8

Consumer Protection

Introduction

8.1 This chapter canvasses aspects of the consumer protection regime that relate to cyber crime. The Federal, State and Territory consumer protection bodies are increasingly dealing with the violation of consumer protection laws perpetrated over the Internet. The first section focuses on the Australian Competition and Consumer Commission's role in the enforcement of the *Trade Practices Act 1974* (Cth). In particular, the challenge of international enforcement of domestic consumer protection laws.

8.2 The discussion in the remaining sections move beyond the status quo and discuss strategic consumer protection interventions that have the potential to better protect ordinary end users from cyber crime:

- a requirement for informed consent and penalties for unauthorised installation of software;
- IT vendor information standards to promote e-security;
- the problem of insecure IT products; and
- industry standards to promote higher level security settings to better protect consumers.

Australian Competition and Consumer Commission

8.3 The Australian Competition and Consumer Commission (ACCC) administers the *Trade Practices Act 1974* (Cth) and has a responsibility to

protect consumers from economic harm: 'This includes conduct that is fraudulent and has the purpose of misleading consumers for financial gain'.[1]

8.4 The ACCC received 77,000 complaints in the 2008-2009 financial year. Of these, 18,000 related to scams of all types. Scams perpetrated over the Internet accounted for 12,000 of these complaints.[2]

8.5 The Committee noted that many complainants reported fraudulent conduct that also involved the proliferation of malware, such as via phishing emails.[3] As has been noted throughout this report, the combination of cyber crime techniques involving crimes and civil wrongs is often difficult to disentangle and requires strategic policy and enforcement intervention.

8.6 Finally, in line with the Government's overall strategy, the ACCC emphasise the importance of consumer education (see Chapter 10). The ACCC also hosts the *SCAMwatch* website, which provides public information, alerts and access to complaints mechanisms on a wide range of consumer scams, including scams perpetrated online (see Chapter 5).

International and Domestic Cooperation

8.7 The ACCC identified cross agency information sharing and cooperation and, where appropriate, enforcement action, as key elements of their approach.[4] Where online scams impact on consumers in multiple jurisdictions, domestic and international cooperation was described as crucial.[5]

8.8 To this end, the ACCC chairs the Australasian Consumer Fraud Taskforce (ACFT), which includes 20 Commonwealth and State agencies, departments and research institutes as well as the New Zealand Ministry of Consumer Affairs and the NZ Commerce Commission.[6] The Committee was told that the ACFT provides a mechanism for sharing information on enforcement activities as well as educative and information campaigns, and is also involved in research on consumer fraud.[7]

---

1 ACCC, *Submission 46*, p.2.
2 ACCC, *Submission 46*, p.3.
3 ACCC, *Submission 46*, p.3.
4 ACCC, *Submission 46*, p.2.
5 ACCC, *Submission 46*, p.6.
6 ACCC, *Supplementary Submission 46.1*, p.7.
7 ACCC, *Submission 46*, p.5.

8.9 In 2009 the ACCC worked with a number of other agencies:

> Domestically, the ACCC has worked with the Australian Federal Police, Australian Communications and Media Authority, Australian Securities and Investments Commission, Queensland Police, Australian Taxation Office and the state and territory offices of fair trading. Internationally, the ACCC has worked with the United States Federal Trade Commission and the Washington State Attorney-General's office.[8]

8.10 The Committee was told that the ACCC will often refer alleged scam matters to other agencies or organisations. This may occur at the first point of contact or be more formal or take place in one of the less formal forums for discussion and information sharing.[9] However, while the ACCC 'records the handling of each complaint' there were no statistics that differentiate the different types of referrals. Consequently, the Committee was unable to ascertain the number of matters referred for criminal prosecution by Australian authorities.[10] It was noted in Chapter 5, that the NSW Police believed that while a lot of resources are devoted to online scams, there are few criminal prosecutions (as opposed to civil enforcement action).[11] A more centralised approach to complaint handling across a wider range of cyber crime types is discussed in Chapter 5.

8.11 Broader international liaison is facilitated through the International Consumer Protection and Enforcement Network (ICPEN), a network of over 30 national fair trade agencies mainly from OECD countries. The ACCC took over the Presidency of ICPEN in August 2009 for 12 months.[12] The objectives of ICPEN include sharing best practices in legislative and other measures for effective consumer protection enforcement; taking action to combat cross border breaches of consumer protection laws; and facilitating effective cross border remedies.[13]

8.12 The ACCC also has a bilateral agreement with the US Federal Trade Commission on Mutual Enforcement Assistance in Consumer Protection Matters. This MOU provides a detailed elaboration of the obligations of

---

8 ACCC, *Supplementary Submission 46.1*, p.1.

9 ACCC, *Supplementary Submission* 46.1, p.1.

10 ACCC, *Supplementary Submission 46.1*, p.1.

11 Detective Inspector William van der Graff, NSW Police Force, *Transcript of Evidence*, 8 October 2009, p.77.

12 ACCC, *Submission 46*, p.6.

13 See Article 4 (a) to (f) of Memorandum on the Establishment and Operation of the International Consumer Protection and Enforcement Network, agreed to at the Conference in Jeju, Republic of Korea, 26-28 March 2006.

both parties to cooperate to ensure effective enforcement of consumer protection laws in both countries.[14] On the question of Australia – US cooperation, the ACCC advised that the US passed the *Undertaking Spam, Spyware and Fraud Enforcement with Enforcers Beyond Borders Act 2006*, which broadened the US powers to reciprocate information sharing and collection of information and evidence for foreign agencies.[15] It was submitted that the bilateral agreement did not require any strengthening at this stage.

8.13 In addition to the US, the ACCC also has MOUs to facilitate international cooperation with other counterparts, including with agencies in the UK, Korea and New Zealand.[16]

Litigation Issues – Online Scams

8.14 The Committee was told that whether enforcement action under the *Trade Practices Act 1974* (Cth) is taken in Australia will often depend on jurisdictional and evidential issues. Jurisdictional issues arise when the offender is located outside Australia, and, in some cases, the difficulty of ascertaining the identity and location of scam promoters can make enforcement more difficult.

8.15 Some of the issues identified were:

- if the ACCC requires further evidence it would ordinarily use its statutory powers but cannot serve those notices in other jurisdictions;
- court documents need to be served on parties outside the jurisdiction. This requires leave of the court and then service of documents in the relevant country once the relevant respondent is located; and
- the utility of orders the ACCC may seek from a court may be undermined by the difficulty in enforcing those against the respondent.[17]

8.16 While these challenges are present in a number of consumer protection genres, the ACCC said such problems are particularly prevalent in the online scam environment.[18]

---

14 Available at <http://www.ftc.gov/os/2000/07/ftcacccagrmnt.htm>, viewed 10 April 2010.

15 ACCC, *Supplementary Submission 46.1*, p.14.

16 ACCC, *Supplementary Submission 46.1*, p.14.

17 ACCC, *Supplementary Submission 46.1*, p.1.

18 ACCC, *Submission 46*, p.1.

8.17 Out of approximately 12,000 complaints of online scams in the 2008-2009 financial year there were only two matters in 2009 concluded by the ACCC. The two cases categorised by the ACCC as 'cyber crime or cyberscam activity', were referred to the ACCC from the US. The ACCC said that 'assistance in providing information about conduct based in Australia affecting consumers more generally' was influential in the decision to pursue the matters.[19]

8.18 One earlier example where the ACCC had a measure of success was the 2003 *Sydney Opera House Case,* which involved a fraudulent website hosted and administered from overseas that purported to be the official booking site for the Sydney Opera House. Consumers in the UK and Europe had been caught by the fraudulent site. In August 2003, the Federal Court declared that the site was illegal and, although the injunction could not be formally registered in the US, the court accepted that Australian orders would support Australia's request for assistance from the US Federal Trade Commission.[20]

8.19 Even where an alleged perpetrator is outside the country there are sometimes opportunities to use Australian enforcement orders against them within this jurisdiction. The ACCC said:

> The ability to quickly transfer funds and the propensity to morph and phoenix without the same reputational issues mainstream traders have make effective enforcement orders very important. Court orders may be sought to secure assets in Australia, such as funds in bank accounts, to ensure money is available for consumer redress.[21]

8.20 In 2009, the *Designer Brand Outlet Case,* a matter referred by the US Federal Trade Commission (FTC) in June 2008, was concluded and serves as a useful case study (see below).[22]

---

19 Mr Scott Gregson, Group General Manager, Enforcement Operations, ACCC, *Transcript of Evidence,* 18 November 2009, p.6.

20 ACCC, *Submission 46*, p.7.

21 ACCC, *Supplementary Submission 46.1*, p.3.

22 *ACCC v Bindert (Ben) Loosterman & Ors* FCA 1391/2008; Resolved by consent with final orders available on the Federal Court Website at: <https://www.comcourts.gov.au/file/Federal/P/NSD1391/2008/3549912/event/25652026/document/150771>, viewed 10 April 2010.

ACCC v Bindert (Ben) Kloosterman & Ors

The FTC provided the ACCC with a number of consumer complaints. In addition, the ACCC also received complaints from consumers in the United Kingdom and a number of Australian states. The complaints variously related to Designer Brand Outlet accepting payment and not delivering the goods, goods received not matching the goods ordered (including issues relating to authenticity), refunds not provided and consumers unable to contact the company.

The investigation included liaison with international counterparts, a major Australian bank responsible for the credit merchant facilities for the website and Australian Domain Registrar, Netregistry Pty Ltd, in relation to the registration of the website.

In September 2008, the ACCC sought interim injunctions against the operators of the website, Mr Bindert (Ben) Kloosterman and Ms Xin Fang (Lucy) Shi, and asset preservation orders to ensure the assets of the company and individuals were not sent off shore.

In December 2008 final orders were made, with the Court declaring that the alleged conduct was in breach of ss. 52, 53(a), 53(d), 53(g), 55 and 58 of the *Trade Practices Act 1974.* Injunctions restraining the operators of the website from engaging in similar conduct in the future on any website were also made, and a timeframe for negotiating a compensation scheme for affected consumers was also set out.

In April 2009, the ACCC reached agreement with the respondents as to terms of compensation for affected consumers. In June 2009 the monies received by the respondents was returned to consumers that had provided a valid claim for compensation.

Reciprocal registration and enforcement of judgements

8.21 The reciprocal registration and enforcement of overseas judgments is dealt with under the *Foreign Judgements Act 1991* (Cth) but the scheme only applies to 'enforceable money judgments' unless the regulations also provide for 'non-money' judgements. At the commencement of this inquiry pecuniary penalties were not available in relation to consumer protection matters under the *Trade Practices Act 1974* (Cth). And, to date declarations of breaches of the *Trade Practice Act 1974* (Cth) and injunctions to prevent future violations are not covered by the scheme.

8.22 The *Australian Consumer Law* is intended to replace provisions of the various State and Territory Acts and *Trade Practices Act 1974* (Cth) and to be fully implemented nationally by 31 December 2010.[23] Part of these reforms includes stronger remedies, including empowering regulators to seek civil and pecuniary penalties, injunctions, damages, and compensation orders for contravention of the *Australian Consumer Law*.

Committee View

8.23 The availability of money judgments under the new *Australian Consumer Law* means that the *Foreign Judgments Act 1991* (Cth) will have greater potential for utility in the field of consumer protection.[24] However, whether non-money orders should be provided for by regulation under the *Foreign Judgments Act 1991* (Cth) remains an outstanding question.

8.24 In the Internet age national governments need to utilise all the mechanisms available to enforce their consumer protection regimes. In the *Sydney Opera House Case*, Justice Sackville took the opportunity to comment that:

> While domestic courts can, to a limited extent, adapt their procedures and remedies to meet the challenges posed by cross border transaction in the Internet age, and effective response requires international co-operation of a high order. As the evidence in this case shows, some steps have been taken to secure that cooperation ... [but] much more needs to be done if Australian consumers are to be adequately protected against fraud or misleading conduct perpetrated over the Internet.[25]

8.25 This Committee is of the view that combating the globalisation of online scams and other forms of cyber crime requires a comprehensive and integrated approach to enforcement. As Australia moves into an era of stronger and nationally consistent consumer protection law it makes sense to pay attention to the international cooperation and enforcement aspects of the new regime.

---

23 The Trade Practices Amendment (Australian Consumer Law) Bill 2009 passed both Houses of Parliament on 17 March 2010. State and Territory Governments will introduce application legislation to apply the entire Australian Consumer Law in each jurisdiction.

24 The *Foreign Judgments Act 1991* (Cth) provides a mechanism for the registration and enforcement of overseas judgments on the basis of 'substantial reciprocity of treatment' (s.5(1)).

25 *ACCC v Chen* [2003] FCA 897 at 62.

8.26 The bilateral MOUs with the US and other countries and the ICPEN Memorandum are intended, among other things, to improve the effective enforcement of consumer protection laws and have benefits for consumers everywhere. Further institutionalising enforcement through formal court procedures will also enable the Australian regulator to assertively and efficiently enforce Australian law to protect Australian consumers. This is not a substitute for administrative cooperation, which remains of vital importance and in many cases will be the most appropriate way forward. However, closing the gap between the *Australian Consumer Law* and the *Foreign Judgments Act 1991* (Cth) is one area of legislative reform that can strengthen the protection of consumers in the Internet age.

Recommendation 22

That the Australian Government ensure that:

- **remedies available under the new Australian Consumer Law can be effectively asserted against perpetrators outside Australia; and**
- **the *Foreign Judgments Act 1991* (Cth) be amended to allow for the reciprocal registration and enforcement of non-money judgments made under the Australian Consumer Law.**

Consumer Privacy and the Problem of Spyware

8.27 The evidence has demonstrated the complex interplay between different crime methodologies that combine activities crossing criminal and civil law boundaries. The Cyberspace Law and Policy Centre (CLPC) argued that regulatory and policy analysis tends to focus on one or two elements (DDOS and malware or spam and phishing) creating artificial distinctions that result in wrongly targeted approaches.[26]

8.28 For example, the installation of unwanted software without the user's informed consent was said not to be 'expressly illegal in Australia'.[27] The CLPC said the existing approach misses the connection between legitimate

26 CLPC, *Supplementary Submission 62.1*, p.4.

27 CLPC, *Supplementary Submission 62.1*, p.5.

and illegitimate conduct, which if properly targeted could cut through the fragmentation in the Australian system.[28]

8.29 The *Trade Practices Act 1974* (Cth) does not explicitly address the problem of unauthorised installation of software *per se*. Whether an unauthorised installation of software contravenes the *Trade Practices Act 1974* (Cth) will depend on whether the conduct takes place within the context of misleading and deceptive conduct or false representation.

8.30 The problem of spyware illustrates the inherently complex relationship between legitimate commercial and criminal online conduct:

> … the distinction between spyware and adware can turn on the issue of informed consent: Spyware is software that is installed on a computing device and takes information from it without the consent or knowledge of the user and gives that information to a third party.[29]

8.31 Spyware can be deployed through various means, for example, through free software that includes browser toolbars and personal organisers, downloaded accidentally via an email attachment or simply clicking onto a website.[30] Adware is software that supports the automatic download and display of advertisements and is generally bundled as part of a software package. With permission it also often tracks the end users web browsing activity, this personal information is then used to tailor the display advertisements.

8.32 Where adware is deployed through a third party that bundles the software with its own product, liability is transferred to the third party affiliate through an online contract.[31] In this complex arrangement the adware is less visible, the ability to avoid liability greatly enhanced and the prospect of genuine or informed consent probably redundant.

8.33 In 2005 a Spyware Bill was introduced to the Parliament which sought to ensure that no program, cookie or tracking device could be installed without the user being given full and clear information about the purpose of the program or tracking device.[32] However, in a review of the legislative framework the then Government concluded that spyware is like other forms of malware and existing criminal offences adequately deal

---

28 CLPC, *Supplementary Submission 62.1*, p.5.

29 DCITA, *Taking Care of Spyware*, September 2005, p.3.

30 K Howard, Mallesons Stephen Jacques, *Computers and Law*, March 2006, p.17.

31 CLPC, *Submission 62*, p. 7.

32 Paul Clarke, *Do we need a Spyware Act?*, Internet Law Bulletin, Volume 8 Issue 4, p. 58.

with the problem.[33] In addition, the *Privacy Act 1998* (Cth) prohibits the unlawful collection of personal information; the *Trade Practices Act 1974* (Cth) applies where spyware is downloaded in the context of misleading or deceptive conduct and the *Australian Securities and Investments Commissions Act 2001* (Cth), *Corporations Act 2001* (Cth), and the *Telecommunications Act 1997* (Cth) also apply.[34]

8.34 It was contended that Australia's legal framework is convoluted and works against investigation and prosecution.[35] The ACCC said that:

> Careful consideration is needed to determine whether ... [it] would be appropriate to apply industry specific regulations rather than general prohibitions.....[36]

8.35 The CLPC argued that:

> From the legal perspective, charges and fines have not been made against *a single* corporation or organisation for spyware or malware distribution in Australia. Contrast this finding to jurisdictions that have mandated an authority such as OPTA or the United States Federal Trade Commission, where over 100 fines and charges have been made against spyware and malware distribution companies such as DollarRevenue in the United States, Canada and Europe.[37]

The DollarRevenue Case

8.36 The CLPC cited the example of Dutch company DollarRevenue, an advertising company, held responsible for the illegal installation of spyware on 22 million computers. The company used an affiliate business model where third parties agreed to deploy DR Software through ActiveX and software bundling (Active payouts in Northern America average $.25c per installation).[38] According to CLPC, the affiliates use a variety of means to trigger DR software downloads including spam, botnets, and chatroom sessions. Although the company is structured legally, in practice the model is intended to transfer liability to third party affiliates through an online contract.[39]

---

33 DICITA, *Outcome of the Review of the Legislative Framework on Spyware*, 2004

34 DICITA, *Outcome of the Review of the Legislative Framework on Spyware*, 2004.

35 CLPC, *Supplementary Submission 62.1,* p.8.

36 ACCC, *Supplementary Submission 46.1*, p.11.

37 CLPC, *Supplementary Submission 62.1,* p.8. Emphasis added.

38 CLPC, *Supplementary Submission 62.1*, p.7.

39 CLPC, *Supplementary Submission 62.1*, p.8.

8.37 The CLPC submitted that DollarRevenue is or has also been involved with 'malicious spam, iframe injections and Trojan downloads, which initialise information capturing software (such as passwords or browser histories)'. The CLPC also stated that IT security company Sunbelt Malware Research Labs identified over 2,000 additional adware/spyware programs downloaded in a single DR software application.[40]

8.38 Installing software without a user's informed consent is a violation of the Dutch *Telecommunications Act 2004*, and the Dutch Telecom Regulator has powers to investigate, fine and issue penalties and compliance notices. The regulator also works with the Dutch police 'to bring criminal charges where it is warranted'.[41] In this case, the company was fined by the regulator for installing unsolicited software without the informed consent of computer owners. The company directors are reported to be subject to separate criminal investigation.[42]

8.39 The AGD reiterated to the Committee that the computer offences would 'generally apply in cases where software, such as spyware, is installed in a PC without the owner's informed consent' (s.477.2 makes it an offence to use the Internet to infect a computer with spyware).[43] However, the CLPC's main point was that legitimate adware makes consumers more vulnerable to illegitimate spyware, and other malware applications such as Trojans that 'collect usernames and passwords for Internet banking and e-commerce websites'.[44]

Committee View

8.40 The Committee believes that while there must be appropriate criminal offences, traditional criminal law enforcement will not always be the most effective approach. Tackling the problem through clear consumer protection measures will help to protect consumer privacy, reduce the opportunities for cyber crime and support criminal law enforcement goals.

8.41 This approach will also support consumer education on the importance of reading the terms and conditions of user agreements and licences, which are often given little or no attention. The browser activity and online

40 CLPC, *Supplementary Submission 62.1*, p.6.

41 CLPC, *Supplementary Submission 62.1*, p.8.

42 CLPC, *Supplementary Submission 62.1*, p.5.

43 Note also that corporate liability can apply where the fault element is attributable to a body corporate that has expressly, tacitly or impliedly authorised the commission of the offence. See Chapter 2 of the Criminal Code.

44 CLPC, *Submission* 62, p. 6.

purchasing habits of an end user are, in our view, a form of personal information and is unlikely to be consented to in the offline world. While there are technical solutions, not all anti-virus and spyware detection software works all the time. Additionally, consumers may be being surreptitiously tricked into 'consenting' to the download. There is also a problem of young people, including children, agreeing to downloads that they not understand or do not have legal capacity to consent to.

8.42 In theory, the Criminal Code applies to the unauthorised installation of spyware, but the lack of enforcement action (domestically or in concert with international partners) suggests Australian agencies are not making inroads into this particular problem. In any event, the existence of a criminal offence on the statute book does not negate the role that a more strategically positioned consumer protection measure can play in preventing further criminal activity. It also empowers ordinary citizens to respond to privacy violation in a commercial context and strengthens regulators – in this case the ACCC and the Privacy Commissioner.

Recommendation 23

That the Treasurer amend the Australian Consumer Law to include specific protections against the unauthorised installation of software programs:

- **the reform should target the unauthorised installation of programs that monitor, collect, and disclose information about end users' Internet purchasing and Internet browsing activity;**
- **the authority to install a software program must be based on informed consent; and**
- **to obtain informed consent the licence/agreement must require clear accessible and unambiguous language.**

Information Standards

8.43 A common theme in the inquiry has been how to best get the e-security message across to ordinary consumers. The evidence canvassed in Chapter 4 highlighted that, although general levels of awareness are reasonable among the Australian public, this does not always translate

into action. The value of a national e-security awareness strategy is discussed in Chapter 10.

8.44 Some witnesses argued that providing e-security information at the point of sale may be the best time to prompt consumers to take protective action.[45] The Australian Computer Society (ACS) said:

> The ACS believes that governments should look to developing agreements with vendors to ensure that computer systems and mobile devices are not sold without supplying adequate e-security and cyber safety information that covers not only current threats but also emerging threats.[46]

8.45 The Australian Senior Computer Clubs Association (ASCCA) was clear that senior Australians must get consistent messages from both government and industry. The ASCCA said:

> That anti-virus software and a firewall should be pre-installed on all new computers purchased. An easy to understand brochure, written in plain English, outlining how to be safe online should also be provided with each purchase. Translating this brochure into relevant community languages should also be considered.[47]

8.46 Mr Peter Coroneos, CEO, Internet Industry Association (IIA) agreed that the industry needs to look at every point of contact with the consumer to get across the e-security message. He said:

> Absolutely. This is where we need to be lateral in our thinking. We need to look at every point in the chain from the initial purchase of the computer through the setting up of the computer to the ongoing usage of the computer. Each of those points represents an opportunity for awareness raising and behavioural change.[48]

8.47 The IIA used the example of routers and modems, which are vulnerable to being hijacked and the home user would have no way of knowing that it had occurred. Mr Peter Coroneos said that more needs to be done to promote router and modem security.[49] The IIA is working directly with

45 ACCAN, *Submission 57*, p.11.

46 ACS, *Submission 38*, p.4; ACCAN, *Submission 57*, *Surfing on Thin Ice: Consumers and Malware, Adware, Spam & Phishing,* p.11.

47 ASCCA, *Submission 63,* p.4.

48 Mr Peter Coroneos, IIA, *Transcript of Evidence*, 11 September 2009, p.19.

49 Mr Peter Coroneos, IIA, *Transcript of Evidence*, 11 September 2009, p.20.

manufacturers and distributors to develop standardised information to give to consumers at point of sale of these devices.[50]

Committee View

8.48 There was general agreement that point of sale information is a useful step in getting out the e-security message to consumers. This will take different forms depending on the product. There is no impediment to the IT industry creating an industry wide e-security messaging standard that applies to the point of sale but none has yet emerged. The Committee is conscious of IIA's efforts in this regard, but considers that a more comprehensive approach is needed if we are to see any real gains in promoting an e-security culture.

8.49 The Australian consumer protection legal framework provides for information standards that industry must comply with in order to protect consumers for known risks. Under the new *Australian Consumer Law*, there will be a national approach and new information standards will be created by the Commonwealth Minister.

8.50 The Committee is of the view that the problem of cyber crime, which is predicted to continue to grow in volume and sophistication, poses a sufficiently serious risk of economic and social harm to Australian consumers that a national information standard is warranted. The ACCC should, in consultation with manufacturers and distributors of personal computers, mobile phones and related IT devices such as modems and routers, develop information standards to address the e-security vulnerabilities of these products and the provision of e-security information to consumers at the point of sale.

50 Mr Peter Coroneos, IIA, *Transcript of Evidence*, 11 September 2009, p.19.

Recommendation 24

That the Australian Competition and Consumer Commission, in consultation with manufacturers and distributors of personal computers, mobile phones and related IT devices such as modems and routers, develop information standards to:

- **address the e-security vulnerabilities of these products and the provision of e-security information to consumers at the point of sale; and**
- **require that the information is presented in a manner that is clear and accessible to a non-IT literate person.**

IT Vendor Responsibilities

Security of IT Products

8.51 The Committee was told that the problem of cyber crime can largely be traced to the lack of adequate testing of hardware and software products before they are released onto the market.[51] There has been a steady climb in the number of vulnerabilities reported, which was illustrated to the Committee by the IBM *Internet Security Systems X Force 2008 Trend and Risk Report* published in January 2009.[52]

8.52 The IT vendors usually follow up with security updates and patches, which consumers can often receive automatically, but these may not follow for many months and can involve additional cost and inconvenience. Major vendors, such as Microsoft, provide options for automatic updates but as the evidence has indicated many consumers do not make use of the updates.

8.53 As AusCERT pointed out, the lack of security in technology products exposes all end users (including government, business and the home users) to e-security risks:

51 ACS, *Submission 38*, p.10; AusCERT, *Submission 30*, p.4; Internet Safety Institute, *Submission 37*, p.6; see also, C Wilson, *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress*, CRS Congress Research Paper, Updated January 29, 2008, p.26.

52 Internet Safety Institute, *Submission 37*, p.6; viewed 13 April 2010, <http://www-935.ibm.com/services/us/iss/xforce/trendreports/xforce-2008-annual-report.pdf page 18>.

> We have built vast networks and information systems using technology that cannot be properly or easily secured, ... despite the fact that the software security industry is big business in its own right.[53]

8.54 In 1998, the National Security Agency (NSA), in its paper *The Inevitability of Failure: The flawed assumption of security in modern computing environments* (1998), summarised a key aspect of the problem as follows:

> The goal of this paper is to motivate a renewed interest in secure operating systems. [The NSA] argues that the threats posed by the modern computing environment cannot be addressed without support from secure operating systems and, [...] any security effort which ignores this fact can only result in a "fortress built upon sand".[54]

8.55 The problem extends beyond operating systems to software applications, which AusCERT said need to be securely designed because vulnerabilities in applications such as browser plug-ins, for example Adobe Flash and Shockwave, can compromise entire computer systems. The general point was made that NSA analysis remains valid but in fact the threat environment has 'substantially worsened and the modern software environment has not kept pace.'[55]

8.56 The ACS concurred with this overall assessment:

> Ultimately, many cyber crime risks can be mitigated by industry developing more secure hardware and software and integrating improved security into the software and hardware development cycles. Technology must become more trustworthy in terms of its security vulnerabilities.[56]

8.57 There has been a trade off in the market between security with speed, interoperability and the desire to allow an openness that will foster innovation. However, as ACS said, the downside is that:

> The competitive nature of computing and the rush to market to achieve first mover advantages appear to be driving a less thorough testing of code, system and hardware vulnerabilities.[57]

---

53 AusCERT, *Submission 30*, p.4.
54 AusCERT, *Submission 30*, p.4.
55 AusCERT, *Submission 30*, p.4.
56 ACS, *Submission 38*, p.10.
57 ACS, *Submission 38*, p.10.

8.58 According to ACCAN's research the cost and inconvenience to consumers is significant and warrants specific research, perhaps by the Productivity Commission. In ACCA's report *Surfing on Thin Ice: Consumers and Malware, Adware, Spam & Phishing* it was found that:

> More than 1 out of every 10 consumers surveyed had suffered financial loss or unexpectedly high bills as a result of security problems, with the majority of these losses exceeding $100. These results, combined with written comments we received, highlight the significant burden consumers face as a result of online security issues and hints at their impact on the economy, consumer satisfaction and productivity. Projected to the wider Australian population, consumers as a whole may be experiencing hundreds of millions of dollars of financial loss as a result of security problems, and many may be experiencing emotional distress and spending significant amounts of time dealing with security issues.[58]

8.59 The lack of IT security and the risks and costs of cyber crime are also a factor that inhibits the growth of e-commerce. It has been reported that although over 90 per cent of small and medium sized businesses are connected to the Internet, the risk that company systems can be hacked into is the number one concern in relation to e-commerce.[59]

8.60 The ACS would like to see vendors embrace secure development of applications more fully. In their view, this should be done on a voluntary basis and 'consistent with the international standards to which all hardware and software developers and suppliers sign up to comply with'.[60]

8.61 A voluntary security assurance scheme based on an International Common Criteria Framework already exists. In Australia, the Defence Signals Directorate (DSD) provides evaluation and testing of products as part of this scheme in its role of providing technical security support to government departments and agencies.[61] Lists of certified products are available online but the audience is generally IT security professionals working within government.

---

58 ACCAN, *Surfing on Thin Ice: Consumers and Malware, Adware, Spam & Phishing,* p.24.

59 Sensis, *E-Business Report: The Online Experience of Small and Medium Enterprises*, July 2008, p.5; Sensis, *E-Business Report: The Online Experience of Small and Medium Enterprises*, August 2009, pp.5 and 11.

60 ACS, *Submission 38*, p.11.

61 Australasian Information Security Evaluation Program.

8.62 Microsoft Australia advocated a wider take up of the existing framework for testing and evaluation of the security features of IT products.[62] However, as AusCERT pointed out, although software assurance occurs as part of the Common Criteria program there is no requirement for products to undergo security assurance checking before being released to the market. Nor is there any requirement for those that do undergo the testing process to display the level of security assurance obtained to consumers.[63]

8.63 According to AusCERT most products do not achieve a level of security that is sufficient for the purposes of reducing cyber crime:

> Hence, a lot more work needs to be done by software manufacturers to attain a software evaluation that allows consumers to have confidence that they are buying products that are relatively secure to deploy, ie are able to reliably defend themselves from attack. This applies to both operating systems manufacturers and application software, both proprietary and open source.[64]

8.64 The ACCC confirmed that there is no code of practice or standards under the *Trade Practices Act 1974* (Cth) that require IT manufacturers to build security into their products. As Mr Nigel Ridgway, Group General Manager, Compliance, Research, Outreach and Product Safety, ACCC, pointed out, the problem of e-security vulnerabilities in hardware and software products have been responded to by the growth of anti-virus products.[65]

8.65 The ACS suggested that to drive greater trustworthiness of the technology manufacturers should advertise their compliance with security standards (for example the Common Criteria). This would enable consumers to make more informed choices about the security of the product.[66] AusCERT took a similar approach and advocated a software labelling scheme.[67] This would require national regulation requiring software manufactures to display consumer labels with independent evaluation of the product's security.[68]

---

62 <http://www.commoncriteriaportal.org/theccra.html>

63 AusCERT, *Submission 30*, p.21.

64 AusCERT, *Submission 30*, p.21.

65 Mr Nigel Ridgway, ACCC, *Transcript of Evidence,* 18 November 2009, p.7.

66 ACS, *Submission 38*, p.11.

67 AusCERT, *Submission 30*, p.20.

68 AusCERT, *Submission 30*, p.20.

8.66 As noted above, Microsoft advocated a greater take up of the existing testing and evaluation scheme under the Common Criteria. However, they argued that any legislative reforms should protect innovation in the IT industry and government should fund research into security issues.[69] Symantec also argued that a healthy competitive market in security solutions was vital to promote innovation and combat the fast pace of the changing threats.[70]

Committee View

8.67 Throughout this inquiry liability has been a key issue that many stakeholders appeared reluctant to address directly. When considering the same problem in the UK, the House of Lords Science and Technology Committee concluded that efforts to promote better security standards have been hampered by a lack of commercial incentives and that IT vendors can too easily shift the risks and costs onto consumers through licensing agreements.[71] The consumer group, ACCAN, has indicated that it believes the cost to consumers is such a significant issue that it should be looked into by the Productivity Commission.

8.68 The question is what is the best way to drive manufacturers toward greater security in hardware and software applications? The Committee agrees with the House of Lords' general view that industry should be making security a much higher priority. While it has been important to foster innovation and competition the Committee queries whether the market may have gone too far in this direction at the expense of the security of consumers. The widespread claim that innovation and interoperability will suffer if security is given a higher priority is not entirely convincing.

8.69 The Committee accepts that, to a significant extent, there is an 'arms race' to discover and exploit vulnerabilities by highly sophisticated criminal networks. Vulnerabilities cannot be entirely eliminated because of the complexity of these products and the importance of interoperability with third parties. However, in our view, manufacturers must start taking their duty of care to their customers more seriously.

8.70 The costs to end users, especially ordinary consumers but also small and medium size businesses, have been largely hidden. A more secure online

69 Microsoft Australia, *Submission 35*, p.1.

70 Symantec, *Submission 32*, p.12.

71 Science and Technology Committee, *Personal Internet Security*, Volume 1 Report, House of Lords, August 2007, pp.41-42.

environment is needed to build and maintain trust, protect vulnerable end users as much as possible from cyber crime and support the expansion of e-commerce and the digital economy.

8.71 It is the Committee's view that consumers should not have to rely on the general prohibition on false representation or misleading or deceptive conduct. A more direct approach would be to require by law that IT manufacturers that sell product in Australia should disclose known vulnerabilities so that a consumer can make an informed choice at the point of purchase. To improve security standards manufacturers should adopt best practice to testing and evaluation *before* release to market. There is a case for specific industry regulation through a code of practice on security standards based on the internationally accepted standards regime. This framework could then provide the basis for a security labelling scheme.

8.72 However, the Committee is conscious there are difficulties with developing a single national regulation for the IT products industry that is global in nature. One issue is the need for such a regime to be consistent with Australia's international trade obligations.

8.73 The Productivity Commission is an appropriate body to conduct in depth investigation into the economic and social costs of the systemic security issues in the IT hardware and software market, and its impact on efficient functioning of the Australian economy. At this stage the Committee recommends that this in depth investigation be carried out to provide more comprehensive analysis to support future policy development.

Recommendation 25

That the Treasurer direct the Productivity Commission to conduct an in depth investigation and analysis of the economic and social costs of the lack of security in the IT hardware and software products market, and its impact on the efficient functioning of the Australian economy.

That, as part of its inquiry, the Productivity Commission address the merits of an industry specific regulation under the Australian Consumer Law, including a scheme for the compulsory independent testing and evaluation of IT products and a product labelling scheme.

8.74 That said, inadequate security is a systemic problem in the IT market and the risks and many of the costs of cyber crime are widely accepted and known. The Committee believes that IT manufacturers have an obligation to make products as secure as possible (subject of course to the rules of anti-competitive conduct). As an interim step, end users should have statutory cause of action against manufacturers who release products to market with known vulnerabilities that result in losses that could not otherwise have reasonably been avoided. The courts are well equipped to apply principled reasoning to complex facts and work out the liability between respective multiple parties.

Recommendation 26

That the Treasurer consult with State and Territory counterparts with a view to amending the Australian Consumer Law to provide a cause of action for compensation against a manufacturer who releases an IT product onto the Australian market with known vulnerabilities that causes losses that could not have reasonably been avoided.

Security Settings

8.75 One of the issues raised with the Committee was the lack of sufficient prompting to end users to adopt more secure settings when setting up new products. A case in point is the vulnerability of routers to being hacked and compromised, which affects the security of an entire computer system. It is widely known and accepted that consumers often do not change router settings and this is a risk factor that could be addressed without significant expense to manufacturers.[72] But despite industry knowledge that consumers often do not change the default settings, no industry wide practice has yet emerged to address it.

8.76 The question was why manufacturers do not make default settings as secure as possible or ensure that when setting up there are automatic prompts or actually require the consumer to adopt the strongest possible setting? For example, in the case of a router, a prompt that requires the user to change the setting with a strong password before it can be used would be a simple solution. Secondly, is the failure of industry to provide

72 See discussion, *Transcript of Evidence,* 18 November 2009, pp.12-15.

adequate e-security prompts and secure settings a breach of the *Trade Practices Act 1974* (Cth)?

8.77 Under the *Trade Practices Act 1974* (Cth), consumers are entitled to products that are 'fit for purpose' and 'free of defects'. These entitlements are statutory conditions that are implied into consumer contracts. In essence, this means that goods must match the description given; be fit for the purpose for which they have been sold; and be of 'merchantable quality'.[73]

8.78 A product, such as a router, which is 'fit for purpose' at the point of sale is arguably no longer 'fit for purpose' if the way in which it is set up actually makes the computer system more vulnerable to attack. Some might regard the ability to connect a router to a computer system and the Internet without adequate security setting as an inherent defect in the design of the product.

8.79 The current legal regime does not oblige manufacturers to take any responsibility for designing security into the product.[74] It is not a statutory condition implied into a contract of sale, and nor is it addressed by any industry specific regulation or industry code of practice. As Mr Nigel Ridgway, ACCC, explained:

> We do look at these issues on a case by case basis but, in the hypothetical, something that functions quite well or quite appropriately, absent that malicious attack by a third party, is not, I would think, going to fall foul of the warranty provisions.[75]

Committee View

8.80 It seems likely that the vast majority of end users, whether they are home users, or small or medium sized businesses, lack the knowledge to make an informed choice about appropriate security setting for their operating system, the additional hardware devices or the software applications used on it. This appears to be a widespread and well known problem that neither governments nor industry can ignore, because of the financial and social impacts of cyber crime.

---

73 The latter means the goods should be free from defects not obvious at the time of purchase and be of reasonable quality and performance taking into account the price and description at the time of purchase.

74 Mr Nigel Ridgway, ACCC, *Transcript of Evidence,* 18 November 2009, p.15.

75 Mr Nigel Ridgway, ACCC, *Transcript of Evidence,* 18 November 2009, p.15.

8.81 The Committee believes that IT vendors can do more to prompt and guide consumers to adopt better security without locking consumers into completely secure systems that will prevent interoperability. The industry should be encouraged to take account of the reality that most consumers are not IT literate and are unlikely to understand all the implications of poor security settings.

Recommendation 27

That the manufacturers of IT products adopt a best practice approach that ensures products are designed to prompt and guide end users to adopt more secure settings.

That the Australian Government monitor industry practice in this regard, and promote international standards that put a higher priority on security through product design.