7

Protecting the Integrity of the Internet

Introduction

7.1 This chapter discusses current and future initiatives for promoting a more secure Internet environment. In particular, it considers the role of the Australian Communications and Media Authority (ACMA), Internet Service Providers (ISPs), and Domain Name Registrars and Resellers in promoting greater resilience within the Australian Internet networks.

7.2 The chapter focuses on six key issues:

- the effectiveness of the Australian Internet Security Initiative (AISI) to detect and drive the remediation of bots;
- the role of ISPs in the AISI and the proposed Internet industry e-security code of practice;
- remediation of infected computers;
- ACMA's capacity to respond to the threat of compromised websites;
- ACMA's spam reporting initiative and the role of ISPs under the *Spam Code of Practice*; and
- e-security and the Domain Name Registration System.

Australian Internet Security Initiative

7.3 The ACMA is a statutory authority within the Australian Government portfolio of Broadband, Communications and the Digital Economy. The

ACMA is responsible for regulating broadcasting, the Internet, radio communications and telecommunications.[1]

7.4 The ACMA developed the AISI in 2005. The AISI identifies computers operating on the Australian Internet that have been infected by malware and are able to be controlled for illegal activities.[2] The Committee was told that AISI has been progressively expanded over time and has attracted international interest.[3]

7.5 As noted previously in this report, 99 per cent of spam is sent from botnets.[4] Spam email is one of the primary vectors of malware and the dissemination of scams and phishing attacks on end users. By detecting malware infected computers, regulators can address the problem of spam and make strategic in roads into the problem of botnets. The AISI recognises that link and is intended to target the source of the spam problem by detecting compromised machines and botnet activity.[5]

7.6 In essence, AISI is a 'data handler' system that collates data into one central database and enables ACMA to standardise the information. ACMA issues daily reports to ISPs about types of compromises detected in their customers' machines.[6] ACMA explained:

> Through the AISI, the ACMA collects data from various sources identifying IP address that have been detected as exhibiting 'bot' behaviour on the Australian internet. Using this data, the ACMA provides daily reports to participating … ISPs identifying IP addresses on their networks that have been reported as compromised (infected with malware) in the previous 24-hour period.[7]

7.7 There has been a steady increase in the number of compromises reported daily through the AISI, and 'a marked increase since March 2009'.[8] In June 2009, ACMA was reporting more than 10,000 individual compromises per day to Australian ISPs. At the hearing on 21 October 2009, Mr Bruce Mathews, Acting Executive Manager, Strategy and Coordination Branch, ACMA, submitted that the prevalence of botnets on the Australian

[1] The ACMA was established on 1 July 2005 by the merger of the Australian Broadcasting Authority and the Australian Communications Authority.

[2] ACMA, *Submission 56*, p.3.

[3] Mr Bruce Mathews, ACMA, *Transcript of Evidence*, 21 October, 2009, p.2.

[4] Mr Bruce Mathews, ACMA, *Transcript of Evidence,* 21 October 2009, p.10.

[5] ACMA, *Submission 56*, p.3.

[6] Mr Bruce Mathews, ACMA, *Transcript of Evidence,* 21 October 2009, p.7.

[7] ACMA, *Submission 56*, p.3.

[8] ACMA, *Submission 56*, p.5.

internet remains of considerable concern and warrants the attention of the Committee.[9]

7.8 The data obtained through AISI is expanding due to:

- an increase in the number of sources and improvements in compromise data resulting in the identification of more malware types and infected machines;
- an expansion in the number of ISPs participating in AISI providing greater coverage of Australian IP addresses;
- an expansion of IP address ranges by ISPs to provide for customer growth; and
- more comprehensive IP address range information provided to ACMA.[10]

7.9 The Committee was also told that the increased number of reported compromised machines has required a 'substantial increase in ACMA resources':

> ACMA's interaction with ISPs and their customers – the latter being usually via the ISP – has increased markedly since March 2009. These most generally involve the ACMA providing further information on individual compromise reports in response to enquiries.[11]

7.10 The effectiveness of the AISI depends on three elements:

- access to information on zombie computers and botnet activity;
- the willingness and capacity of ISPs to take action; and
- the ability of end users to remediate infected computers and protect themselves in the future.

7.11 These issues are discussed in the following sections.

Access to Network Data

7.12 Access to network data is vital to detecting IP addresses of compromised machines and botnet activity. ACMA told the Committee that network

[9] Mr Bruce Mathews, ACMA, *Transcript of Evidence*, 21 October, p.2.

[10] ACMA, *Submission 56*, p.5.

[11] ACMA, *Submission 56*, p.8.

data comes from a range of sources, including some on a confidential basis:

> The AISI collects data from a number of parties who run honeypots, spamtraps, sinkholes and other mechanisms for the purpose of identifying compromised hosts or other malicious activities on the internet.[12]

7.13 To ensure access to this information ACMA often agrees 'not to disclose the operations, tools, methods and infrastructure utilised by its partners'.[13] The publicly acknowledged sources are The Shadowserver Foundation[14], The Australian Honeynet Project,[15] and SORBS (Spam and Open Relay Blocking System).[16] The ACMA also operates its own honeypots and spamtraps.[17]

7.14 The Committee heard there is also a vast wealth of network intelligence available from global IT companies that could be tapped by government. As noted in Chapter 5, Symantec told the Committee that it possesses a rich repository of intelligence data. The issues raised by Symantec in relation to sharing real time cyber threat intelligence are also relevant to the sharing of network data in the context of AISI. In particular, the extent to which authorities monitor the data, who the data is shared with, where the data is stored and legal implications regarding privacy are all pertinent.

7.15 Sophos also pointed out the high commercial value of data from filtering technologies that identify the IP addresses of botnets. The Committee was told that this data is not likely to be shared openly between competitors.[18]

7.16 Sophos said:

> Although ACMA/AISI is already tackling this problem, with additional co-operation … Australia could be seen to be leading the world in anti-botnet activity, and to encourage such a process to be rolled out as worldwide best practice.[19]

[12] ACMA, *Supplementary Submission 56.1*, p.2.

[13] ACMA, *Supplementary Submission 56.1*, p.2.

[14] <http://www.shadowserver.org/>.

[15] <http://www.honeynet.org.au/>.

[16] <http://www.au.sorbs.net/>.

[17] ACMA, *Supplementary Submission 56.1*, p.2.

[18] Sophos, *Submission 66*, p.6.

[19] Sophos, *Submission 66*, p.6.

7.17 As a step toward greater cooperation with the private sector, Sophos proposed that interested security vendors, together with government, should consider mechanisms to increase data sharing on botnets.[20]

Internet Industry Participation

7.18 The Internet industry has grown rapidly over the past decade and it was estimated there are now between five to six hundred ISPs currently operating in Australia.[21] Although large companies such as Telstra and Optus have the largest share of the market, a significant proportion of the industry is made up of small providers. Elsewhere it has been estimated that more than a quarter of ISPs have an annual turnover of less than $3 million.[22]

7.19 The Committee heard that ISPs occupy a unique position as the only party that can link an individual user to an IP address identified by AISI.[23] And ACMA emphasised the importance of this role in the overall national strategy to combat cyber crime.[24]

7.20 The AISI started as a pilot project in 2005 with six ISPs. The Committee was told that 'the 2007 Budget allocated approximately $4.7 million (over four years) to enable the expansion of the AISI to all Australian ISPs who wish to participate'.[25] There are now 71 ISPs participating in the scheme, which ACMA estimated covers 90 per cent of Australian residential customers.[26]

7.21 ACMA's published statement to the ISPs states:

> There are no costs to ISPs associated with participation in the AISI. It is a free service provided by ACMA to assist in reducing spam and to improve the security level of the Australian internet. By participating, you will contribute to the overall reduction of spam and e-security compromises, thereby reducing costs for all ISPs.[27]

7.22 The ACMA also states that:

[20] Sophos, *Submission 66*, p.6.

[21] Mr Bruce Mathews, ACMA, *Transcript of Evidence,* 21 October 2009, p.6.

[22] See *ALRC Report 108*, pp.1330-1331; see also, Office of the Privacy Commissioner, *Submission Draft Internet Industry Association eSecurity Code of Practice*, p.3.

[23] Mr Keith Besgrove, DBCDE, *Transcript of Evidence*, 25 November, 2009, p.9.

[24] ACMA, *Submission 56*, p.23.

[25] IIA, *Submission 54*, p.7.

[26] ACMA, *Submission 56*, p.3; Mr Bruce Mathews, ACMA, *Transcript of Evidence,* 21 October 2009, p.1.

[27] <http://www.acma.gov.au>, viewed 27 May 2010.

> The number of compromises listed in the daily AISI reports will vary considerably for each ISP, depending on the customer base of the ISP and the quantity of the information feeding into the AISI on a given day. Large ISPs may receive hundreds (and in some cases thousands) of compromises per day, whereas some smaller ISPs may rarely get any reports.[28]

7.23 In the absence of Australian data, ACMA pointed the Committee to a 2008 survey by Arbor Networks of 66 IT network operators from North America, South America, Europe and Asia that 'indicated considerable support from ISPs in combating botnets':

> We also asked if respondents believe that ISPs should be responsible for detecting and monitoring botnets. Sixty-one percent said Yes, while 23 percent disagreed, and another 17 percent responded Yes, with some criteria.[29]

7.24 The Committee was also told that ISPs are dedicating resources to addressing compromised computers, and, as ACMA pointed out, have a commercial interest in addressing bot malware.[30] Some ISPs utilise independent sources of compromise data separate to those fed into the AISI system, and some have developed their own internal systems to identify compromised IP addresses. Although the volume of IP addresses identified this way was unknown, ACMA expects it to be a significant number.[31]

7.25 Mr Peter Coroneos, CEO, Internet Industry Association (IIA), informed the Committee that ISP members see a 'win-win benefit' because malware infected machines are a 'threat to the integrity of the network itself'.[32]

7.26 It was also suggested that ISPs could benefit further from selling a remediation service or getting commission from the sale of anti-virus products at the point of selling the Internet connection.[33]

7.27 The Committee was told that 'best practice' requires that an ISP identify the customer, reduce their access to the Internet, provide the support and advice to remove the compromise, and then reinstate the normal service.[34]

[28] <http://www.acma.gov.au>, viewed 27 May 2010.

[29] Arbor Networks, *Worldwide Infrastructure Security Report,* Volume IV, October 2008, p.23 as cited in ACMA, *Submission 56*, p.23.

[30] ACMA, *Submission 56*, p.22.

[31] ACMA, *Submission 56,* p.5.

[32] Mr Peter Coroneos, IIA, *Transcript of Evidence*, 11 September 2009, p.15.

[33] Mr Mike Rothery, AGD, *Transcript of Evidence*, 25 November 2009, p.10.

[34] Mr Keith Besgrove, DBCDE, *Transcript of Evidence*, 25 November, 2009, p.10.

However, in practice, there is considerable variation in the way ISPs respond to compromised machines operating across their networks.[35]

7.28 Mr Bruce Mathews, ACMA, said the level of assistance provided by ISPs to end users varies 'very significantly':[36]

> ISPs are prepared to voluntarily take actions to combat bots and botnets. The AISI is not a mandatory program and … ISPs currently participate in the program at the level they consider appropriate to their own resources, systems and processes for customer interaction.[37]

7.29 AISI is a purely voluntary scheme. There is no mechanism for monitoring ISP action, or whether the infected machine has been remediated.[38] Consequently, there is no data to show how many AISI reports actually result in clean-up of infected computers. Nor does ACMA have any power to order the quarantining or disconnection of a machine if an ISP declines to take action or an end user fails to remediate the problem.[39]

7.30 While the best approach is said to be contacting the customer by phone, this is not 'economically feasible' given that some large ISPs can 'receive 2,000 reports per day'.[40] An alternative is to notify customers by email and then monitor whether there is a response. In some instances, the ISPs do not notify customers at all, some take AISI data and correlate it to their own information, other ISPs take a graduated approach and, in a severe case, will disconnect a customer (see below).

7.31 The IIA advised the Committee that some of the larger ISPs have already developed automated systems for notifying their customers as a way of dealing with the volume of reports received, while smaller ISPs may call their customers and use it as an opportunity to maintain their customer relationship. One example of how some ISPs are responding to the problem of zombie computers is Queensland based ISP, Dreamtilt, which has a clear statement informing customers about their participation in AISI and what to do in the case of a notification:

> What if I receive an notification from Dreamtilt?

[35] Mr Keith Besgrove, DBCDE, *Transcript of Evidence,* 25 November 2009, p.9; ACMA, *Submission 56*, p.3.

[36] Mr Bruce Mathews, ACMA, *Transcript of Evidence,* 21 October 2009, p.6.

[37] ACMA, *Submission 56*, p.22.

[38] Mr Bruce Mathews, ACMA, *Transcript of Evidence,* 21 October 2009, pp.3-4.

[39] Mr Bruce Mathews, ACMA, *Transcript of Evidence,* 21 October 2009, p.3.

[40] Mr Bruce Mathews, ACMA, *Transcript of Evidence,* 21 October 2009, p.4

> As part of our commitment to the Australian Internet Security Initiative, Dreamtilt aims to inform all customers which may have a zombie computer. If you receive an email from Dreamtilt in regards to an infected zombie computer, follow the instructions in the email. If the problem continues please review our Support section or call us on ... . If the problem cannot be rectified by support from Dreamtilt you may need to visit a computer technician. We have a number of resellers that can offer such a service and can be viewed here. Under our Terms and Conditions, if a computer is found to be affected or vulnerable you will be given 7 days to cleanse your computer. If the problem has not been rectified during this time, we may put your connection on hold until the problem is rectified.[41]

7.32 Telstra, the largest ISP in Australia, explained their approach to the issue:

> Telstra gathers lists of potentially infected systems from a large number of sources including from the ACMA AISI. This provides Telstra with a variety of information which it can use to verify that such reports are not false positives or other errors.
>
> All information gathered is processed in Telstra systems to allow tracking of which subscribers are potentially infected, what they are infected with and when and how Telstra has contacted them. The majority of contact made with customers is done via email as this is the preferred method of communication specified by our customers, this is also an automated process to allow tracking of who has received the email and what emails have not been delivered for various reasons.[42]

7.33 In 2009, ACMA undertook 'a brief survey of a subset of AISI participants (those who had received a threshold level of AISI reports)'.[43] The responses indicate a diverse range of actions including:

- limiting the data rate for accessing the Internet, and emailing the customer advising of the infection and the need for remediation;
- temporary suspension of accounts of re-offenders;
- placing the customer's internet service in a 'walled garden';[44]

[41] <http://www2.dreamtilt.com.au/index.php/internet-services/wireless-broadband/installation/159-aisi.html>, viewed 27 May 2010.

[42] Correspondence to the Committee, Jamie Snashall, Senior Adviser Government Relations,Telstra Corporation Ltd, 1 June 2010.

[43] ACMA, *Submission 56*, p.22.

- temporary suspension to the 'offending ports and protocol activity'; and
- regenerating account passwords (thereby preventing customer access to the Internet) in order to prompt a call to the ISP's helpdesk.[45]

7.34 These measures are being incorporated in a new voluntary Internet Industry *E-Security Code of Practice,* which is discussed in more detail below.

End User Attitudes

7.35 The evidence on end user attitudes was also mixed. Sophos told the Committee that anecdotally some customers are dismissive or defensive when contacted.[46] The IIA described notifying an end user their computer is infected as akin to telling someone they have 'digital bad breath' although many ISPs subscribers appreciate receiving the information.[47]

7.36 The Committee also heard that:

> Anecdotal information from ISPs … indicates that some customers are continually identified in the AISI reports, which has resulted in the adoption of escalated procedures by many ISPs for these 'repeat offenders', including termination of their internet accounts in the most extreme cases.[48]

7.37 In 2008, AusCERT commissioned research into end user attitudes towards a range of personal Internet security issues. The AusCERT *Home Users Computer Security Survey 2008* found that 92 per cent of the 1,000 respondents wanted their ISP to let them know their computer was compromised. The survey also found that:

- 29 per cent were prepared for their ISP to disconnect them completely from the Internet until the computer was fixed;
- 89 per cent said they would want the ISP to provide them with assistance to fix the problem; and

[44] In this context, placing an end user in a 'walled garden' means restricting Internet access from that computer only to approved IP addresses.

[45] ACMA, *Submission 56*, p.22.

[46] Sophos, *Submission 66*, p.6.

[47] IIA, *Submission 54,* p.8.

[48] ACMA, *Submission 56*, p.8.

- 61 per cent thought it preferable for the ISP to reduce their access to a few websites to help correct the problem.[49]

7.38 AusCERT concluded that end users recognise that remaining connected to the Internet while compromised 'is neither in their best interests nor in the interests of the Internet community more generally'.[50] A smaller but still significant proportion of 14 per cent took no action, even when a malware infection had been confirmed. While this latter finding is worrying, overall the survey results were considered positive and suggest that end users want information, advice and assistance.

Committee View

7.39 The AISI is an innovative and world leading initiative that illustrates the benefit of public-private cooperation to address a significant societal problem. However, the Committee is concerned that, in this current form, the AISI is unlikely to realise its full potential unless there is a clearer commitment to notify an end user when their PC is operating as a zombie computer. The impact of AISI on remediation by end users is ad hoc and difficult to measure because of the wide variation in ISP responses. The Committee also noted there was no evidence that AISI data is shared with CERT Australia to support other threat assessment or emergency response functions.

7.40 As Chapter 2 demonstrates, there is wide agreement that end users are highly vulnerable to being coopted into botnets that are the primary tools of mass automated global cyber crime. The problem of malware has grown as cyber criminals become increasingly sophisticated and this trend is predicted to continue. The expansion in the number of residential and business Internet connections will also continue to impact on the scope of the problem.

7.41 In the Committee's view, the size, nature and complexity of malware infections and the problem of botnets warrants a more concerted effort led by government but involving all parties in a cooperative effort to reduce the number of zombie computers operating in Australia. A more integrated model built on AISI, involving ISPs, IT security specialists, and end users in a more tightly coordinated scheme will, in our view, yield better results. That said, the Committee recognises that some ISPs will obtain their network data from their own sources.

[49] AusCERT, *Home Users Computer Security Survey 2008*, p.30.

[50] AusCERT, *Home Users Computer Security Survey 2008*, p.30.

7.42 Nevertheless, as part of an expanded but more integrated scheme, the Committee recommends that ACMA should further increase its access to network data. This should include:

- active consideration of how to increase access to network data held by global IT security companies;
- whether legal reform is desirable to protect the commercial sensitivity of data, and address the regulatory, privacy concerns and other related issues raised by IT security vendors who participated in this inquiry;
- how best AISI network data might be used to support other threat assessment and emergency response functions of government.

Recommendation 12

That the Australian Communications and Media Authority further increase its access to network data for the purpose of detecting malware compromised computers. This should include active consideration of how to increase access to network data held by global IT security companies and, in consultation with relevant departments, whether legal protections to address commercial, regulatory and privacy concerns are desirable.

Recommendation 13

That the Australian Communications and Media Authority consider how best the Australian Internet Security Initiative network data might be used to support the threat assessment and emergency response functions of government.

Internet Service Providers – E Security Code of Practice

7.43 As a result of the *E Security Review*, the Australian Government has encouraged the Internet industry to develop an e-security code of practice for ISPs. The Committee heard that the e-security code of practice is being developed by IIA as a 'voluntary industry best practice document' and that ACMA is '… only tangentially involved as an observer, despite the focus on the AISI reports present in the Code'.[51]

7.44 Mr Keith Besgrove, First Assistant Secretary, Department of Broadband Communications and Digital Economy (DBCDE), reinforced the view that getting ISPs involved is essential. He suggested that developing a voluntary code is faster than regulation:

> We have always said that if this does not work then government will have to consider firmer options because this is really serious stuff. This is damn dangerous and we have got to do something about it.[52]

7.45 Mr Peter Coroneos, CEO, IIA, asserted that the new code will encourage ISPs to address what is a 'large and growing problem' of botnets operating across their networks.[53] A consultation draft was released on the day that IIA appeared before the Committee. The Committee was advised the code would be launched by 1 December 2009; take effect in 2010 and be reviewed in 2011.[54]

7.46 The e-security code of practice is intended to coexist with the existing *Spam Code of Practice*, and, related Commonwealth, State and Territory laws on crime, consumer protection, and privacy. The new code is proposed to be voluntary, which means that ISPs are free not to participate in AISI or any other form of bot detection. It also means that ACMA lacks power to give a direction to any section of the industry in respect of these matters.

7.47 The Committee was told the voluntary code is intended to promote greater consistency in the Internet industry by:

- encouraging ISPs to be involved in the AISI scheme or use other sources to detect infected machines;
- setting out options on what might be done to notify the subscriber and reduce Internet access; and
- providing ISPs with standardised information to promote consistent basic plain English e-security messages to their subscribers.[55]

[51] ACMA, *Supplementary Submission 56.1*, p.3.

[52] Mr Keith Besgrove, DBCDE, *Transcript of Evidence*, 25 November, 2009, p.9.

[53] Mr Peter Coroneos, IIA, *Transcript of Evidence*, 11 September 2009, pp.15-16.

[54] IIA, *Submission 54*, p.8; Mr Keith Besgrove, DBCDE, *Transcript of Evidence*, Wednesday 25 November, 2009, p.9.

[55] IIA, *Internet Service Providers Voluntary Code of Practice for Industry Self-Regulation in the Area of e-Security*, (Consultation Version 1.0), September, 2009, p.9.

7.48 In effect, the intention is to codify existing practice and provide basic standardised information for use by ISPs with subscribers.[56] An ISP will have to take at least one of the listed actions to be considered code compliant. These include, for example, simply notifying the customer of the problem, a reduction in connection speed, placing the computer in a 'walled garden', temporary suspension, and, in extreme cases, disconnection of the service.[57]

7.49 The Committee noted that neither the ISPs nor IIA are expected to provide scanning software to detect malware or technical assistance to remove the bot (see discussion of remediation below). However, the ISPs can refer a subscriber to an IT security company via the IIA website.[58]

7.50 The IIA is creating an e-security branding scheme.[59] Code compliant ISPs are entitled to use the IIA Security Friendly ISP Trustmark. The brand icon (a small tortoise) will lead to a standardised information page, which in turn links to the IIA security portal.[60] The IIA security portal provides links to companies that specialise in anti-virus and e-security. The Committee was told this approach is intended to alleviate the workload for small ISPs.[61]

7.51 There was a range of views on the importance of ISP action. One witness said that, by definition, ISP action will always be reactive rather than pre-emptive, and ISPs have a limited role in protecting network integrity.[62] Another viewpoint was that ISPs could play a preventative role if they required their customers to adopt security measures before being connected to the Internet.[63]

7.52 There was also advocacy for a more integrated approach that would require an ISP to notify and refer their subscriber to a publicly funded centre for malware detection and removal. The aim would be to provide a

[56] Mr Peter Coroneos, IIA, *Transcript of Evidence*, 11 September 2009, p.15; see also, Ben Grubb, ZDNet.com.au, *Privacy Commissioner delays zombie code*, 27 January 2010.

[57] IIA, *Internet Service Providers Voluntary Code of Practice for Industry Self-Regulation in the Area of e-Security*, (Consultation Version 1.0), September, 2009, p.9.

[58] Mr Peter Coroneos, IIA, *Transcript of Evidence*, 11 September 2009, p.17.

[59] Mr Peter Coroneos, IIA, *Transcript of Evidence*, 11 September 2009, p.16.

[60] <www.tortoise.iia.net.au>.

[61] Mr Peter Coroneos, IIA, *Transcript of Evidence*, 11 September 2009, p.16.

[62] Mr Michael Sinkowitsch, Fujitsu Australia Ltd, *Transcript of Evidence*, 11 September 2009, p.54.

[63] Mr Alastair MacGibbon, Internet Safety Institute, *Transcript of Evidence*, 11 September 2009, pp.60-61.

more effective response to end user needs.[64] The issue of remediation is discussed in more detail below.

Liability of ISPs

7.53 The Committee was informed that ISPs were concerned about potential liability for losses caused by restricting or denying access to the Internet. Telstra, for example, said that:

> Under current telecommunications regulations, Telstra is required to provide and protect its cyber infrastructure from attack, but if Telstra was to take action against a retail or wholesale customer who has been identified as the sources of a cyber attack, then that customer may initiate civil court action if Telstra disconnected that customer in order to protect its infrastructure and other customers.[65]

7.54 It was recommended that carriers and ISPs be provided with immunity from third party claims for actions taken in good faith or agreed with government or industry, to protect their networks and services and customers from being used in, or in relation to, the commission of criminal offences.[66] Another contributor suggested that, in the US, some companies are already denying service to end users with infected machines and liability may not be such a significant issue.[67]

7.55 The Committee was advised that s.313 of the *Telecommunications Act 1997* (Cth) places several obligations on ISPs. These obligations arise in connection with the ISP's operation of telecommunications networks and facilities, and their supply of 'carriage services'.[68] In summary, the obligations include:

- doing the carrier's 'best' to prevent telecommunications networks and facilities from being used to facilitate a criminal offence; and
- giving Commonwealth, State and Territory authorities 'such help as is reasonably necessary' to enforce the criminal law, protect the public revenue, and safeguard national security.[69]

[64] AusCERT, *Submission 30*, pp.14-24.

[65] Telstra, *Submission 43*, p.5.

[66] Telstra, *Submission 43*, p.5.

[67] Ms Alana Maurushat, CLPC, *Transcript of Evidence*, 8 October 2009, p.27.

[68] DBCDE, *Supplementary Submission 34.1*, p.2.

[69] Subsections 313 (1)(2)(3) of the *Telecommunications Act 1997* (Cth).

7.56 If an ISP does an act in 'good faith' as part of fulfilling one of the duties it will be immune from civil action for damages in relation to that action.[70]A similar immunity is extended to the officers, employees and agents of a carriage service provider.[71] The immunity also applies to circumstances where an ISP undertakes action in compliance with a direction by ACMA.[72]

7.57 The DBCDE suggested that:

> … it could be argued that the act of responding to reports on compromised computers (e.g. computers with trojans/malware) could be considered to be reasonable action undertaken by the ISP to prevent its telecommunication networks and facilities from being used to commit cyber crimes under Commonwealth laws.[73]

7.58 The implication was that ISPs have an existing positive duty to prevent a malware infected computer from operating across the Internet. If this is correct, the existing immunity from civil action for losses arising from slowed or denied Internet access would also apply.

7.59 The Committee also sought views from ACMA on this point. The ACMA referred the Committee to the *Spam Code of Practice*, which requires each ISP to have an 'acceptable use policy' in its contract with each customer. The contract must include a clause that allows for immediate account disconnection or suspension when an ISP becomes aware a customer's computer is used for sending spam emails.[74]

7.60 The ACMA stated that, in its view, in circumstances where the ISP exercises a contractual right, such as that required by clause 7.3 of the *Spam Code of Practice*, the ISP should 'generally be able to terminate or suspend the service without adverse legal consequences'.[75]

Committee View

7.61 The industry codification of existing practice is a useful tool to promote greater participation by the many hundreds of ISPs that are not yet part of the AISI. It also encourages ISPs to access other sources of network data to

[70] Subparagraph 313(5)(a) of the *Telecommunications Act 1997* (Cth).

[71] Subsection 313(6) of the *Telecommunications Act 1997* (Cth).

[72] DBCDE, *Supplementary Submission 34.1*, p.2; subparagraph 313(5)(b) of the *Telecommunications Act 1997* (Cth).

[73] DBCDE, *Supplementary Submission 34.1*, p.3.

[74] Clause 7.3 of the IISCP; as cited, ACMA, *Supplementary Submission 56.1*, p.1.

[75] ACMA, *Supplementary Submission 56.1*, p.1.

detect zombie computers. However, the Committee is concerned that in its present form the code is not a sufficient advance on the current state of play.

7.62 First, the consultation draft merely codifies the existing range of practices, leaving the widest possible discretion to the ISP. To be code compliant an ISP need only notify a subscriber of the compromised machine to be entitled to adopt the trust mark icon. As noted above, the Committee understands that many ISPs already have either an automated system of notification, provide email advice to the customer or, in some instances of smaller ISPs, have a policy of making contact by phone to explain the problem. However, because of the wide discretion in the existing code, there is no guarantee that a compromised machine will not simply continue to operate with full access and infect other Internet users. The Committee considers that, in this respect, the proposed code sets the bar too low.

7.63 In the Committee's view, the industry code should reflect the seriousness of the situation and the unique role of ISPs as commercial gatekeepers to the Internet. The continued operation of zombie computers exposes the owner to a higher risk of identity theft and fraud, with all its attendant financial and emotional costs. If left unchecked the zombie computer continues to support criminal activities and is a public nuisance to other Internet users. The inter-connected nature of the Internet infrastructure, which is often compared to a public highway, means there is a shared responsibility for protecting the security and safety of the wider community. The Committee believes there is a strong public interest in:

- a mandatory obligation to inform end users when their IP address has been identified as linked to a compromised machine(s);
- a clear policy on graduated access restrictions and, if necessary, disconnection until the machine is remediated; and
- basic advice and referral for technical assistance for remediation (see below).

7.64 Second, the Committee is also disappointed the industry has not yet taken a more comprehensive approach to the issue. While many ISPs do provide e-security products, the code itself does not, for example, promote the use of anti-virus software at the point of connection to the Internet or other security advice or software services. This is a missed opportunity that could provide some benefits to ISPs and make a real contribution to promoting a culture of e-security

7.65 The e-security code of practice should include additional matters, such as:

- that the ISP provides basic security advice when the account is set up to assist the end user to protect themselves from hacking and malware infections; and
- acceptable use policies that include a requirement that the subscriber agree to:
  - ⇒ install anti-virus software and firewalls before the Internet connection is activated;
  - ⇒ endeavour to keep e-security software protections up to date; and
  - ⇒ take reasonable steps to remediate their computer(s) when notified of suspected malware compromise.

7.66 The inclusion of these terms would assist an ISP which is subject to a complaint before the Telecommunications Ombudsman. It also sends a clear message that end users also have a responsibility to protect themselves and other Internet users.

7.67 Third, the Committee is concerned that, although the industry and the regulator co-regulate in other areas of industry practice, this code is proposed to be voluntary. In 2003 the IIA released a draft *Cyber Crime Code of Practice,* which did not eventuate into a general cyber crime code of practice for the industry.[76] In 2004, the Parliamentary Joint Committee on the Australian Crime Commission expressed concern about the voluntary nature of that proposed code.[77] This Committee agrees with that view.

7.68 The registration of the e-security code of practice would be consistent with existing law and policy, and will ensure a greater consistency across the industry.[78] It would provide a more certain basis to the contractual relationship with subscribers and reduce uncertainty about liability. Registration would also enable ACMA to make an order if it was necessary to do so as a measure of last resort.

[76] That draft code set out to establish guidelines for cooperation in criminal and civil investigations and to promote positive relations between industry and law enforcement. It was also intended to give users confidence their privacy and the confidentiality of their transactions will be protected from unlawful intrusion; Internet Industry Code of Practice, paragraph 1.11, as cited, Joint Parliamentary Committee on the Australian Crime Commission, *Cybercrime*, March 2004, p.17.

[77] Joint Parliamentary Committee on the Australian Crime Commission, *Cybercrime*, March 2004, p.17.

[78] See, for example, existing law regulating ISPs: *Telecommunications Act 1997* (Cth), *Telecommunications (Intercept and Access) Act 1979* (Cth); and, the *Spam Code of Practice.* In relation to prohibited classified content, the Internet industry *Content Services Code* was registered under the *Broadcasting Act 1992* (Cth) in 2008; to block access to foreign online gambling sites, the IIA *Interactive Gambling Industry Code* was registered by ACMA in 2001.

Recommendation 14

That the Australian Communications and Media Authority take the lead role and work with the Internet Industry Association to immediately elaborate a detailed e-security code of practice to be registered under the *Telecommunications Act 1997* (Cth).

That the code of practice include:

- **an obligation that the Internet Service Provider provides basic security advice when an account is set up to assist the end user to protect themselves from hacking and malware infections;**
- **a mandatory obligation to inform end users when their IP address has been identified as linked to an infected machine(s);**
- **a clear policy on graduated access restrictions and, if necessary, disconnection until the infected machine is remediated;**
- **the provision of basic advice and referral for technical assistance for remediation; and**
- **a requirement that acceptable use policies include contractual obligations that require a subscriber to:**
  - ⇒ **install anti-virus software and firewalls before the Internet connection is activated;**
  - ⇒ **endeavour to keep e-security software protections up to date; and**
  - ⇒ **take reasonable steps to remediate their computer(s) when notified of suspected malware compromise.**

7.69 Finally, the Committee considers that it may be the better policy view that s.313 of the *Telecommunications Act 1997* (Cth) already imposes a positive duty to take action in response to compromised machines. However, the matter is not entirely free from doubt, and, in the absence of judicially binding authority, there is merit in reviewing the legislative provisions. The Committee notes, for example, that most subscribers are innocent victims of malware and are not knowingly or intentionally distributing malware infections to other Internet users.

Recommendation 15

That the Australian Government, in consultation with the Internet industry, review the scope and adequacy of s.313 of the *Telecommunications Act 1997* (Cth) to promote Internet Service Provider action to combat the problem of malware infected machines operating across the Internet.

Remediation of Infected Machines

7.70 As noted above, it was put to the Committee that a model that integrates AISI, ISPs and IT specialists and IT security vendors is needed to ensure ready and cost effective access to technical assistance to deal with the problem of malware infected computers.[79]

7.71 The Committee has recommended that scanning software be a feature of a centralised cyber crime reporting centre (see Chapter 5). However, the Committee was made aware that scanning software is often unable to detect malware, which has the 'ability to hide, obfuscate and subvert anti-virus scanning programs'.[80] Mr Graham Ingram, AusCERT, explained that once the malware is on the computer, it usually requires professional expertise to remove it.[81] This involves taking the computer off line, and contracting an IT technician, which can be time consuming and expensive.[82]

7.72 The Internet Engineering Task Force draft *Recommendations for the Remediation of Bots in ISP Networks* also recognises that bot removal often requires '…specialised knowledge, skills and tools, and may be beyond the ability of average users and often beyond the capabilities of IT staff.'[83]

7.73 Similarly, IIA agreed that scanning software has limits:

> Online scanning websites offer some remote scanning possibilities for users, but scanning is limited to browser's security settings.

[79] See, AusCERT, *Submission 30*, pp.14-24; AusCERT, *Exhibit 13, Internet Industry Code of Practice*, pp.1-16.

[80] AusCert, *Exhibit 13, Internet Industry Code of Practice Submission*, p.13.

[81] AusCert, *Exhibit 13, Internet Industry Code of Practice Submission*, p.13.

[82] AusCert, *Exhibit 13, Internet Industry Code of Practice Submission*, p.13.

[83] Internet Engineering Task Force, *Draft Recommendations for the Remediation of Bots in ISP Networks,* September 15, 2009; see also, AusCert, *Exhibit 13, Internet Industry Code of Practice Submission*, p.3.

> The prior installation of a 'root kit' may render such scanning ineffective. Online scans are not to our knowledge able to detect if a computer is part of a botnet, only whether it may have software installed that could render it susceptible to such. And even then, this is not infallible. The increasing sophistication and funding of the zombie threat seems to be reducing the effectiveness of such approaches.[84]

7.74 The Committee was advised of a number of overseas initiatives, including the publicly funded Japanese Cyber Clean Centre (CCC) and the recently announced German initiative (see below), that include remediation as part of a more coordinated model.

7.75 The Japanese CCC is a cooperative effort between government, ISPs and a number of IT security companies (e.g. Trend Micro, McAfee and Symantec). Symantec explained:

> Set up in 2006, the CCC initiative analyses bot characteristics, provides information on bot-infestation, promotes bot cleaning and prevention amongst Internet users in Japan. A cooperative effort between the Japan government with ISPs and security vendors, it functions along a five-step process whereby botmalware samples are collected; 'cleaners' (or anti-malware tools) are developed; infected users are identified and instructed to 'clean' their computers; 'cleaners' are downloaded by users; and the bot-malware samples are sent to participating security vendors for creation of malware signatures.[85]

7.76 The CCC conducts the malware analysis and IT specialist companies develop specific file signatures to clean the computers.[86] The CCC also allows for:

> … statistics and metrics to be developed which can then be used to track the success of the program over time and provide insights into how the malware problem is evolving and changing.[87]

7.77 IIA commented that the publication of rates of botnet infections and responses to inform policy and education campaigns is particularly useful.[88] Symantec agreed that one of the benefits is that:

[84] IIA, *Supplementary Submission 54.1*, p.1.

[85] Symantec, *Supplementary Submission 32.1*, p.6.

[86] AusCERT, *Exhibit 13, Internet Industry Code of Practice,* p.12.

[87] AusCERT, *Exhibit 13, Internet Industry Code of Practice,* p.11.

[88] IIA, *Supplementary Submission 54.1*, p.4

> A clearer understanding of the nature of bot infections within the local environment also seems to have been developed. An initiative like the CCC could lead to better situational awareness of the local bot landscape, more proactive remediation of end-users' bot-infected computers and increased public awareness.[89]

7.78 Japan's CCC FY2008 report states that the project has 'accomplished "concrete results" and gained "wide acceptance", although the number of bot infections still remained large and further effort was needed to clean up infected computers'.[90]

7.79 The IIA stressed that the Japanese model could work provided there are adequate resources to fund its operations, research and promotion. The Japanese CCC, which is fully funded by the Japanese Government and managed by a Steering Committee chaired by two Ministers, is better funded as a public body than the current approach in Australia.[91]

7.80 It was proposed that Australia adopt a similar model to 'provide practical assistance and tools to help Australian Internet users recover from serious forms of malware attacks'.[92] The ACMA concurred that while it may not clear all infections this 'would be a very good initiative'.[93]

7.81 Mr Bruce Mathews, ACMA, concluded that:

> I think that would be a good movement. I am not sure that any software is going to ever be able to disinfect everything, but certainly software is very important in part of the overall approach to this problem. Of course, there are many economic competitors in what is a very large industry, the anti-malware industry, and they may also have views on such a centre in relation to their own activities.[94]

7.82 The German Government is also working with ISPs in a similar way to Japan. The Association of the German Internet Industry, with support

[89] Symantec, *Supplementary Submission 32.1*, p.6.

[90] Cited in Symantec, *Supplementary Submission 32.1*, p.6.

[91] See <https://www.ccc.go.jp/en_ccc/index.html>; see also <http://blog.cytrap.eu/?p=287>; IIA *Supplementary Submission 54.1*, p.3.

[92] AusCERT, *Exhibit 13*, *Internet Industry Code of Practice,* p.11

[93] Mr Bruce Mathews, ACMA, *Transcript of Evidence*, 21 October 2009, p.14.

[94] Mr Bruce Mathews, ACMA, *Transcript of Evidence*, 21 October 2009, p.14.

from Germany's Federal Office for Information Security, has announced a help service that includes a telephone hotline for customers.[95]

7.83 Once a customer's computer has been identified as malware infected, the ISP can send a message to their subscriber, guiding them to the Association's website that shows them how to remove the malware. The botnet cleanup hotline gives consumer access to anti-virus specialists who provide personal assistance if it is necessary.[96]

7.84 Some individual large ISPs have also taken their own initiatives. In the US, the ISP Comcast Corporation has announced a trial of an in-browser notification 'Service Notice', that alerts a subscriber whose computer appears to be infected. The notice requests that they go to an Anti-Virus Centre for instructions on removing the bot from their computer.[97]

Committee View

7.85 As stated above, the Committee is of the view that a more integrated model built on AISI, involving ISPs, IT security specialists, and end users in a more tightly coordinated scheme will yield better results in the detection and remediation of compromised machines. A more coordinated approach would also ensure a reliable source of data from which to tackle the botnet problem in Australia.

7.86 The Committee has addressed each element of this scheme in the sections above with recommendations to:

- expand ACMA's access to network data to detect malware infected machines;
- a mandatory e-security code of practice for the ISPs to address compromised machines operating across their networks; and
- new contractual obligations for end users to strengthen prevention and cure of infected machines.

7.87 The scheme would be incomplete without addressing the fourth element – the issue of remediation. There was a clear message to the Committee that

[95] *AusCERT, Exhibit 23*, p.3; Eco-Association of the German Internet Industry, *Quick remedy for botnet infections*, 14 December 2009; John Leyden, *German ISPs teams up with gov agency to clean up malware*, The Register, 9 December 2009.

[96] *AusCERT, Exhibit 23*, Eco-Association of the German Internet Industry, *Quick remedy for botnet infections*, 14 December 2009; John Leyden, *German ISPs teams up with gov agency to clean up malware*, The Register, 9 December 2009.

[97] *AusCERT, Exhibit 23,* Comcast, *Comcast Unveils Comprehensive 'Constant Guard' Internet Security Program*, Press Release, 8 October 2009.

end users and small and medium sized businesses would benefit from direct and cost effective assistance to not only detect malware but also to remediate malware infected computers. The Committee considers that there needs to be a more direct pathway for end users to access malware detection software and bot removal services that are readily available, cost effective and provide a timely solution to the problem.

7.88 This will necessarily involve closer public and private partnerships, with one or more IT vendors and/or not for profit specialist service providers such as AusCERT. It could involve IIA in providing the technical helpline service, as is the case in Germany. Alternatively, a model that is closer to the Japanese approach may be more effective and, if designed correctly, appropriate to the needs of Australian end users. It may also be possible to integrate such a scheme with the national cyber crime reporting centre recommended in Chapter 5.

Recommendation 16

That a more integrated model for the detection and removal of malware, built on the Australian Internet Security Initiative, be implemented. The new scheme should involve the Australian Communications and Media Authority, Internet Service Providers, IT security specialists, and end users in a more tightly coordinated scheme to detect and clean malware infected computers.

Compromised websites

7.89 As noted in Chapter 2, the corruption of legitimate websites has taken over from spam as the main way malware is spread to innocent end users.[98] For example, Symantec told the Committee that:

> Most web based attacks are launched against users who visit legitimate website that have been compromised by attackers in order to serve malicious content. A popular, trusted site with a large number of visitors can yield thousands of compromises from a single attack, thus providing an optional beachhead for distributing malicious code.[99]

[98] ACMA, *Submission 56*, p.15; Symantec, *Submission 32*, p.2.

[99] Symantec, *Submission 32*, p.2.

7.90 Given the 'role of compromised websites as the primary vector for cyber crime' ACMA said that:

> Developing a comprehensive and timely response to this problem needs to be a key and urgent focus of all areas of internet governance and by key internet industry stakeholders.[100]

7.91 ACMA expressed its concern that website owners are not aware that this is 'one of the most significant e-security problems on the Internet':

> …there needs to be a much greater focus on maintaining the e-security on websites, particularly websites that have forms for entering data onto the website, because they are the most vulnerable to being infected.[101]

7.92 The education of 'website owners would help raise awareness of this problem and how to rectify the compromise'.[102]

7.93 The Committee asked ACMA to consider in more detail what proactive strategies Australia could take; and, what legal powers and technical and personnel resources are needed to implement a more strategic response to infected websites. In supplementary evidence, ACMA advised that a range of options exist for addressing the problem of infected websites.[103]

7.94 These include a web compromise reporting and detection system:

> Such a system could operate under a similar framework to that of the AISI, that is, the ACMA could obtain data on compromised web pages from various sources (including developing an internal capability), collate this data, and provide daily aggregated reports to ISPs identifying infected web pages residing on their networks. In addition to ISPs, domain owners and hosting companies could also be included.[104]

7.95 The reporting and detection system could be supported by a registered industry code outlining industry procedures for dealing with infected websites and notifications of infected websites could apply:

> As the ACMA has the power to enforce the provisions of registered codes, this could be pertinent in cases where there was a need to direct a service provider to remove malicious content. A

[100] ACMA, *Submission 56*, p.15.

[101] Mr Bruce Mathews, ACMA, *Transcript of Evidence,* 21 October 2009, p.5.

[102] ACMA, *Submission 56*, p.15.

[103] ACMA, *Supplementary Submission 56.1*, p.5.

[104] ACMA, *Supplementary Submission 56.1*, p. 5.

> registered code would also serve the purpose of indemnifying ISPs who act on reports of infected websites.[105]

7.96 The Committee was told the problem of compromised websites was considered during the *E-Security Review*. AGD said the 'Cyber Security Policy and Coordination Committee agencies will further explore the legal issues of infected websites' and this 'work will guide any allocation of new resources and powers as required'.[106]

7.97 In the meantime, it has been reported that Microsoft recently joined forces with Symantec, The Shadowserver Foundation and International Secure Systems to obtain a US District Court order to compel Verisign, the .com domain registry, to sever 273 'malicious domain names'.[107] This civil action was part of Operation b49 to dismantle the Waledac botnet that, according to Microsoft, has the capacity to send 1.5 billion spam emails a day. The civil action highlights the integral role of Domain Name Registrars in a more strategic approach to tackling the problem of botnets.

Committee View

7.98 The Committee is concerned that the targeted infection of legitimate and trusted websites is now the number one vehicle for distributing malware, and poses a significant threat to the integrity of the Internet. The evidence indicated that it is practically impossible for any ordinary consumer to detect when a website has been infected, leaving them exposed to malware infection, identity theft and fraud. This is an area in which consumer education is less useful. However, an education program geared toward small and medium sized businesses would be useful, especially for businesses that transact with clients online and, in that process, take personal and financial information. Education initiatives are discussed in Chapter 10.

7.99 It is also a matter of concern that the regulator, ACMA, lacks technical capacity to detect infected websites or powers to order the remediation or the take down of an infected website. The Committee sees considerable merit in building on the success of the AISI to tackle the problem of infected websites supporting malicious code. The problem was identified

[105] ACMA, *Supplementary Submission 56.1*, p.5.

[106] AGD, *Supplementary Submission 44.2*, p.4.

[107] Nick Wingfield, *Microsoft wins 'botnet' order,* The Wall Street Journal Asia, 26 February 2010, p.6; William Jackson, *Microsoft unplugs spammer botnet with legal strategy*, Government Computer News, 1 March 2010 http://gcn.com/Articles/2010/03/010, viewed 3 March 2010.

by the *E Security Review*, but the process and timeframe for developing a legal and a technical response is unclear.

7.100 The Committee is also aware there are a range of complex issues to be worked through and some potential overlap with the problem of fraudulent sites established to launch phishing attacks. This raises a range of related issues about the responsibilities of domain name registries, registrars and resellers to verify the identity of applicants, cooperate with law enforcement authorities, and provide procedures for rapid takedown of illegitimate infected sites or those spreading spam or that are part of a botnet. The Domain Name System and the role of registries, registrars and resellers are discussed in more detail below.

Recommendation 17

That the Australian Communications and Media Authority be funded to develop a system that can obtain data on compromised web pages from various sources (including developing an internal capability). This data be collated and provided as daily aggregated reports to Internet Service Providers identifying infected web pages residing on their networks.

That in addition to Internet Service Providers, domain owners and hosting companies also be included in the new scheme.

Recommendation 18

That the system for reporting and detecting compromised web pages proposed in recommendation 17 be supported by a registered industry code that outlines industry procedures for dealing with infected websites.

That the Australian Communications and Media Authority be empowered to enforce the provisions of the registered code, including, for example, where there is a need to direct a service provider to remove malicious content.

That Internet Service Providers and hosting companies who act on reports of infected websites be indemnified against claims for losses.

Reporting Spam Email

7.101 *SpamMatters* is a software program developed by ACMA that gives end users an easy automated way of reporting of spam email directly to ACMA. There are 290,000 registered users and 41 million reports of spam since the program was launched on 30 May 2006. The total number of Internet connected residences and businesses in Australia has been estimated by the Australian Bureau of Statistics (ABS) in 2008 to be at eight million.[108] Against this background, while the number of registered *SpamMatters* users is significant, it remains a small proportion of the total number of end users in Australia.

7.102 The software can be downloaded from the ACMA website. It installs a plug-in to Microsoft Outlook or Outlook Express. Once installed a button appears in the subscriber's email system that allows the user to select the spam email and click the button to send the spam directly to ACMA 'in a forensically intact manner'.[109] This means the headers are intact, which is important for investigative purposes.

7.103 There is a form of *SpamMatters* that appears as a button in the Telstra webmail client. ACMA advised that a very large number of the 290,000 registered for *SpamMatters* are Telstra webmail subscribers:

> This is a great initiative. We get lots of very good data from that button, and we have been encouraging other ISPs as well to move in that direction and install a similar button. We hope to be successful in encouraging more ISPs to participate over time.[110]

7.104 ACMA wants to encourage more ISPs to install a spam button in their webmail systems, because this is easier to maintain than updating the *SpamMatters* software with each successive release of Microsoft operating and email systems.[111]

7.105 The spam reported via *SpamMatters* is the spam email that has got through ISP filters and any spam filtering software, so it is not representative of general spam on the Internet.[112] It is used to identify 'campaigns of spamming activity' such as phishing email campaigns, which are reported regularly to the AFP.[113] In the US, the US CERT located in the Department

[108] Australian Bureau of Statistics, *Internet Activity*, Australia, Cat. No. 8153.0, December 2008.

[109] Mr Bruce Mathews, ACMA, *Transcript of Evidence,* 21 October 2009, p.8.

[110] Mr Bruce Mathews, ACMA, *Transcript of Evidence,* 21 October 2009, p.8.

[111] Mr Bruce Mathews, ACMA, *Transcript of Evidence,* 21 October 2009, p.8.

[112] Mr Bruce Mathews, ACMA, *Transcript of Evidence,* 21 October 2009, p.8.

[113] Mr Bruce Mathews, ACMA, *Transcript of Evidence,* 21 October 2009, p.8.

of Homeland Security is the central location for the online reporting of phishing emails.[114]

7.106 The Committee was told that ACMA is also working on the next generation of *SpamMatters,* which will include an 'interrogation system' to 'improve the analysis of the data'.[115] This will enable ACMA to 'identify trends within that data and also use it to extract information on what we consider to be infected IP addresses, which will feed back' into the AISI in a more 'sophisticated manner than is currently done through the *SpamMatters* software'.[116]

7.107 There was also evidence that spamming is occurring via social networking sites as commercial operators seek to find new ways of messaging potential consumers.[117] The *Spam Act 2003* (Cth) applies to emails, and there is a question mark about its application in the context of social networking media and in a range of other instant electronic messaging systems. This issue is discussed in Chapter 6.

Committee View

7.108 The Committee commends ACMA on developing an automated reporting system that gathers useful intelligence and can be used to feed into law enforcement efforts. In particular, it looks forward to a future briefing on the development of *SpamMatters* that links this intelligence to AISI data.

7.109 However, the Committee is disappointed this innovation has not been widely taken up by ISPs, which would, in the Committee's view, provide the most effective way of increasing the reach of *SpamMatters*. The wider adoption of the *SpamMatters* button by ISPs would substantially increase the level of spam reported to ACMA.

7.110 The Committee understands it is a requirement of the *Spam Code of Practice* that ISPs give their customers spam filter options, and advise customers how to report spam, as well as accepting spam reports from their own customers.[118]

7.111 In 2006, the then Department of Communications, Information Technology and the Arts (DCITA) reviewed the *Spam Act 2003* and recommended that no change be made to the role of ISPs under the

[114] <http://www.us-cert.gov/nav/report_phishing.html>, viewed 1 March 2009.

[115] Mr Bruce Mathews, ACMA, *Transcript of Evidence,* 21 October 2009, p.9.

[116] Mr Bruce Mathews, ACMA, *Transcript of Evidence,* 21 October 2009, p.9.

[117] Australian Computer Society, *Transcript of Evidence,* 9 October 2010, pp.34-35.

[118] Clauses 6, 10.1 and 10.4, *Spam Code of Practice.*

Telecommunications Act 1997 (Cth) or the *Spam Code of Practice*.[119] However, there was limited opportunity to evaluate the effectiveness of the *Spam Code of Practice*, which only came into force on 16 July 2006.[120]

7.112 Since then spam has developed as a vector for the distribution of malware and the proliferation of scams and phishing attacks. It would be timely for ACMA and the IIA to review the *Spam Code of Practice*. In particular, the reporting of spam via *SpamMatters* through the ISPs email services should be considered for inclusion in any revised code. That review should include consumer representatives such as the Australian Communications Consumer Action Network and the Australian Competition and Consumer Commission as well as the Internet industry.

Recommendation 19

That the Australian Communications and Media Authority and the Internet Industry Association review the *Spam Code of Practice* to assess the effectiveness of current industry standards for the reporting of spam.

That serious consideration be given to obliging Internet Service Providers to include the Australian Communications and Media Authority's *SpamMatters* program as part of their email service to subscribers.

Domain Name System

7.113 The Domain Name System (DNS) is a hierarchy for the naming of computers and other devices connected to the Internet. The authority to allocate and sell the licence to use a domain name is distributed via a system of registries, registrars and resellers.[121]

[119] DCITA, Report on the *Spam Act 2003* Review, June 2006, p.77.

[120] DCITA, Report on the *Spam Act 2003* Review, June 2006, p.104.

[121] Domain name servers (DNS) convert web addresses into Internet Protocol addresses and routes the computer user to the correct location. Thirteen root DNS servers cover the entire Internet along with a number of local servers. Once reconfigured, the DNS can send users to any number of websites and seriously compromise the entire Internet system. In the case of Domain Name Server poisoning, the list of addresses in a DNS server are altered so that a legitimate URL address points to an illegitimate Internet Protocol address, the fraudulent web

7.114 The Internet Corporation for Assigned Names and Number (ICANN) explained that:

> … every domain name around the world ends with a top-level domain (TLD); these are the 2 or more letters that come after the dot. There are currently two types of TLDs: generic top-level domain (gTLDs) such as .com, .mobi, and .info, and country code top-level domains (ccTLDs) such as .uk, .br, and .cn. A gTLD or a ccTLD is managed by a registry operator, an organization that maintains the registry database, including the nameserver information for names registered in the TLD.[122]

7.115 The ease of access to domain names, the hijacking of domains, and hijacking of the DNS raise e-security issues in both the technical and management aspects of DNS.

7.116 Some witnesses argued that the regulation of Domain Name Registrars and Resellers should be reviewed and, in particular, a 'know your customer' regime instigated.[123] For example, the Australian Computer Society expressed the view that ICANN should raise the performance of registrars and require more vigilance over the way domain names are allocated.[124] While ABACUS - Australian Mutuals recommended legislation to prevent criminals obtaining domain names to engage in phishing:

> Abacus urges the committee to examine in detail the regulation of domains and to consider stronger regulation of domain registration and the internet generally. The ease of establishment and hijacking of sites for criminal purposes has affected mutual ADIs since 2003 and the threat is growing. In 2009 two mutual ADIs experienced sustained cyber attacks that affected service delivery to members.[125]

7.117 AusCERT also stressed the important role of DNS registration and said that:

> "Self-regulation" exists among ISPs and Domain Name Registrars but can be problematic as potential conflicts of interest arise

site (Brody, R.G., Mulig, G., and Kimball, V. 2007, '*Phishing, pharming and identity theft*', Academy of Accounting and Financial Studies Journal) as cited AFP, *Submission 25,* p.4.

[122] <http://www.icann.org/en/topics/new-gtlds/strategy-faq.htm>, viewed 1 March 2010.

[123] See, for example, AusCERT, *Submission 30*, p.15; Abacus – Australian Mutuals, *Submission 55*, p.4; Australian Computer Society, *Transcript of Evidence*, 9 October 2009, p.39.

[124] Australian Computer Society, *Transcript of Evidence*, 9 October 2009, p.39.

[125] Abacus – Australian Mutuals, *Submission 55*, p.4.

> between taking action that is in the interests of the external community to what may be perceived to be detrimental to their own commercial interests. For example, Domain Name Registrars could be more discerning and adhere to more stringent processes before registering domains designed to support criminal activity. The deregistration of domains used for fraudulent activity could also be substantially improved.[126]

7.118 The Committee was advised that the Anti-Phishing Working Group[127] (APWG) has developed *Anti-Phishing Best Practices Recommendations for Domain Name Registrars.* AusCERT argued that if registrars around the world adopted the APWG best practice guide, this would help prevent some types of cyber crime.[128] The APWG recommendations address three core issues:

- evidence preservation for investigative purposes;
- proactive fraud screening; and
- phishing domain takedown.[129]

Generic Top Level Domain

7.119 The ICANN is the international not for profit, multi-stakeholder body which is responsible for coordinating the DNS. Mr Paul Twomey, Senior President, ICANN explained that ICANN is not 'the governor of the internet' but coordinates the domain name system and, among other things, allocates the protocols for the IP addressing system.[130]

7.120 ICANN sets the policy for all generic top level domains such as .com, .net, .org, and .info but does not set policy for the country code top level domains. In practice, this means that ICANN sets the rules for registries and accredits registrars for the gTLDs. For example, VeriSign Inc. is the domain name registry for .com and .net under a binding agreement with ICANN.

7.121 ICANN has no authority to accredit the registrars that operate in the country code Top Level Domains (ccTLDs), such as '.au', '.nz' and '.uk' as each country has different systems in place regulating their country code top level domain. The regulation of country code level domains is a matter

[126] AusCERT, *Submission 30*, p.15.

[127] The APWG is an international industry association focused on eliminating phishing.

[128] AusCERT, *Submission 30*, p.15.

[129] APWG, *Best Practices Recommendations for Registrars*, October 2008, p.1.

[130] Mr Paul Twomey, Senior President, ICANN, *Transcript of Evidence*, 8 October 2009, p.1.

for each country. In the Australian context, the registry is called AusRegistry and is administered by .auDA.[131]

7.122 Mr Paul Twomey, ICANN, explained that security was not part of the design of the Internet, which originated as a research network in the university sector. ICANN has:

> … increasingly observed the use of the DNS as an aspect of how botnets operate within the Internet ecosystem – as a means of pointing attacks at targets; as a mechanism for malware to receive commands and updates; and the DNS itself as a target of such attacks.[132]

7.123 ICANN said it was faced with 'retrofitting security back inside the protocols' through the installation of a 'domain name system security extension protocol' (known as the Root Server DNSSEC):

> DNSSEC is basically a way of digitally signing a domain name so that, if you were to go to a particular site and the site showed that it had been signed, you would have confidence that was authoritative material and had been put in by the owners of the site. It does not fix all of the security issues but it certainly diminishes the risk of spoofing.[133]

7.124 The DNSSEC is discussed in Chapter 11. During evidence, ICANN said that the DNSSEC may not prevent the misuse of domain names but it will assist 'police, the banks and other technical people who work in this area' to identify 'domain names literally within minutes when they're being used for … attacks.'[134] Mr Twomey also said that, as part of the planned expansion of the gTLDs, ICANN will require all new top-level domain applicants to implement DNSSEC.[135]

7.125 ICANN maintains legally binding contracts with the gTLD registrars, which outline a number of obligations. For example, the registrar Accreditation Agreement (RAA) provides that registrars must submit to ICANN data such as the name and addresses of registrants and the IP

[131] In fact, there are five country codes associated with Australia - .au for Australia, .cc for Cocos Islands, .cx for Christmas island, .hm for Heard and MacDonald Island and .nf for Norfolk Island.

[132] ICANN, *Submission 40*, p.1.

[133] Mr Paul Twomey, Senior President, ICANN, *Transcript of Evidence*, 8 October 2009, p.2; the domain name system security extension protocol is discussed in Chapter 11 of this report.

[134] ICANN, *Supplementary Submission 40.1*, p.1.

[135] Mr Paul Twomey, Senior President, ICANN, *Transcript of Evidence*, 8 October 2009, p.2

addresses of the primary and secondary name servers used by the registered name. The DBCDE said, however, that:

> At present there is no requirement on ICANN accredited registrars to verify the identity of registrants, although in many cases the use of an alias would be a breach of the terms and conditions of registration.[136]

7.126 Elsewhere it has been noted that gTLDs are:

> … subject to fewer exclusions based on where the registrant resides or does business. For example, most gTLD's do not require the registrant to indicate residency, in or a business connection with, a particular country.[137]

7.127 Ms Holly Raiche, Executive Director, Australian Internet Society also explained that identity verification standards vary across the industry:

> If you want to be a .com.au, you have to [provide] an ABN which proves that you are not only an individual but that you are also a company. To get a .com you just have to produce a credit card number and name.[138]

7.128 The evidence also indicated that simple measures such as requiring the three digit security code that appears at the back of a credit card are not mandated but would eliminate a lot of 'card not present' fraud on the DNS.[139]

7.129 In relation to, for example, domain name hijacking, ICANN's own Security and Stability Advisory Committee (SSAC) identified weaknesses in the registration and administration processes as far back as 2005.[140] The SSAC found that:

> … domain name hijacking incidents are commonly the result of flaws in registration and related processes, failure to comply with

[136] Mr Paul Twomey, Senior President, ICANN, *Transcript of Evidence*, 8 October 2009, p.1-12; DBCDE, *Submission 34.1*, p.1.

[137] Mr Neil Brown QC, *The New Internet – The Expansion of Top Level Domains – An Update*, Domain Times, <http://www.domaintimes.info/>, viewed 1 March 2010.

[138] Ms Holly Raiche, Executive Director, Internet Society of Australia, *Transcript of Evidence*, 9 October 2009, p.6.

[139] Ms Holly Raiche, Internet Society of Australia, *Transcript of Evidence*, 9 October 2009, p.6.

[140] As noted in Chapter 2, 'domain hijacking' is where a cyber criminal takes control of a domain name by stealing the identity of a domain name owner, then uses this domain name to host a malicious website. 'Typo-squatting' is also sometimes known as website hijacking. This where a person registers domain names with a common typographical error in an established domain name to divert traffic to an illegitimate site.

> the transfer policy, and poor administration of domain names by registrars, resellers, *and*, registrants.[141]

7.130 A widespread lack of security measures has been identified as one of the risks that will accompany the introduction of hundreds, and, possibly, thousands of new websites when ICANN increases the number of gTLDs to accommodate the demand for domain names.[142] In response to e-security concerns, ICANN said that contracts with new gTLDs will require new measures including:

- an anti-abuse policy that details procedures for addressing reports of malicious conduct occurring via registered domain names including how rapid takedown/suspension of those names would occur;
- a publicly identified designated anti-abuse point of contact responsible for taking action in support of these policies; and
- "thick WHOIS" data available at the registrar level which will facilitate action by specifying domain names and identifying individuals involved in potential malicious conduct.[143]

7.131 The Committee was assured that ICANN's proposed measures will be mandatory, and are intended to address a range of malpractice and malfeasance problems. ICANN has also proposed 'voluntary verification programs' for 'high security zones' that will establish criteria for how:

> …registries and registrars will establish stronger controls over who gets to register domain names in those TLDs, as well as operational IT security controls to improve trust that registered names will not support malicious code.[144]

7.132 The policy for the new agreements and some of these technical measures are currently under debate in the DNS community.

7.133 Finally, ICANN informed the Committee that it continues policy development on the basic Registrar Accreditation Agreement (RAA) between itself and existing registrars.[145] Ms Holly Raiche, Australian

[141] ICANN, Security and Stability Advisory Committee, *Domain Name Hijacking: Incident, Threats, Risks and Remedial Actions*, July 2005, p.5.

[142] ICANN, New gTLD Program Explanatory Memorandum, *Process for Amendments to New gTLD Registry Agreements*, 15 February 2010; ICANN, New gTLD Explanatory Memorandum, *Mitigating Malicious Conduct*, 3 October 2009.

[143] More detail is available at <http://www.icann.org/en/topics/new-gtlds/mitigating-malicious-conduct-04oct09-en.pdf>; ICANN, *Supplementary Submission 40.1*, p.1.

[144] Mr Paul Twomey, Senior President, ICANN, *Transcript of Evidence*, 8 October 2009, p.9-10.

[145] ICANN, *Supplementary Submission 40.1*, p.3.

Internet Society, also said there is progress toward better protection for registrants:

> In terms of what registrars do, there is now cooperation between the 'At-Large' community and the generic names organisation to develop a registrants charter of rights, which is going to focus on what registrars should do to look after registrants.[146]

Country Code Top Level Domain Name

7.134 In Australia, the .au Domain Administration (.auDA) is a private company responsible for the accreditation of registrars, and regulates numerous registrars and resellers of website names in the .au space.[147] The Committee invited .auDA to make a submission to the Inquiry but none was forthcoming.

7.135 Currently there are approximately thirty companies accredited by .auDA as registrars selling second level domain names under the .au TLD (.com.au, .edu.au etc). In 2003, .auDA estimated there were approximately 725 registrar appointed resellers and other companies selling .au domain names without a formal agreement with an accredited registrar.[148] DBCDE explained that neither:

> .auDA nor ICANN have direct contractual relationships with resellers. However, in both the gTLDs and .au resellers operate under an agreement with their registrar, which must include minimum terms and conditions.[149]

7.136 The *.au Domain Name Suppliers Code of Practice* explicitly applies to all registrars and their 'appointed resellers' and forms part of the *Registrar's Agreement.*[150] The *Registrar's Agreement* requires that any subsequent 'contract, arrangement or understanding' between a registrar and reseller for a Reseller's Licence must require the reseller to comply with .auDA's published policies.[151] The Australian system was said to be more advanced

[146] Ms Holly Raiche, Executive Director, Internet Society of Australia, *Transcript of Evidence,* 9 October 2009, p.1; see also, ICANN, *Supplementary Submission 40.1*, p.3.

[147] For example, the gov.au Domain Name Registrar function is delegated to the Australian Government Information Management Office.

[148] .auDA, *Proposed Changes to the Regulation of Registrar-Appointed Resellers*, October 2003, pp.1-3.

[149] DBCDE, *Supplementary Submission 34.1*, p.1.

[150] See, clause 3 of the *.au Domain Name Supplies Code of Practice,* 2004-04, 14 October 2004.

[151] Clause 15.4 of the .auDA *Registrar Agreement* (Approved Version 3-1 June 2008).

than in many countries and the *Domain Name Supplies Code of Practice*, which applies in Australia, does not apply internationally.[152]

7.137 The Committee was told that under subclause 9.1.2 of .auDA's non-negotiable *Registrar Agreement*, registrars must 'use reasonable endeavours' to verify the information provided in domain name applications. Equally, under .auDA's published policies registrants must 'warrant that the information that they provide is true, accurate and complete'. [153]

7.138 The DBCDE said that '… .auDA has advised that a "warranty"provided by the Registrant is considered sufficient' and there are a range of mechanisms used in the industry, 'some for instance ask for ACN or ABN numbers'.[154] However, DBCDE said that even where a business or company name is produced it is not known whether this information is checked against the Federal and State databases.[155]

7.139 The DBCDE agreed that identity verification in the .au name space is an important issue and .auDA has undertaken to consider how identity verification procedures could be improved.[156]

7.140 There is no statute law that deals specifically with domain name registration although the *Trade Marks Act 1995* (Cth) will affect the choice of name. The Committee asked what enforceable legal obligations exist to require an Australian Domain Name Registrar to remove a domain name that is associated with phishing or some other forms of illegal activity. DBCDE advised that:

> General domestic Australian laws, such as the *Crimes Act 1900*, the *Criminal Code 1995*, and the *Trade Practices Act 1974*, may apply to the conduct of registrars, depending on the specific jurisdictional circumstances. Provisions relating to theft, unauthorised access and misleading and deceptive conduct may apply to registrars that are complicit in a breach of these laws.[157]

7.141 The importance of Domain Name Registrars cooperating to refrain from registering or to disable websites involved in fraud or misleading and

[152] Ms Holly Raiche, Internet Society of Australia, *Transcript of Evidence*, 9 October 2009, p.39.

[153] DBCDE, *Supplementary Submission 34.1*, p.1.

[154] DBCDE, *Supplementary Submission 34.1*, p.1.

[155] DBCDE, *Supplementary Submission 34.1*, p.1.

[156] DBCDE, *Supplementary Submission 34.1*, p.1.

[157] DBCDE, *Supplementary Submission 34.1*, p.1.

deceptive conduct was highlighted by the Australian Competition and Consumer Commission (ACCC).[158] The ACCC told the Committee that in:

> Late 2008, the activities of the Designer Brand Outlet website were brought to the ACCC's attention by the US Federal Trade Commission, after reviewing complaints made by a number of overseas consumers to the eConsumer.gov website.[159]

7.142 The Committee was told that the 'Domain Name Registrar disabled the website and the bank where the website's merchant facility was held, suspended the service after conducting its own inquiries'.[160] In another example, a website that purported to be the official booking site for the Sydney Opera House was hosted and administered in the USA by US Domain Name Registrar NameSecure Inc. In that case, the offending material was removed but there was no order to take down the entire site, which was part of other legitimate business activity.[161]

7.143 Cooperation to deregister domain names that host malware is also important for dealing with the problem of botnets. As mentioned previously, recent civil action by Microsoft and Symantec resulted in an order compelling Verisign to sever over 200 domain names in the US as part of a strategy to dismantle the Waledac botnet.

Committee View

7.144 The Committee agrees with the principle expressed by the APWG that organisations that are part of the infrastructure of the Internet—ISPs, registries, registrars and resellers—have an obligation to take reasonable steps to protect the stability and security of the Internet.

7.145 There are a range of potential risks that Domain Name Registrars and Resellers should guard against in the sale, renewal and transfer of domain names. Preventing fraudulent acquisition of a domain name to conduct phishing attacks requires stringent identity verification. Preventing the reservation and sale of domain names for websites intended to be used for

[158] ACCC, *Submission 46*, p.7.

[159] ACCC, *Submission 46*, p.7.

[160] ACCC, *Submission 46*, p.7.

[161] *ACCC v Chen* [2003] FCA 897 at 25; ACCC, *Submission 46*, p.7; Justice Sackville granted declaratory relief and an injunction under the *Trade Practices Act 1952* (Cth) to mark its disapproval. The injunction in this case was granted to facilitate cooperation with the US Federal Trade Commission to take measures under US law to prevent Mr Chen from publishing misleading or deceptive material relating to the Sydney Opera House.

scams also requires more stringent regard for the rights of others.[162] In these instances the domain name is part of the misleading and deceptive conduct enabling fraud.

7.146 The Committee notes that the existing gTLD system is relatively small, with only 21 gTLDs, but the proposed expansion of the gTLD will lead to hundreds and eventually thousands of new registries worldwide. Internationalised Domain Names will appear in global languages including Chinese, Russian, Thai and so forth. The Committee urges ICANN and the Internet community to adopt robust measures to ensure the DNS registration system is not used to undermine the legal protection of consumers and businesses from phishing attacks and fraud.

7.147 In the current gTLD policy development process, ICANN should ensure that the APWG *Anti-Phishing Best Practices Recommendations* are incorporated and implemented in the gTLD Agreements. It is vital that these issues are addressed and clear policy on e-security measures are settled and adopted *before* ICANN massively expands the gTLD system.

7.148 The Committee supports proposals for new measures such as the vetting of registry operators and the deployment of DNSSEC technology. The Committee believes these agreements should also include:

- measures to prevent the registration of fraudulent sites;
- requirements for rapid take down of fraudulent domain names;
- requirements for the take down of domain names that host malware; and
- cooperation with law enforcement, consumer protection agencies and national regulators, such as ACCC, Australian Securities and Investment Commission (ASIC) and ACMA.

7.149 At the country code level, the Committee recognises that .auDA policies may be more advanced than in some other counties. For example, .auDA requires an applicant to have a registered trade mark, company or registered business. However, the Committee is still concerned that the existing *Registrar Agreements* and the *Domain Name Suppliers Code of Practice* does not impose more stringent requirements for:

- identity verification;

[162] The standard definition of 'phishing' is fraudulent activity to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication.

- cooperation with law enforcement authorities;
- clear procedures for the deregistration of fraudulent sites; or
- deregistration of compromised sites persistently identified as part of a botnet.

7.150 As the APWGP has pointed out, better fraud protection at the registration end of the process will contribute to combating phishing, improve the protection of customers and reduce operating costs. Without better front end processes there is likely to be a growing number of reports of abuse and requests to take down sites identified as phishing sites.[163]

7.151 The same principle also applies in the wider context of scams and trade mark infringements that are increasingly committed over the Internet. In the Committee's view, there should be clear rules that prevent the reservation, sale and registration of domain names that are intentionally similar to established companies and other websites.[164]

7.152 The problem of websites that intentionally host malware or are unknowingly infected also needs to be addressed in an industry code of conduct. Such sites must be remediated or, if necessary, severed from the Internet as part of a strategy to tackle botnets.

7.153 In Australia, as elsewhere, the domain name registration system is a self regulated industry involving numerous registrars and many hundreds of resellers. The DNS is a critical element of the digital economy that intersects with established common law and statutory regimes in trademarks, trade practices, privacy, consumer protection, crime prevention and law enforcement. There is no statute law that deals specifically with domain name registration or regulates the rights and obligation of Domain Name Registrars, resellers and registrants.

[163] The APWG best practice guide applies only to domain names registered solely for a fraudulent or criminal purpose. The procedures recommended do not apply to websites of a legitimate domain that is compromised and used by criminals to attack or compromise other computers; APWG, *Best Practices Recommendations for Registrars*, October 2008, p.3.

[164] *British Telecommunications plc v One in a Million Ltd* [1998] 4 All ER 476, [1999] 1 WLR 903, [1999] FSR 1, [1998] NLJR 1179, [1998] All ER (D) 362 (Held: the court has jurisdiction in a passing off action to injunct the registration of a domain name calculated to infringe the rights of others. The registration was regarded as having equipped another with an instrument of fraud. A threat to infringe the trade mark of another was established because the defendant (registrant) sought to sell domain names which were confusingly similar to registered trademarks); see also *.auDomain Administration Ltd v Network.com.au Pty Ltd* [2004] ATMO 36 (29 June 2004) where the registration of www.network.com.au as a trade mark was opposed on the grounds that the company was not the licence holder of the domain name.

7.154 The Committee did not take detailed evidence on all aspects of the regulation, standards and practices in the domain name registration system generally. The Committee believes that a wider parliamentary inquiry into the operation of this relatively new sector is justified to examine industry practices. That inquiry should include an examination of the:

- nature, scope and interaction of rights and obligations of registrars, resellers and registrants in relation to each other and other rights holders; and
- the powers of law enforcement authorities, and regulators such as the ASIC, ACCC, ACMA and IP Australia.

Recommendation 20

That the Australian domain name registration industry be subject to a code of conduct that is consistent with the Anti-Phishing Working Group *Best Practices Recommendations for Registrars*.

The code of conduct should:

- **enumerate the type of information that should be collected during the domain name registration process by the registrar, that would help to preserve evidence and assist law enforcement authorities;**
- **identify processes that should be put in place to identify fraudulent activity before the domain name registration takes effect; and**
- **provide clear procedures for responding to requests for rapid take down of fraudulent sites and sites that host malware.**

Recommendation 21

That the Minister for Broadband, Communications and the Digital Economy make a reference to the House of Representatives Standing Committee on Communications to inquire into the regulation, standards and practices of the domain name registration industry in Australia.