline. This is unlikely to happen until security is a part of the training for all ICT professionals, and endorsed by business management.¹⁰³

6.101 The Committee heard that industry led security awareness training is being carried by industry and at tertiary institutions. Among others:

- The Abacus-Australian Mutuals, the peak body for ADIs, has a dedicated Fraud and Crimes Team which offers security training to members in partnership with the enforcement community, including the Queensland Police Services, the ACCC, and ACMA.¹⁰⁴
- The CIS offers courses on cyber security and industry awareness at the University of Canberra. In 2012 the Centre launched its 'Surf Between the Flags Internet Safety Roadshow' specifically targeting regional and rural SMEs and end users to help improve online trust and safety in those audiences.¹⁰⁵

6.102 Another issue was the standard of available security products and their cost to business. Existing research suggests that the costs of security products are prohibitively high for small business. In a 2009 study, for example, businesses estimated they had spent \$1.95 billion on computer

100 Small businesses 15 per cent, compared with medium at 6 per cent or large at 4 per cent. K Richards, 'ABACUS: a National Survey', *Australian Institute of Criminology Research and Public Policy Series no. 102*, June 2009, p. 41.

101 Professor Phair, CIS, *Committee Hansard*, 14 March 2012, p. 2.

102 Referring to the Sony PlayStation attacks in 2011, *Submission 32*, p. 9.

103 AISA, *Submission 32*, p. 7.

104 Abacus-Australian Mutuals, *Submission 44*, p. 2.

105 CIS, *Submission 26*, p. 6.

security over the previous year.¹⁰⁶ While these estimates are not verifiable, one conclusion could be that available security solutions are not as effective as they could be.

- 6.103 Submitters suggested that ISO International Standards, developed in Europe for the safety and reliability of products, should be applied to internet security products here.¹⁰⁷ The CIS regarded product safety standards for security products as essential as those for whitegoods.¹⁰⁸ AISA noted the Government's acknowledgement that consumer protection law on the sale of insecure IT products in Australia is currently inadequate. It recommended that Standards Australia be funded to work for better laws internationally and that the ACCC be adequately funded to enforce existing laws.¹⁰⁹
- 6.104 The Committee was also alerted to evolving market-based opportunities for SMEs to improve their capacity to deal with cyber threats through remote outsourced security and fraud services. Cloud 'software-as-a-service' data storage arrangements could also provide SMEs with new and more economical opportunities for improved security.¹¹⁰

Industry/government partnerships for cybersafety

- 6.105 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 in industry and in the broader community.
- 6.106 The AFP regarded information sharing between government and industry as essential to address the numerous challenges emerging in the cybercrime environment, noting:

Technology reliance, combined with the reach and speed of the internet, allows criminal elements to operate from international

106 K Richards, 'The Australian Business Assessment of Computer User Security (ABACUS): a National Survey, *AIC Research and Public Policy Series no. 102*, June 2009, Forward, see data ref. in Abacus-Australian Mutuals, *Submission 44*, p. 1.

107 CIS, *Submission 26*, p. 3, and AISA, *Submission 32*, p. 8.

108 Mr MacGibbon, CIS, *Committee Hansard*, 14 March 2012, p. 8.

109 Ref: *Government Response to the [former] House of Representatives Standing Committee on Communications, Hackers, Fraudsters and Botnets: Tackling the Problem of Cyber Crime: Report of the Inquiry into Cyber Crime*, June 2010, Response to Recommendation 26, and see AISA, *Submission 32*, pp. 10-11.

110 CIS, *Submission 26*, p. 6.

regions with limited regulation or legislation. In this environment, the sharing of information internationally between industry, private sector, government and third-party organisations in an open and timely manner enables law enforcement to protect the community and develop safe strategies against technology enabled crimes.¹¹¹

- 6.107 The AFP reported on the strong partnership it has developed under its cyber awareness ThinkUKnow program, involving State and Territory regulators, the ASCCA and industry partners, such as Facebook, Microsoft Ninemsn and Datacom.¹¹² International enforcement alliances further involve the Australian New Zealand Policy Advisory Agency and the International Liaison Officer Network.¹¹³
- 6.108 The Australian Institute of Crime (AIC) commended the work of the Australasian Consumer Fraud Taskforce (ACFT) in building regional co-operation. The ACFT comprises 22 government regulatory agencies and departments, the private sector, community and non-government partners in Australia and New Zealand.¹¹⁴ Telstra advised that it is the principal industry partner with the ACCC in the ACFT National Consumer Fraud Week, which runs annually in March.¹¹⁵
- 6.109 The ACC reported on recent changes to its establishing legislation that had facilitated its capacity to collaborate with industry, particularly in relation to SOIF schemes. The ACC has worked to ensure industry participants understood and managed the risks of the hacking of legitimate leads market client files. Ms Harfield also emphasised the importance of banks and financial institutions having similar opportunities to discuss risk and vulnerability without commercial damage being done to their industry.¹¹⁶
- 6.110 Telstra saw potential to build on existing engagement between Government and ISPs to address cybersafety risks to seniors under the NBN:

Focusing on the positives that technology brings to people's lives while remaining aware of these risks is an important step to enabling older Australians to achieve the most value from the

111 AFP, *Submission 20*, p. 1.

112 Dr Jenny Cartwright, Co-ordinator, Strategic Initiatives, and Commander Glen McEwen, Manager, Cyber Crime Operations, AFP, *Committee Hansard*, 13 March 2013, pp. 2-3, 6.

113 Commander McEwen, AFP, *Committee Hansard*, 13 March 2013, p. 1.

114 AIC, *Submission 12*, p. 4.

115 Mr Kane, Telstra Corporation Ltd, *Committee Hansard*, 23 March 2012, p. 24.

116 *Committee Hansard*, 15 August 2012, p. 4.

internet. This could be achieved through a partnership between government and industry where industry assistance could be harnessed to deliver cyber-safety and more broadly, ICT training through the government's Digital Economy Strategy.¹¹⁷

Bringing all partners together

6.111 In other chapters of this report the Committee has made recommendations to consolidate crime reportage, information and victim support services to a central reporting and awareness portal. This co-ordination also provides a platform for collation of data on cybercrime trends and impacts on the community.

6.112 The AIC maintained that still more must be done to ensure effective enforcement and policy making are not disabled by the large number of partners involved:

Cybercrime prevention and detection falls within the remit of a large number of law enforcement, regulatory and other government agencies, as well as the private sector. While these organisations may do an admirable job with the resources that they have available to them, there is still a need for greater integration of activities and cooperation between organisations.¹¹⁸

6.113 The cybercrime thinktank CIS's Co-Director Mr MacGibbon stated:

We believe the Australian government can be more robust in engaging content service providers in understanding where the Australian law stands for the collection of evidence and for behaviour online generally. That includes businesses that have no domestic nexus with Australia but are doing business in Australia.¹¹⁹

6.114 It was put to the Committee that a co-ordinating entity, taskforce or figurehead is urgently needed to help raise industry and consumer awareness, to attack the contagion of crime, and defend vulnerable users.

6.115 Professor Fraser, Director of CLC, asked for a central co-ordinator and whole of community taskforce to strengthen existing industry codes and standards, suggesting:

117 Telstra Corporation Ltd, *Submission 22*, p. 8.

118 AIC, *Submission 12*, p. 4.

119 *Committee Hansard*, 14 March 2012, p. 1.

That agency needs to bring all the players around the table: all the law enforcement agencies, the hardware companies, the software companies, the ISPs, the consumer groups, and the representatives of vulnerable groups such as seniors or the young. It needs to bring these actors together to develop interoperable standards and industry codes that will reduce the opportunity for cybercriminals in what is now a very open network which is very vulnerable.¹²⁰

- 6.116 AISA supported this proposal, also asking for establishment of a top level advisory body to bring together government agencies, Australian industry groups and subject matter experts, such as security professionals, social scientists, economists and technologists, to promote the importance of security and compliance to Australian industries.¹²¹
- 6.117 The eBay and PayPal supported establishment of a Consultative Working Party (CWP) to bring together industry experts and key government agencies to improve responses to online and mobile crime during commercial and financial transactions. This body would be important to break down institutional barriers, build sustainable partnerships, and to determine which agency leaders are best suited to work constructively with industry.¹²²

Recommendation 12

That the Australian Government establish a consultative working group, with wide stakeholder representation, to co-ordinate and promote government and industry partnerships and initiatives in support of a healthy and secure online environment.

- 6.118 The Committee considers that an important task of this body will be to examine the effectiveness and promote awareness of relevant industry codes of practice, and make recommendations to all levels of government on these matters. Considerations may extend to clarification of the definitions and content of these codes to ensure industry has input into, and a clear understanding of, the Government's expectations.

120 *Committee Hansard*, 23 March 2012, p. 31.

121 AISA, *Submission 32*, p. 6.

122 eBay and PayPal, *Submission 11*, p. [2].

Recommendation 13

That the proposed consultative working group should examine the effectiveness and promote awareness of relevant industry codes of practice, and make recommendations to governments at all levels on these matters.

- 6.119 This body might also consider related matters such as proposals for industry standards for security products and the cost incentives and disincentives to online security.

Concluding comments

- 6.120 The Committee is convinced that improving cyber security awareness across the community will be essential to ensure Australia reaps the benefits of a digital economy. Equally, the Committee believes that there are sound market incentives for Australian ISPs and businesses to work for the health of the cyber sphere in partnership with the Government and the community.
- 6.121 By adopting defensive IT security practices, one small business can do a lot to reduce contagion across international borders, and potentially prevent long term abuse of a victim of credit card or personal information fraud.
- 6.122 The Committee notes that ACMA's recent report on online business found that successful businesses meet three consumer requirements: value, convenience, and choice. Lack of confidence in the security and safety of the online environment nullifies advantage based on these factors. More confident consumers will engage more, and spend more.¹²³
- 6.123 The Committee's recommendation for establishment of a Digital Economy Taskforce responds to the urgency of bringing together all partners to address the challenges of cybercrime. Senior Australians will be more confident to engage in a healthier, safer and more secure online environment.
- 6.124 The Committee also considers that issues such as the cost of IT hardware and security software might merit further review by the Government, in consultation with industry and consumers, to ensure that price is not a barrier to the community's cybersafety and security.

123 ACMA, *Let's Go Shopping...Online 2011*, October 2011 <engage.acma.gov.au/commsreport/e-commerce/> viewed 25 February 2013.

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.

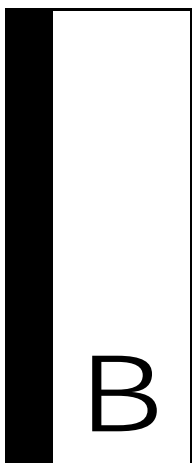


Appendix A — Submissions

- 1 Tandara Lodge Community Care Inc.
- 2 Australian Human Rights Commission
- 2.1 Australian Human Rights Commission
(Supplementary to Submission No. 2)
- 3 Frankston Ageing Positively Reference Group
- 4 National E-Health Transition Authority
- 5 Life Activities Clubs Victoria Inc.
- 6 Australian Library and Information Association Ltd
- 7 Australian Seniors Computer Clubs Association
- 8 Hobart Older Persons Reference Group
- 9 Australian Crime Commission
- 10 Legacy Australia Council
- 11 eBay Australia & New Zealand and PayPal Australia
- 12 Australian Institute of Criminology
- 13 Brotherhood of St Laurence
- 14 Moorook 8 Neighbourhood Watch
- 15 Consumers Health Forum of Australia
- 15.1 Consumers Health Forum of Australia
(Supplementary to Submission No. 15)
- 16 Department of Health and Ageing
- 16.1 Department of Health and Ageing
(Supplementary to Submission No. 16)
- 17 Name Withheld
- 18 The African Seniors Club - Australia Inc.

- 19 Western Australian Government
- 20 Australian Federal Police
- 21 Name Withheld
- 22 Telstra Corporation Ltd
- 22.1 Telstra Corporation Ltd
(Supplementary to Submission No. 22)
- 23 Name Withheld
- 24 Australian Communications and Media Authority
- 25 Department of Broadband, Communications and the Digital Economy
- 25.1 Department of Broadband, Communications and the Digital Economy
(Supplementary to Submission No. 25)
- 26 Centre for Internet Safety, University of Canberra
- 27 National People with Disabilities and Carer Council
- 28 Mr Ken Smith
- 29 National Seniors Australia
- 30 Department of Veterans' Affairs
- 31 University of Technology, Sydney
- 32 Australian Information Security Association
- 33 Work Ventures
- 34 Brisbane Seniors OnLine Association Inc.
- 35 The Allannah and Madeline Foundation
- 36 Facebook
- 37 South Australian Government
- 38 Your Life Choices
- 39 Council on the Ageing NSW Inc.
- 40 Federation of Ethnic Communities' Councils of Australia
- 41 Consumers e-Health Alliance
- 42 Mr Keith Harvey
- 43 Australian Taxation Office
- 43.1 Australian Taxation Office
(Supplementary to Submission No. 43)
- 44 Abacus - Australian Mutuals
- 45 Mrs Joyce M Sheasby
- 46 Australian Securities and Investments Commission

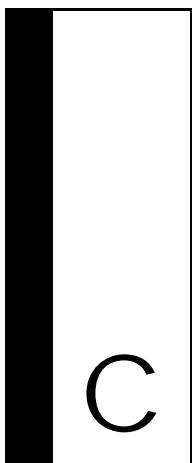
- 47 Stay In Touch Pty Ltd
- 48 CC Medical Offices Pty Limited
- 49 Queensland University of Technology



Appendix B — Exhibits

- 1 Name withheld
Phishing Scam: Big Pond Service Cancellation Notice
- 2 Telstra
Life's More Fun When You're Connected
(Related to Submission No. 22)
- 3 Telstra
Workshop 1: Mobile Phones Made Easy
(Related to Submission No. 22)
- 4 Telstra
How to Explore the World Wide Web
(Related to Submission No. 22)
- 5 Telstra
How to Use Your Mobile Phone
(Related to Submission No. 22)
- 6 Australian Communications and Media Authority
Digital Parenting
(Related to Submission No. 24)
- 7 Australian Seniors Computer Clubs Association
Bridging Research in Ageing and ICT Development
(Related to Submission No. 7)
- 8 Australian Seniors Computer Clubs Association
Additional Information
(Related to Submission No. 7)

- 9 Australian Seniors Computer Clubs Association
Seniors Telecommunication Issues and Concerns
(Related to Submission No. 7)
- 10 Australian Taxation Office
Australian Taxation Office - Refund Status
- 11 Australian Taxation Office
Australian Government No-resident landlord scheme
- 12 Australian Crime Commission
Serious and Organised Investment Fraud in Australia
(Related to Submission No. 9)
- 13 Australian Institute of Criminology
Trends and Issues - Risk factors for advance fee fraud victimisation
(Related to Submission No. 12)
- 14 Australian Institute of Criminology
Australasian Consumer Fraud Taskforce: Results of the 2010 and 2011 online consumer surveys
(Related to Submission No. 12)
- 15 Queensland University of Technology
The Donald Mackay Churchill Fellowship to study methods for preventing and supporting victims of online fraud
(Related to Submission No. 49)
- 16 National Seniors Australia and National Seniors Australia Ltd
Older Australians and the Internet: Bridging the Digital Divide
(Related to Submission No. 29)



Appendix C — Witnesses

Wednesday, 14 March 2012 - Canberra

Centre for Internet Safety

Mr Alastair MacGibbon, Director

Prof Nigel Phair, Director

Wednesday, 21 March 2012 - Canberra

Department of Health and Ageing

Mr Richard Bartlett, First Assistant Secretary, Medical Benefits Division

Mr Russell de Burgh, Assistant Secretary, Office for an Ageing Australia Branch

Ms Elizabeth Forman, Assistant Secretary, eHealth Division

Mr Paul Madden, Chief Information and Knowledge Officer

Ms Sharon McCarter, Assistant Secretary, eHealth Division

Friday, 23 March 2012 - Sydney

Australian Communications and Media Authority

Ms Lesley Osborne, Manager, Digital Society Policy and Research Section

Ms Sharon Trotter, Manager, Security Safety and e-Education Branch, Digital Economy Division

Ms Andree Wright, General Manager, Content, Security, Safety and e-Education Branch, Digital Economy Division

Australian Human Rights Commission

Ms Fabienne Balsamo, Senior Policy Officer

The Hon. Susan Ryan AO, Age Discrimination Commissioner

Australian Seniors Computer Clubs Association

Ms Nancy Bosler, President

Communications Law Centre, University of Technology, Sydney

Prof Michael Fraser, Director,

National E-Health Transition Authority

Mr David Bunker, Head, Architecture

Dr Mukesh Haikerwal, Head, Clinical Leadership Engagement and
Clinical Safety

Telstra Corporation Ltd

Mr James Shaw, Director, Government Relations

Telstra Corporation Ltd, Victoria

Mr Darren Kane, Director, Corporate Security and Investigations;
Telstra's Officer of Internet Trust and Safety

Wednesday, 9 May 2012 - Canberra**Australian Library and Information Association Ltd**

Ms Vanessa Little, President Elect

Friday, 18 May 2012 - Melbourne**Australian Taxation Office**

Mr Bill Gibson, Chief Information Officer, Enterprise Solutions and
Technology

Mr Todd Heather, Chief Technology Officer, Strategy, Planning and
Assurance

Brotherhood of St Laurence

Dr Helen Kimberley, Principal Researcher, Retirement and Ageing/
Research and Policy Centre

Ms Bonnie Simons, Senior Research Officer, Retirement and Ageing,
Research and Policy Centre

Consumers e-Health Alliance

Mr Peter Brown, Convenor

Life Activities Clubs Victoria Inc.

Ms Lindsay Doig, President

Dr Heather Wheat, Secretary

The Alannah and Madeline Foundation

Dr Judith Slocombe, Chief Executive Officer

Ms Sandra Craig, Manager, National Centre Against Bullying

YOURLifeChoices website

Mrs Kaye Fallick, Publisher, Owner and Director

Mr Drew Patchell, Digital Operations Manager

Tuesday, 7 August 2012 - Hobart**Council of the Ageing (Tasmania) Inc.**

Ms Jane Bowman, Peer Education Co-ordinator

Mrs Sue Leitch, Chief Executive Officer

Digital Tasmania

Mr Andrew Connor, Spokesperson

Hobart Older Persons Reference Group

Ms Danielle Walker, Community Development Officer, Community Inclusion Unit, Hobart City Council

Mr Malcolm Grant, Member

Italian Australian Pensioners Welfare Association of Tasmania Inc. Day Centre

Mrs Diana Edwards, Manager

Migrant Resource Centre (Southern Tasmania) Inc.

Ms Monika Dutkiewicz, Home and Community Care Manager

NBN Co.

Ms Lalla McKenzie, Lead Community Account Manager

TasmaNet

Mr Joel Harris, Managing Director

University of the Third Age (Hobart) Inc.

Mrs Jackie Salathé, Committee Member

Ms Catherine Walpole, Database Officer

Individuals

Mr Graziano Ceron

Mrs Karina Ceron

Wednesday, 15 August 2012 - Canberra**Australian Crime Commission**

Ms Belinda Cole, Acting National Manager, Strategic Policy and Stakeholder Engagement

Mrs Karen Harfield, Executive Director, Fusion, Target Development and Performance

Wednesday, 12 September 2012 - Canberra**Department of Broadband, Communications and the Digital Economy**

Mr Abul Rizvi, Deputy Secretary, Digital Economy and Services Group

Mr Chris Drew, Acting Assistant Secretary, National Security and International Branch, Digital Strategy Division

Wednesday, 19 September 2012 - Canberra**Consumers Health Forum of Australia**

Ms Carol Bennett, Chief Executive Officer

Ms Anna Greenwood, Deputy Chief Executive Officer

Wednesday, 10 October 2012 - Canberra**Australian Institute of Criminology**

Dr Rick Brown, Deputy Director (Research)

Ms Alice Hutchings, Senior Research Analyst, Global, Economic and Electronic Crime Program

Dr Russell Smith, Principal Criminologist and Manager, Economic and Electronic Crime Program

Wednesday, 31 October 2012 - Canberra**National Seniors Australia Ltd**

Mr Michael O'Neill, Chief Executive Officer

Ms Sarah Sanders, General Manager, Public Affairs

Individual

Ms Joyce M Sheasby

Wednesday, 6 February 2013 - Canberra

Stay In Touch Limited

Ms Joanne Lambie, Owner, Stay In Touch

Individual

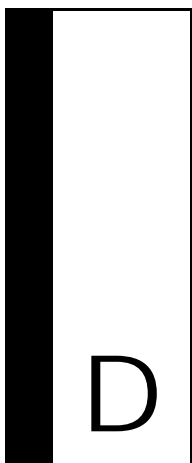
Dr Cassandra Cross, Lecturer, School of Justice, Faculty of Law,
Queensland University of Technology

Wednesday, 13 March 2013 - Canberra

Australian Federal Police

Commander Glen McEwen, Manager, Cyber Crime Operations

Dr Jenny Cartwright, Co-ordinator, Strategic Initiatives



Appendix D — Online survey evaluation

The survey

The Committee launched an online survey for seniors to give as many seniors as possible the opportunity to tell the Committee about their internet use and their concerns, if any, about their cybersafety.

The survey was designed to be as simple to answer as possible so that even people with low computer literacy would be able to complete it without difficulty. It was designed using the 'SurveyMonkey' website¹. The 'SurveyMonkey' summary of the 'response per cent' and 'response count' for each question of the survey is included at the end of this appendix.

Participation in the survey was anonymous. It was designed to take approximately 10 minutes to complete.

All questions had set answers that respondents could choose from as well as an optional free text space for some questions.

Launching and advertising the survey

The Committee launched its Australian seniors' cybersafety survey online on 30 April 2012.

A media release was put out by the Committee announcing the launch of the survey and inviting everyone aged 55 and over to complete it. The survey was advertised in all subsequent Committee media releases during the next six months.

Information about the survey was included in the fortnightly advertisement for Parliamentary Committees in *The Australian* on several occasions.

¹ SurveyMonkey is a free online survey software and questionnaire tool. It can be accessed at <www.surveymonkey.com/>.

The survey was advertised on the Committee's home page of its website and Committee members tried to reach seniors who are not online at home by distributing the survey in hard copy whenever they had the opportunity.

Several seniors organisations and clubs which made submissions to the Committee's inquiry notified their members of the online survey in their member newsletters.

Closing the survey

Initially it was stated on the Committee's website that the survey would close on 30 June. However, at that date the survey was still receiving a steady number of responses so the Committee decided to extend it for a further four months.

The survey was closed on 9 November 2012 at which time it had received 504 online responses and a further 32 responses posted to the secretariat in hard copy.

YOURLifeChoices survey

The Committee received a submission from YOURLifeChoices which is an Australian-based publisher of a website, newsletters and online magazine for people aged 50-75 (submission 38).

YOURLifeChoices told the Committee that it conducted an online survey of members between December 2011 and February 2012. The survey asked 39 questions across a range of topics, with 12 questions being directly relevant to the Committee's inquiry into the cybersafety of seniors online. The YOURLifeChoices survey received 2 563 responses – 65.5 per cent from females, 38.5 per cent from males and 86 per cent of respondents were aged between 50 and 75.

It must be noted that, in the words of YOURLifeChoices, their respondents:

...are not confused, isolated seniors afraid to use the internet. They are active online daily – and keeping up-to-date with new technology. If anything is holding them back, it is probably access to high speed broadband.²

In several places in the following analysis of the Committee's survey, there is some discussion of those responses to those 12 questions from the YOURLifeChoices survey, where relative to the findings of the Committee's survey.

2 YOURLifeChoices website, newsletters and magazine, *Submission 38*, p. 3.

Other research

The Australian Communications and Media Authority (ACMA) published research in late 2012³ which explored some of the same questions which the Committee's online survey of seniors canvassed. ACMA's research covers all age groups and is derived from 'ACMA-commissioned research' from May 2012 and 'Roy Morgan Single Source' research from June 2012. Many of the ACMA research questions were similar to the questions asked by the Committee.

Discussion of responses to the Committee's survey

The total number of responses to the Committee's survey was 536.

In the following discussion about the responses, percentages are mostly used and where a bracketed number follows the percentage, this number refers to the actual number of responses.

Who completed the survey

Slightly more men than women completed the survey, 54.1 per cent (276) to 45.9 per cent (234). This contrasts with the YOURLifeChoices survey which was completed by substantially more women (61.5 per cent to 38.5 per cent).

Just over a quarter of respondents were from NSW (25.5 per cent) but all States and Territories were represented more-or-less appropriately for their population size. Queensland, Tasmania and Victoria contributed 18.8 per cent, 15.7 per cent and 15.3 per cent respectively. The least number of responses came from the Northern Territory with 1.0 per cent (5).

Just a handful (6) of respondents identify as Aboriginal or Torres Strait Islander.

The majority of respondents to the survey live in a metropolitan area – 59 per cent (301). A further 27.5 per cent (140) live in regional Australia, with just 12.9 per cent (66) of respondents living in a rural part of the country and only 0.6 per cent (3) living in 'remote Australia'. Three responses from remote areas is not a credible number to be drawing assumptions from and, therefore, the remote response is not referred to in all cases where metropolitan/regional/rural is discussed below.

How seniors use the internet

Unsurprisingly, 98.5 per cent of people who completed the survey, including those who completed it in hard copy, have a computer at home. Most people are

3 *'Communications report 2011 – 12 series. Report 2 – Australia's progress in the digital economy. Participation, trust and confidence'* Australian Communications and Media Authority, 2012. Viewed on 3 December at: <www.acma.gov.au/WEB/STANDARD/pc=PC_600063>

connected to the internet at home, with 92.6 per cent of respondents 'most frequently' using the internet at home.

The following table shows the age/gender of the 1.5 per cent of people who do not have a computer at home. It is notable that 100 per cent of the two older age groups of women have a computer in their home.

Table 1 Question: Do you have a computer at home?

	Age	Total Number of responses	Respondent has a computer at home	(Number)
Women	55-64	103	97.1 %	(100)
	65-74	90	100 %	(90)
	75 and over	41	100 %	(41)
Men	55-64	60	98.3 %	(59)
	65-74	144	97.6 %	(141)
	75 and over	72	98.6 %	(71)

Source Joint Select Committee on Cyber-Safety – Australian Seniors' cybersafety survey

The survey found that over half of all respondents, 55.8 per cent, use only a computer to access the internet. However, a substantial number sometimes use other technologies to access the internet with 22.9 per cent using mobiles, 20.3 per cent using tablets and 20.1 per cent using smart phones.

In metropolitan areas, only 52.8 per cent of respondents do not sometimes use other technologies to access the internet, whereas, both regional and rural areas were a bit higher with about 59 per cent not using other technologies, and unsurprisingly, none of the three respondents in remote areas are using other technologies to access the internet.

Most respondents, 87.3 per cent, use the internet on a daily basis with 10.1 per cent using it several times a week. About two thirds of respondents (68.3 per cent) access the internet for 15 hours or more per week.

ADSL Broadband is used by the majority of respondents with 68.5 per cent using it and 19.8 per cent using wireless technology.

Over a third of respondents (40.1 per cent) have service problems in their area and more than a quarter (27.9 per cent) experience problems with their access plan.

Unsurprisingly, people who live in metropolitan areas have fewer service problems (33.7 per cent) compared to those in regional and rural areas with 47.1 per cent and 65.6 per cent respectively.

Question 8 asked what seniors are using the internet for and allowed respondents to choose as many answers as they wished. It found that banking and paying bills is the predominant reason for using the internet (76.5 per cent), however, other uses are close behind with 'accessing government services' attracting 63.4 per cent;

entertainment 58.8 per cent; training and research 56.9 per cent; shopping 54.5 per cent; and social networking coming in last (apart from the ‘other’ category) with 41.8 per cent.

A breakdown across the country shows similar responses across metropolitan / regional / rural areas with the most use being for ‘banking and bills’ in all three areas but an especially high use for this purpose in regional Australia. However, a completely different picture is shown in remote areas but this is no doubt due at least in part to the very low number of respondents and, again, no conclusions can really be drawn from the responses of just three people.

Table 2 Question: What do you use the internet for?

Activity	Metropolitan	Regional	Rural	Remote
Accessing government services	64.8% (195)	62.9% (88)	60.6% (40)	33.3 % (1)
Banking and bills	76.7% (231)	84.3% (118)	65.2% (43)	0.0% (0)
Entertainment	62.5% (188)	57.9% (81)	42.4% (28)	0.0% (0)
Shopping	54.2% (163)	55.7% (78)	57.6% (38)	33.3 % (1)
Social networking (Facebook, etc.)	42.9% (129)	41.4% (58)	43.9% (29)	33.3 % (1)
Training and research	58.8% (177)	59.3% (83)	47.0% (31)	100.0% (3)
Other	40.9% (123)	32.1% (45)	37.9% (25)	33.3 % (1)

Source Joint Select Committee on Cyber-Safety – Australian Seniors’ cybersafety survey

The ACMA research, referred to above, also found that:

Activities relating to communications, research and information, and banking and finance have typically dominated the online activity profile of Australian internet users ...⁴

Most seniors who are online believe that internet access is now important to the quality of their life. Just 6.5 per cent said that internet access is not important to the quality of their life. Comments on this question included:

4 ‘Communications report 2011 – 12 Series, Report 2 – Australia’s Progress in the Digital Economy. Participation, Trust and Confidence’, Australian Communications and Media Authority, 2012, p. 14.

Keeping in touch with friends and relatives and the news of the world is important to me. Online shopping is less so.

I live in an isolated area with almost no neighbours and because of the distance, rarely go to towns. Thus internet is often my only contact with the world.

The internet is extremely important to my quality of life as I have very limited mobility.

Mobile wireless internet enables me to operate my business from anywhere in Australia.

It's hard to imagine life without it now.

We keep in touch with our children and grandchildren interstate. Keep in touch with friends. Keep our brains working by playing games etc.

I have an enquiring mind and always want to know more. So information about places visited & to be visited is important to me, to keep my mind active.

It is especially important in keeping track of our investments.

Keeps you in touch with the world, their news and affairs.

The Committee asked if respondents were aware of friends, relatives or other contacts aged 55 and over who do not use the internet (question 19). Only 17.0 per cent of respondents said they do not know anyone 55 or over who does not use the internet.

Asked the reason why people they know over 55 do not use the internet two answers dominated the responses: 40.4 per cent are 'not interested' and 35.8 per cent have a 'lack of skills'.

There is no point in breaking these responses down by the respondent's age and gender because we do not know the age or gender of the people who do not use the internet.

How seniors acquire their online skills

Respondents were asked where they acquired their computer skills. The question allowed as many answers as applied to be ticked. Almost all respondents indicated that they learned through a mix of the available options with 78.2 per cent being primarily 'self-taught' and 53.9 per cent learning at least some of their skills 'at work'. 'Computer courses' and 'friends and family' also had significant responses with 35.3 and 33.6 per cent respectively.

A breakdown of these figures shows that men tend to be 'self-taught' more than women and women learn from 'friends and family' more than the men. In both

cases, many people in the age group 55-64 have learned at least some of their computer skills at work.

In all age groups learning by computer courses comes a long way behind being self-taught or learning from friends or family or at work.

As respondents could chose as many answers as applied, in the tables below total numbers far exceed the actual number of respondents in each group.

Table 3 Question: Where did you acquire your computer skills?

	Age	Number	Self taught	Friends or family	Work	Courses
Women	55-64	103	77.7% (80)	30.1% (31)	69.9% (72)	40.8% (42)
	65-74	90	75.6% (68)	45.6% (41)	58.9% (53)	44.4% (40)
	75 and over	41	61.0% (25)	63.4% (26)	22.0% (9)	29.3% (12)
Men	55-64	60	81.7% (49)	21.7% (13)	70.0% (42)	36.7% (22)
	65-74	144	80.6% (116)	26.4% (38)	53.5% (77)	34.7% (50)
	75 and over	72	86.1% (62)	31.9% (23)	31.9% (23)	26.4% (19)

Source Joint Select Committee on Cyber-Safety – Australian Seniors' cybersafety survey

In the following table slight differences about location and learning emerge.

In metropolitan areas being self-taught or acquiring computer skills at work are the two dominant ways of learning. Learning via 'friends and family' and 'courses' are about half as popular as self-taught and work.

In regional areas, the percentage of people who are 'self-taught' is quite a bit higher than in the other areas and it is far ahead of 'work', 'friends and family' and courses.

In rural areas 'self-taught' is less used than the other areas but rural seniors are the heaviest users of courses as a method to learn about the internet and rural seniors are least likely to rely on 'friends and family' than other groups.

Table 4 Question: Where did you acquire your computer skills?

Place of learning	Metropolitan	Regional	Rural
Work	59.8% (180)	45.7% (64)	48.5% (32)
Self-taught	78.1% (235)	83.6% (117)	71.2% (47)
Friends and family	33.2% (100)	38.6% (54)	25.8% (17)
Courses	31.2% (94)	42.1% (59)	48.5% (32)
Computer club	9.3% (28)	8.6% (12)	1.5% (1)
Seniors' kiosks	3.0% (9)	2.9% (4)	0
Other	6.3% (19)	3.6% (5)	4.5% (3)

Source Joint Select Committee on Cyber-Safety – Australian Seniors' cybersafety survey

Asked if they find accessing information and/or conducting transactions on the internet difficult or frustrating, 71.8 per cent of responding seniors answered 'no'. This response was more-or-less consistent across all regions of the country but when viewed by age and gender it is apparent that women of all age groups find accessing information and/or conducting transactions on the internet more difficult and/or frustrating than men in the same age group. For women 75 and over, the 'yes' response is nearly as high as the 'no' response. There is a definite increase in frustration and/or difficulty with age for both men and women.

Table 5 Question: Do you find using the internet difficult or frustrating?

	Age	Yes	No
Women	55-64	23.3%	76.7%
	65-74	37.8%	62.2%
	75 and over	48.8%	52.2%
Men	55-64	11.7%	88.3%
	65-74	27.8%	72.2%
	75 and over	31.9%	68.1%

Source Joint Select Committee on Cyber-Safety – Australian Seniors' cybersafety survey

Comments were sought about what would help to make accessing information less difficult or frustrating and 140 people entered a range of comments, a few of which follow:

I often wish they do not assume the user is completely computer literate.

The sites I experience most difficulty with are government sites. Since they appear to have a high volume of traffic which invariably exclude access, I feel the government could/should make extra provisions for this.

Many websites have very complex paths just to get into.

I think that seniors generally need some centre where they can access information on how to use it, not to the extent of training courses, but the sort of thing where you can go and type in a question and receive a simple explanation. For instance, a question I recently got answered through TechTalkRadio was what is an Android? What is an App? etc.

Some websites seem to be more difficult to use than they need to be. Maybe those that set them up don't use them.

Community training access in small groups to learn from each other.

More basic knowledge.

Some form of standardisation of terminology across sites would help, e.g. do the terms pin, password, access number, mean the same thing? And many sites seem just to go around in circles. I think those who design some of the sites are too close to their own work and do not realise that many people do not understand the technical terms that they use.

Better web page design. Response from so-called "help desks".

Plain English and developers understanding the needs and limitations of Seniors.

A help line for basic questions/problems.

Some sites are difficult to navigate. Worst problem is use of unfamiliar language.

How safe do seniors feel when online?

Asked if they are worried about online safety risks, 67.0 per cent, answered that they are 'aware but not worried'. However, 25.7 per cent answered that they are 'aware and very worried'.

A similar question in the YOURLifeChoices survey asked if people have enough information to protect themselves from being scammed and the response found that 77 per cent believe that they do have sufficient information to protect themselves from being scammed.

The survey found that 95.5 per cent of respondents have installed security systems and anti-virus software on their computers. Furthermore, 87.2 per cent regularly update their internet security. The following table breaks these percentages down by gender and age group.

Table 6 Question: Are you worried about online safety?

	Age	Number	Aware but not worried	Aware and very worried	Have installed anti-virus software	Update internet security regularly
Women	55-64	103	62.1%	32.0%	96.1%	83.5%
	65-74	90	60.0%	33.3%	96.7%	87.8%
	75 and over	41	61.0%	26.8%	92.7%	75.6%
Men	55-64	60	75.0%	16.7%	95.0%	93.3%
	65-74	144	68.1%	26.4%	97.9%	93.1%
	75 and over	72	70.8%	16.7%	91.7%	83.3%

Source Joint Select Committee on Cyber-Safety – Australian Seniors' cybersafety survey

Table 6 above indicates that women are more worried about online safety than men in all age groups but they are protecting themselves with anti-virus software in about the same percentages as men across all age groups. However, women are slightly less vigilant about updating their internet security regularly than men.

A look at these responses in the context of the regions of Australia shows that rural and regional Australians feel less confident with about 60 per cent in both groups responding that they are 'aware but not worried' against 70 per cent answering 'aware but not worried' from those living in metropolitan areas.

Asked if password requirements are a problem, 73.8 per cent of respondents do not find password requirements to be a problem, leaving over a quarter at 26.2 per cent who do find password requirements to be a problem. The group who find password requirements a problem the most is the 'women 75 and over' group with 34.1 per cent answering 'yes'. The next highest is the 'men 55-64' group answering 'yes' 28.3 per cent. All other groups ranged between 24.4 and 26.4 per cent.

Again, looking at these responses in the context of the country's regions there is almost no difference between those living in metropolitan, rural or regional areas, with about 7.3-7.4 per cent in each group answering 'no' to finding password requirements to be a problem.

Scams and internet fraud

Question 16 asked if the respondent has been personally affected by e-mail scams, identity theft or other internet related fraud and 75.3 per cent responded that they had not, leaving 24.7 per cent (131) who have been personally affected by scams or internet related fraud.

Looked at across the regions of Australia, metropolitan and regional areas were the same with 76.4 per cent of respondents saying they have not been personally affected by scams, and in rural areas the 'no' response dropped to 66.7 per cent.

Asked about the 'type' of scams or fraud experienced it emerges that 'Phishing: for example donations, inheritance, banking scams and lottery scams' is the scam which most people have experienced, with 73.8 per cent responding in the affirmative. This was the same for all regions of Australia. However, the second highest type of scam, 'malicious software installed on computer' was particularly high in rural Australia with 42.9 per cent as compared to 29.4 per cent in metropolitan areas and 31.3 per cent in regional areas.

The following table breaks the responses to these questions down by age and gender. The figures confirm evidence that the Committee heard during its inquiry that it is men in the 50-70 age group who are more vulnerable to internet fraud than women or older men. It is also interesting to note that men have been caught up in 'romance or dating' scams twice as often as the women in all age groups.

Table 7 Question: Have you been affected by e-mail scams, identity theft or fraud?

	Age	Number	Yes	Phishing scams	Malicious software	Romance or dating
Women	55-64	103	18.4%	77.8%	27.8%	11.1%
	65-74	90	22.2%	89.5%	26.3%	10.5%
	75 and over	41	22.0%	44.4%	22.2%	11.1%
Men	55-64	60	33.3%	88.9%	44.4%	22.2%
	65-74	144	33.3%	70.2%	31.9%	23.4%
	75 and over	72	16.7%	58.3%	33.3%	25.0%

Source Joint Select Committee on Cyber-Safety – Australian Seniors' cybersafety survey

The YOURLifeChoices survey asked if respondents had been the target of a scam and reported that 53.4 per cent believed that they had been the target of a scam but the follow up question "did you lose money or time due to the scam" found that only 14.3 per cent responded affirmatively. This figure is considerably less than that of the response to the Committee's survey which can be attributed to the wording. Some people might consider they have been 'affected' even without the

loss of time or money, possibly because they found it stressful to be targeted in this way.

YOURLifeChoices pointed out that even though 'only' 14 per cent of those targeted by scams lost money, confirming that most older internet users know enough to prevent themselves from being scammed, 14 per cent of those targeted is far too high 'considering that cybercrime robs individuals of their time, damages their emotional wellbeing and costs them, in many cases, significant amounts of money'.⁵

Question 18 asked if those affected by scams or fraud had reported the incident to a regulator or the police and found that just over half had not, with 43.3 per cent saying that they reported the incident. The same question was asked in the YOURLifeChoices survey and received a similar response with 42.3 per cent saying that they reported the scam or fraud.

The YOURLifeChoices survey also asked why respondents had not reported scams or fraud and their breakdown of anecdotal responses found that of 701 responses, 153 people handled the matter themselves; 100 did not know how to report it; 75 felt it was not worth reporting; 65 said 'other' and 234 did not give a relevant answer. Therefore, in this instance about 15 per cent of people who were the target of a scam but did not report it, did not do so because they did not know how to report it.

The Committee also asked for comments at question 18 and received 60, several of which follow:

The police told me there was nothing they could do and to just ignore the problems. So I did not report the next incidences. But I change password and other details on my computer.

I reported it to one of the Microsoft tech agents. The trouble is that us oldies usually can't afford security agents you pay for, and can inadvertently not have enough security by accessing their own freeware (which is what had happened to me). It cost me \$150 to have my computer cleaned up. Admittedly, this is the only time in the last 14 years, and I lost no other money. ... Most of us just don't understand all the different terms fully enough to avoid all the pitfalls.

I reported the scam to Hotmail and they automatically closed my account with the consequence I lost all my contact details. Very frustrating. No help was offered.

Wouldn't know to whom to report. Usually, police are not interested and they always claimed that they are too busy!

5 YOURLifeChoices website, newsletters and magazine, *Submission 38*, p. 4.

Seniors' perception of government involvement

Question 21 asked if respondents are comfortable about accessing government information and services online – 89.5 per cent answered 'yes' with only 10.5 per cent answering 'no'. This figure was the same within one percentage point in all areas (excluding 'remote' for reasons previously explained).

As the table below shows, those in the older age groups are slightly less comfortable about accessing government information and services online.

Table 8 Question: Level of comfort accessing Government information/services online

	Age	Yes	Number	No	Number
Women	55-64	94.1%	96	5.9%	6
	65-74	88.8%	79	11.2%	10
	75 and over	75.6%	31	24.4%	10
Men	55-64	90.0%	54	10.0%	6
	65-74	92.4%	133	7.6%	11
	75 and over	84.5%	60	15.5%	11

Source Joint Select Committee on Cyber-Safety – Australian Seniors' cybersafety survey

The same question also asked if the availability of 'telephone or over the counter advice' is important to the respondent and 82.4 per cent said that it is, with 17.6 per cent answering 'no'. Those percentages were fairly consistent with all age groups and both genders with the exception of 'males 55-64 years of age'. Only 68.4 per cent (39) of this group answered 'yes' while 31.6 per cent (18) responded that the availability of telephone or over the counter advice is not important to them. Again, all areas were within one per cent of the average.

Approximately one third of the total number of respondents made a comment here (177). Unsurprisingly, most comments are in defence of the availability of telephone or over-the-counter advice. A few follow:

Increasing use of automated services when phoning government departments is extremely frustrating and annoying.

Personal contact is very important and should never be undervalued.

Telephone and over the counter advice is essential as (a) fall back where online services are incomplete and (b) where personal circumstances require more specific information.

I find a personal response to questions much more satisfying and generally only needs one call rather than going back and forth on computer.

I would be very comfortable accessing Government services online - if only I could. But apparently it is the volume of use that has consistently blocked my access.

I prefer to speak with a real person, computer is totally inflexible and lacks one on one understanding.

I would use the phone in favour of the internet if there was not such a long waiting time for most of these services. Generally I find the internet quicker and have not had problems with it, but I prefer to talk to a warm body!

Education about cybersafety and regulation

Of those who answered question 23 (516), 74.8 per cent believe that a multi-media campaign about cybersafety targeting seniors is required; 86 per cent believe that communication technology producers/vendors should be required to provide cybersafety advice at point of sale; and 98.3 per cent of respondents believe that businesses and online service providers should be required to meet standards for the privacy and security of user data. These responses were consistent across the age and gender groups with just slight variations. There was some difference between the locations, with metropolitan and rural having similar responses but regional Australia having a higher 'yes' response in each case, as the following table demonstrates:

Table 9 Questions on Education and regulation

Question	Metropolitan		Regional		Rural	
	Yes	No	Yes	No	Yes	No
Is a multi-media campaign about cybersafety targeting seniors required?	72.8%	27.2%	79.3%	20.7%	75.8%	24.2%
Should communication technology producers/vendors be required to provide cybersafety advice at point of sale?	85.0%	15.0%	89.3%	10.7%	86.4%	13.6%
Should businesses and online service providers be required to meet standards for the privacy and security of user data?	98.3%	1.7%	99.3%	0.7%	97.0%	3.0%

Source Joint Select Committee on Cyber-Safety – Australian Seniors' cybersafety survey

Finally, question 24 asked 'how can government better protect consumers, and help them protect themselves online'. There were 328 responses to this and many

of these responses have been used to inform the appropriate report chapter. Below is a small selection of comments:

Raise awareness. Maybe require all internet ready hardware sold in Australia to include a one page summary of security "dos and don'ts".

Require a mandatory Computer Driver's Licence when you buy a new computer such as exists in the EU.

Give them knowledge, via classes or online. Reliable knowledge (not just scare-mongering), on how to install free protective software, to update it, run it etc. plus other practical ways to protect themselves - keep it simple! How to do simple computer housekeeping, to maintain computer health, backup files etc.

Provide user friendly information that is easily accessible.

Education and easy access to training, eg TAFE, or someone coming to clubs.

Do not assume that protecting consumers is a one-off project. Education and information directed at the whole community (not just seniors) should be an on-going activity. Threats change, technology changes, people change. The government needs to treat online safety in the same way as any other social issue such as road safety, health, consumer affairs, finance/banking and building codes.

Restrictions do not seem to work with cyber technology, so it seems that education, clear, simple and targeting everyone, is needed.

Certainly not a major television and press campaign. Use existing services like pension updates and material already sent to seniors.

Governments should stay completely out of this area and leave it to the market.

More media info could be useful & for close family members to talk to their more elderly relatives.

Require hardware be sold with antivirus software included, not an optional add-on (potentially not added-on by the unwary), or at least an opening window/pop-up warning if there is no security system (or has not been updated for some time)

Prosecute the scammers and give hefty penalties - not fines which they will never pay.

Practical education resourcing instead of mountains of pamphlets, advertisements and talk. Give the seniors a "voucher" to spend on computer education.

It really is up to the individual to be aware of pitfalls and scams. ... Might be older but still capable of thinking for myself and keeping watch.

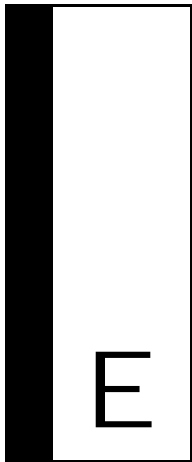
Concluding comments

No hard-and-fast conclusions can be drawn from only 536 responses to a nationwide survey of people aged 55 and over. However, the Committee believes that the online survey was a worthwhile exercise because the results have provided some evidence of trends regarding how seniors use the internet including: where they most often use the internet; for what purposes; how often they use it; and what their experiences have been with the technology, service providers, education opportunities and scams. Results have also provided some insight into the differences between metropolitan, regional and rural users as well as some interesting differences between age groups.

Unfortunately, the survey attracted very few responses from seniors who either do not use the internet, or who may use it a little but are not confident enough to complete an online survey. However, that cohort of seniors was well represented in this inquiry by the many organisations and individuals who made submissions and gave evidence to the Committee in person – as discussed in the body of this report.

In various places throughout this report, the results from the survey have been used to inform and/or complement reporting on the evidence the Committee gathered over the course of its inquiry.

Finally, the Committee would like to thank everyone who took the time to complete the survey.



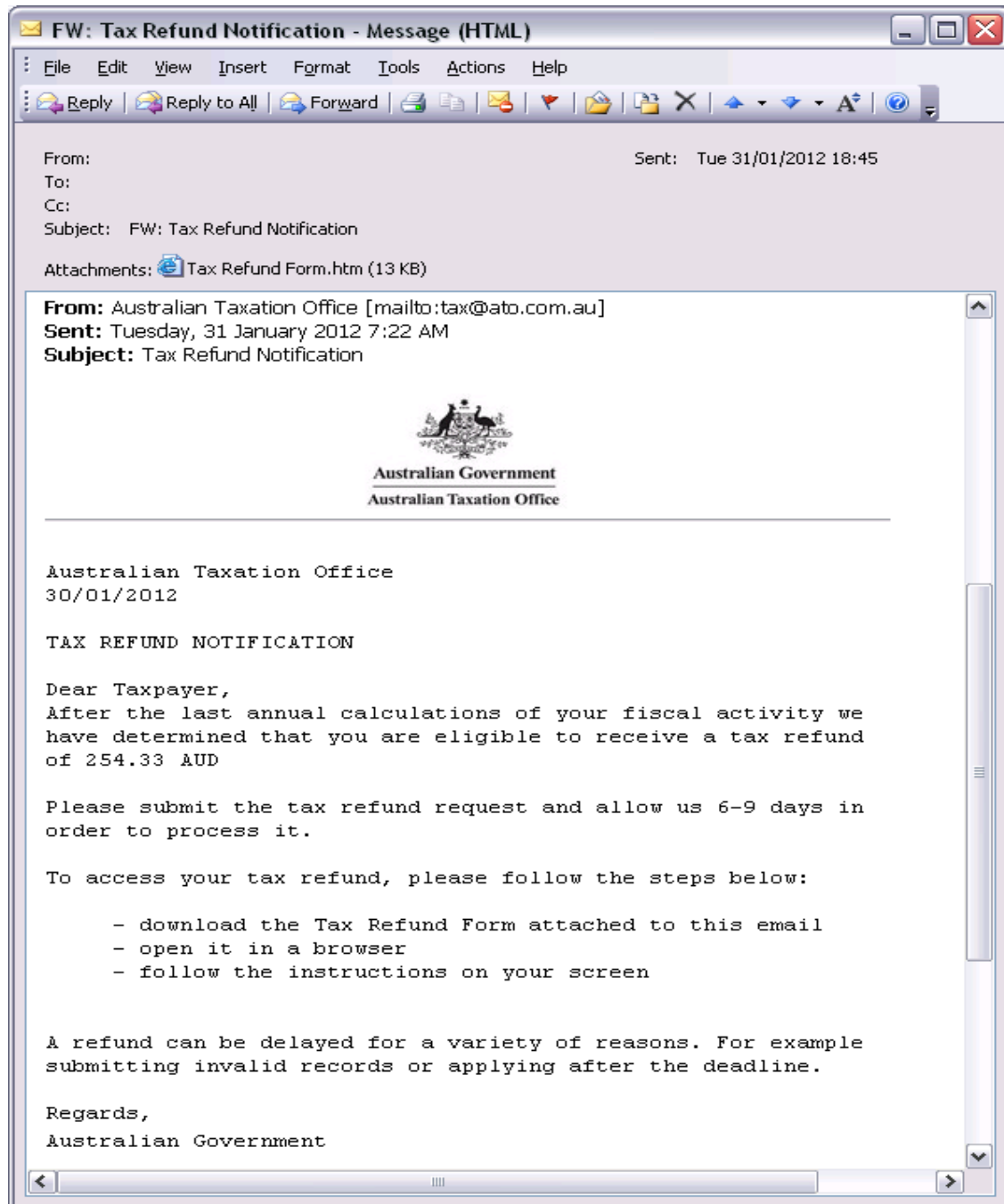
Appendix E — Online resources

Among the many useful online resources that the Committee identified during the inquiry, a selection is listed below:

- Australian Competition and Consumer Commission (ACCC)'s SCAMwatch: www.scamwatch.gov.au/content/index.phtml/itemId/693900
- ACCC's *The Little Black Book of Scams*: www.accc.gov.au/content/index.phtml/tag/littleblackbookofscams
- Australian Communications and Media Authority's Cybersmart website: www.cybersmart.gov.au
- afinerday.com, secure network for seniors: www.afinerday.com/index.php
- Australian Securities and Investments Commission's MoneySmart website, over 55s page: www.moneysmart.gov.au/tools-and-resources/information-for/over-55s/your-money
- Carindale Police Citizens Youth Club's Seniors Online Security Project: www.carindalepcyc.org.au/news.php?display_news=true&news_id=60
- CERT Australia (National Emergency Computer Response Team), single point of contact for cyber security for Australian businesses: www.cert.gov.au
- Department of Broadband, Communications and the Digital Economy: Stay Smart Online www.staysmartonline.gov.au
- Department of Families, Housing, Community Services and Indigenous Affairs: Broadband for Seniors website: www.necseniors.net.au/kiosk-information/staying-safe-online/
- Telstra Connected Seniors: www.telstra.com.au/telstra-seniors
- ThinkUKnow Australia, developed by the Australian Federal Police and Microsoft Australia: www.thinkuknow.org.au/site/index.asp

Appendix F — Phishing Scam

ATO Submission: Example of 2012 phishing e-mail



This phishing e-mail was sent in 2012. This attack used an official looking e-mail with directions to open an attachment. The attachment redirected users to an ATO branded phishing website. This e-mail was set-out more clearly than previous e-mails with clear instructions.

