5

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 Minster 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* <ww.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' 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> 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#ixzz2KlUGrMG8> 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 by14 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 disproportionally 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: Tacking 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 4*1, 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 safety 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 (AISA) 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 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 McGibbon, 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.