6

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 disproportionally 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, C*ommittee 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, C*ommittee 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 Y*OURLifeChoices, 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.