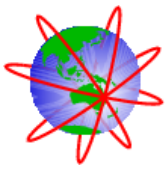


AusCERT

Australia's National Computer Emergency Response Team

Review of Australian Privacy Law

AusCERT Submission

7 December 2007

Summary

The Australian Law Reform Commission (ALRC) has released a discussion paper (*Review of Australian Privacy Law* DP 72)[1] on proposed changes to various Australian privacy laws at federal and state levels. AusCERT's submission contains its views on some of the proposals outlined in DP72.

About AusCERT

AusCERT is the national CERT (computer emergency response team) for Australia and is an independent, non-government, not-for-profit organisation based at the University of Queensland that supports the Australian public interest by helping to protect the security of the Australian Internet using community, primarily by:

- Monitoring, analysing and providing advice about computer network threats and vulnerabilities;
- Providing assistance to Australian networks facing cyber attack sourced from within Australia, and more often, overseas;
- Providing advice on how to protect against and recover from computer security attacks and;
- Providing assistance to Australian law enforcement in cyber crime investigations.

In providing advice and recommendations in this submission, AusCERT does so from its experience and expertise as the national CERT (computer emergency response team) for Australia. As the national CERT, AusCERT is at the forefront of monitoring and analysing

[1] http://www.austlii.edu.au/au/other/alrc/publications/dp/72/

a wide range of computer network attacks, particularly, those able to be launched remotely via the Internet targeting Australian Internet users – organisations, business and individuals.

In particular, AusCERT has been at the forefront of monitoring, analysing and responding to online[2] identity theft attacks in Australia since March 2003. This response has included analysing the technical features of phishing and malware hosting sites and malware used for identity theft and financial fraud and seeking the closure of such sites in Australia and elsewhere.

As such, AusCERT has a unique view of how information systems – both within government, corporations, business and among home users have failed to keep personal identifying information (PII) private and confidential. Indeed, through its response and analysis role, AusCERT has become aware that not only has the privacy and confidentiality of PII been frequently compromised as a result of Internet based attacks, but also the integrity of such information is also at risk. The integrity of PII is also particularly critical when dealing with individual's personal health records. For example, unauthorised changes to health records may have fatal consequences in some circumstances.

e-Government, e-health and e-commerce

AusCERT assesses that existing provisions within the *Privacy Act 1988* are no longer synchronised with the threats that exist targeting PII and the new developments that have emerged in the way PII is collected, accessed or submitted online.

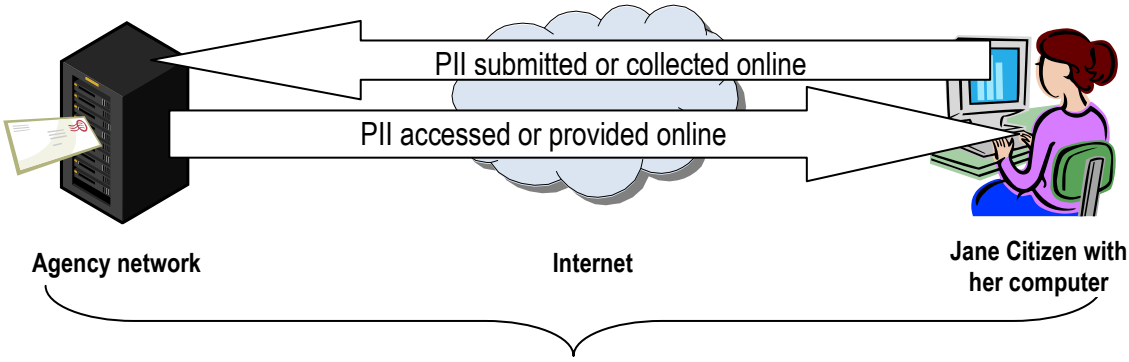
e-Government, e-health and e-commerce services involve the ability to transact or share PII (inter alia) between an organisation's network and other networks and computers over which that organisation has no control or ownership. For example, online transactions allow an individual to access or submit PII (their own or someone else's if they are authorised, eg a GP or pathologist may exchange PII about a patient) over the Internet from any computer in the world that is also connected to the Internet – be it a home computer, a work computer, a friend's computer, a cyber café, etc. In the case of e-government services the situation is assessed to pose a greater risk than e-commerce or e-banking services because some types of e-government transactions involve the aggregation of larger amounts of PII, which makes it easier for attackers to use that information for identity theft and other crimes facilitated by identity theft. Identity information stolen online can just as easily be used to support further identity crime in both the physical and online environments. For example, birth certificate application information stolen online would be of significant value to criminals if used to illegally obtain legitimate birth certificates.

---

[2] In this submission, online refers to any Internet communication (often but not always web based), which occurs between two external parties, ie the parties are not part of the same organisation or network. Examples of these types of communications include a tax agent's online submission of a tax return to the ATO; a member of the public's updating of PII on a web-based Centrelink form; a hospital sending an electronic medical health record of a patient to a GP; a pathologist sending the results of a patient's pathology tests to a GP; a person accessing their own electronic health record from a State government's health department network (such as Healthelink) or a customer accessing their financial account details from their bank online.

Although the media from time to time continues to report about large scale security breaches of PII held by organisations,[3] it is generally well understood and recognised that organisations which hold large volumes of PII need to protect the security of their own information systems and processes. It is this recognition which has lead to improved standards in specific industries such as the Payment Card Industry (PCI) Data Security Standard.[4]

What is less well understood and recognised, however, is that the nature of e-government, e-health and e-commerce frameworks means that the security of that PII is no longer reliant solely upon the security of organisations' information systems and databases and their own procedures for handling and dealing with this information. It is *also* increasingly reliant up the security of any remote computer or network that interacts with those organisational information systems over the Internet *when using e-government or e-commerce services*.



Providing confidentiality, integrity and authenticating identity for PII that is exchanged online depends on the security of the entire channel which includes Jane and her computer

Externally based attackers can potentially attack the 'channel' remotely at any point by targeting the agency network, targeting data in transit or by targeting Jane's computer. However, for the types of attacks that AusCERT refers to in this paper that target PII, attackers principally focus their attacks on the remote client computers, which are

[3] http://www.zdnet.com.au/news/security/soa/Credit-card-breach-exposes-40-million-accounts/0,130061744,139197997,00.htm

http://resources.zdnet.co.uk/articles/features/0,1000002000,39290745,00.htm

[4] https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf

computers like Jane's. Typically, they will use methods to trick Jane (social engineering) into disclosing PII or loading programs that will harvest PII from her computer.

Why securing the online channel is difficult

The inherently insecure design of mainstream operating systems (MSOS)[5] [6]is the fundamental reason why it is difficult to provide high levels of security on computers connected to the Internet and this situation is unlikely to change in the next few years at least even though some improvements in the security design of some MSOS such as Microsoft Vista have occurred.

The basic technology and techniques being used to conduct online ID theft through operating system compromise are not new. The design weaknesses in mainstream operating systems have been recognised for around three decades.[7] Consequently, MSOS security features and application layer add-on security counter-measures, such as firewalls, anti-virus software etc, can all be subverted. In this regard MSOS are considered to be untrusted.[8] The fundamental change in the last few years has been the rapidly increasing use of the Internet for value transactions and the ability of criminals to work out how to extract this value for illicit gain.

The delivery of e-government services relies on the connection of many untrusted remote systems to e-government systems. Caelli asserts that the interconnectivity and reliance on untrusted operating systems and allied software subsystems has virtually made it impossible for trust to be allocated to any transaction.[9] The point is no less applicable to e-government transactions for which assurances of data confidentiality, integrity, identity and authenticity, and in some cases non-repudiation, are required.

---

5 Reid, J (2005), "Prospects for Improved Operating System Security", *2005 Australian Computer Crime and Security Survey*, page 28, http:www.auscert.org.au/crimesurvey

6 Mainstream operating systems include those produced by Microsoft, Macintosh and various UNIX systems. Trusted Solaris and Security-Enhanced Linux are not mainstream operating systems.

7 Losocco, P.A., Smalley, S.D., Muckelbauer, P.A., Taylor, R.C., Turner, S.J, Farrell, J.F. (1998). The Inevitability of Failure: The Flawed Assumption of Security in Modern Computing Environments, National Security Agency, http://www.jya.com/paperF1.htm

8 Caelli, W and McCullagh, A (2000), "Non-Repudiation in the Digital Environment", http://www.firstmonday.org/issues/issue5_8/mccullagh/
Caelli describes a trusted computing system as one which "performs in accordance with its documented specification and will prevent any unauthorised activity. Specifically a trusted computing system can be relied upon to enforce a documented security policy".

9 Ibid.

Threat environment and online identity theft

In 2005, AusCERT identified emerging threats to e-government services.[10] Since then the situation has worsened and there have been many more cases of compromises of PII (Australian and other nationalities) both via e-commerce and e-government services.

A whole cybercrime industry has boomed over the last four years[11] [12] [13] [14] and criminal elements know and are actively exploiting the security weaknesses in these systems to access large volumes of PII for illicit financial gain, *inter alia*. An underground criminal economy actively trades PII and the means (services and knowledge) to obtain PII via online markets and information portals.

In the past four years, there has been a substantial increase in Internet attacks against Australian and other interests around the world[15] which are designed to fraudulently capture a range of PII for illicit financial gain and other forms of identity theft-related crimes.

Internet sites used to host these attacks include existing web sites or computers connected the Internet that have been compromised to host malware or re-direct to malware hosting sites, phishing sites or store fraudulently captured PII and account credentials.

The graph below shows the number of sites (by unique URL or domain name)[16] that have been used to facilitate malware and phishing attacks designed to capture PII or account access credentials targeting Australian Internet users.

---

[10] AusCERT (2005), Managing Risk Associated with Online Identity Theft for Government and Providers of e-Government Services, http://www.auscert.org.au/5777

[11] AusCERT, Australian Computer Crime and Security Surveys – 2003, 2004, 2005 and 2006, www.auscert.org.au/crimesurvey

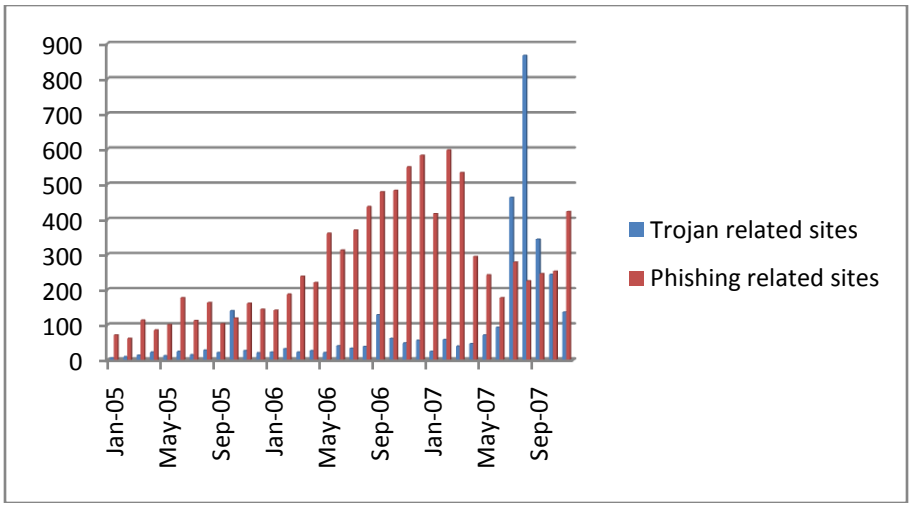
[12] iDefense, (2007) Global Threat Research Report: Russia, http://www.verisign.com/static/042139.pdf

[13] iDefense (2007), Uncovering Online Fraud Rings: The Russian Business Network, http://www.verisign.com/security-intelligence-service/current-intelligence/research-reports/index.html

[14] http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xi_03_2007.en-us.pdf

[15] Whittaker, C. (2006), APACS, Impact of malwae on UK Financial institutions, http://www.oecd.org/dataoecd/33/53/38652807.pdf

[16] Each incident in the graph represents a single unique URL or domain name that is hosted by one or more compromised computers for the purpose of stealing sensitive information and access credentials from other computers. Multiple incidents can be associated with each attack, which is the set of compromised computers needed to launch the attack and collect the stolen data. The number of IP addresses associated in a single incident and a single attack is variable but can range from 1 to around 100. This graph does not include the number of computer infections (compromised hosts) that occur due to each attack of which there is generally many hundreds or thousands.



Online ID theft incidents handled by AusCERT, January 2005 to November 2007

In a subset of attacks directed at Internet users that occurred in 2006, AusCERT identified around 35,000 compromised computers had data captured from them, including PII, including around 11,000 which were computers located in Australia.[17]

In another recent malware attack which targeted mostly German Internet users, AusCERT counted about 13,000 unique computer infections around the world, including 35 in Australia. In this case, as is typical of many cases, the trojan captured protected store data,[18] which includes all user names and passwords users automatically store on their computer which enables access to email and other web log-ins; and web form data, including form data sent over SSL encrypted sessions. Note that the attackers control access to the computer and all files on that computer so are in a position to search for additional PII to supplement the captured PII sent to the logging site (or email address). In at least one of the Australian cases from this attack, the captured data included the user's name, credit card details (including CVE number) and numerous login credentials.

The worsening threat environment is not surprising. MSOS are inherently insecure by design and application software, including browser software, continues to also exhibit a variety of vulnerabilities which can be exploited by attackers. Combined with an abundance of new opportunities to access PII *via the Internet* and with little chance of being identified or prosecuted attackers around the world[19] are capitalising on opportunities for illicit financial gain.

---

17 AusCERT (2006), Haxdoor – Anatomy of an ID theft attack using malware, https://www.auscert.org.au/7069 (available to ALRC on request).

18 http://www.us-cert.gov/reading_room/spywarehome_0905.pdf

19 Whittaker, C. (2007), APACS, Global e-crime threats – do we expect too much from law enforcement?, presented at GovCERT.nl

Despite advances in security, *no technology currently exists that can prevent the compromise of MSOS and the subsequent capture of data from these compromised computers.*[20]

As organisations have no control over the security of the remote computer systems being used to access or submit personal information (which generally they do not), then their ability to control and protect that PII is reduced.

If the security management of those remote computers is inadequate – and often the security on home and some small business computer systems are compared to larger government or corporate networks which have more security resources and skills available[21] – any PII which is accessed or submitted via that channel faces an increased risk of exposure – capture and potential modification by remotely located attackers,

Hence the situation now arises where a citizen using e-government services to apply for a copy of their birth certificate online (via the web) could have that data captured and used by a criminal for identity theft related crimes. So too could a health practitioner seeking to access and update a patient's electronic health record (via the web); or a person applying for a copy of their credit file via an online form which collects a detailed history of their PII.[22]

As noted in DP72, AusCERT agrees that privacy laws should be used to assist in preventing identity theft and minimising the harm caused by it after it has occurred.[23]

This is important as most of AusCERT's concerns with the existing privacy principles (IPPs and NPPs and proposed UPPs) centre around the increased threat of identity theft that now exists as the result of changes in the way governments and business are using and promoting *the Internet* to communicate with customers or clients to conduct aspects of their business, share and access or submit PII. These changes are as much to do with the

---

[20] There are effective mechanisms which can help prevent the modification of financial transaction data but these are currently not widely deployed and not particularly suitable for many e-government PII type transactions. They can protect the integrity but not the confidentiality of the transaction data if the remote client computer has been compromised. For further details of the EMV specification refer to AusCERT's submission for the Electronic Funds Code of Conduct Review, http://www.auscert.org.au/7536, page 7

[21] Please note this is only a generalisation based on assumptions made about comparative resources and skills necessary to implement more effective levels of security. The same vulnerabilities (human and technical) can exist on client hosts on government and corporate networks which make them vulnerable to trojan attack. Note that 20% of organisations surveyed in the *2006 Australian Computer Crime and Security Survey* reported one or more trojan infections on their network. See www.auscert.org.au/crimesurvey

[22] For example: https://services.au.vedaadvantage.com/dlw/servlet/DatalinkServlet2?nextService=/creditExpress/frm_creditExpress&contentService=/creditExpress/fileRequest/f_personalFileRequest&menuService=nav_general

[23] DP72, page 393

technologies and information systems that facilitate these communications[24] as they are with the information and communication frameworks themselves which enable e-government and e-commerce services.

Section 9.22 (DP72) states initiatives aimed at preventing identity theft generally aim to:

1. Educate individuals about how to minimise the risk of identity theft;

2. Enhance the security features of identification documents so that they cannot be altered or forged; and

3. Strengthen the procedures used to authenticate the identity of individuals engaging in transactions with agencies organisations.

Please note that while these initiatives may be effective to prevent off-line non-cyber identity theft, in cases of *online* theft of PII observed by AusCERT involving the use of malware or phishing attacks, the aforementioned measures have little or no effect to *prevent* the capture of PII *online* in the first place.

In the case of user education (first point), as noted in AusCERT's submission on the Electronic Code of Conduct review[25], the volume and sophistication of online malware and (deception-based) phishing attacks are such that it is difficult to reliably eliminate the risk solely from the account holder perspective. The type of malware which is currently in widespread use has functionality far more sophisticated and harmful than has been described in [the ASIC] discussion paper.[26]

In the case of better identity documentation (second point), while this is important to prevent identity theft in other situations, identity documents are not present during *online* transactions so being able to prevent their alteration or forgery will not address this problem.

In the case of stronger authentication and authentication procedures (third point), while this is important to help prevent many forms of identity theft, authentication as an access control mechanism to online systems cannot prevent the capture of PII accessed during an online session *if the remote client host is compromised with malware designed to capture such information – which is how many of these attacks occur*.

As noted in AusCERT's submission to the Electronic Code of Conduct review, single factor authentication credentials can be easily captured and re-used and in the vast majority

---

[24] Technologies such as the TCP/IP suite of protocols, the use of main stream operating systems and various software applications – all of which are prone to vulnerabilities which can be, and often are, exploited by attackers to facilitate various forms of online identity theft, *inter alia*.

[25] AusCERT (2007), Electronic Funds Transfer (EFT) Code of Conduct Review, http://www.auscert.org.au/7536, page 2

[26] http://www.asic.gov.au/asic/pdflib.nsf/LookupByFileName/eft_review_2007.pdf/$file/eft_review_2007.pdf, page 23

of deception-based phishing and malware attacks it is single factor authentication credentials which are fraudulently captured and re-used. [27]

Even some forms of two factor authentication will not prevent some phishing attacks designed to fooling users to disclosing access credentials or other forms of PII.

There have been cases in the past few years where attackers have defeated various forms of two factor authentication, including with the use of one-time passwords and challenge response mechanisms. In these cases, the malware simply waits for the legitimate owner of those credentials to log on and then, captures and can potentially initiate transactions on behalf of the legitimate owner during the session in the background. It can also mean that an attacker can make changes in the background which appear to have been made by the legitimate user.

Similarly, where software based digital certificates[28] have been used and are stored on the certificate owner's computer, malware is now in use which captures these certificates. Hence any PII exchanged with the user of the compromised computer and the e-government, e-health or e-commerce system can be captured in its decrypted form. Similarly, the security goal of non-repudiation cannot be achieved for a digital signature generated by a user from the user's private key stored on a computer that has been compromised. The question must be asked whether any digital signature can be trusted if the private key is stored on the computer itself (as opposed to separately in hardware, eg on a smart card) because it will not be possible to know if the computer has been compromised and the signature can or cannot be trusted.

In terms of the privacy laws and privacy principles, therefore, it must be recognised that an organisation's privacy responsibilities are no longer a matter of simply protecting the privacy of PII it holds and handles. Rather the process of exchanging (collecting and providing access to) PII *online* with a range of other external partners or parties and being a conduit for *online* PII-laden services, means that the scope of an organisation's privacy obligations must change.

Preventing identity theft

When dealing with access to PII online, AusCERT recommends the main options for helping to prevent identity theft need to centre upon:

[27] AusCERT 2007, AusCERT Submission to Electronic Funds Code of Conduct Review http://www.auscert.org.au/7536, page 7

[28] Here digital certificates refer to the set of files associated with a person's public and private key pair, and associated passphrase, which allows a person to decrypt encrypted communications sent to them and/or digitally sign messages from them.

1. Where possible, encourage the use of secure and trustworthy computers[29] when accessing e-government or e-health services from locations remote to the organisation or agency network; and/or
2. The ability of organisations to deny access to their e-government or e-commerce channels to users whose computers do not meet minimum security standards;[30]
3. Limiting the aggregation of PII that is collected or made available to a person or organisation online during any single session to what is essential, as opposed to desirable;
4. Where appropriate (such as electronic health records) use unique identifiers instead of personal identifying information (such as name, telephone number, address and date of birth) that help anonymise the key identifying particulars of an individual but still allows personal information about an individual to be exchanged in a meaningful way to both parties. This does not mean that the individual's identity will be anonymous to the organisation/agency. The idea is that in the event that the communication exchange is captured by a third party, it will be more difficult for the attacker to readily identify the individual concerned and hence the personal information will have less value.

Detecting and responding to identity theft

Section 9.23 (DP72) states initiatives aimed at minimising the harm of identity theft tend to focus on assisting victims of identity theft to remedy the adverse effects of the theft.

However, there is an important preliminary step which has been overlooked. It is not possible to do even this until the theft of identity information has been *detected*. The insidious and often hidden nature of this crime makes it difficult for both victims and organisations with privacy obligations to know that an attack has occurred and that PII has indeed been captured by criminals. Therefore, with many forms of identity theft, it is not until a subsequent fraud (or other crime) has occurred and been detected that the original identity theft crime is realised and even then it may not be evident how the PII was captured.

---

[29] Here 'trustworthy' is not necessarily being used in its traditional sense which refers to a specific stringent set of hardware and software design criteria, even though this is highly desirable. Rather it is suggested using a more pragmatic approach of using a mainstream operating systems that is fully maintained in terms of its software patches, which limits only a known set of out and inbound connections to facilitate (a) managing the security of the computer system itself and (b) to enable the particular e-government or e-health transactions it is being used for to occur. The computer would need to be in a relatively secure physical location, with no possibility of installing or running software or hardware devices except by the security administrator and hence is not suitable for all situations.

[30] How an organisation assesses whether a remote partner meets a certain standard could be the subject of OPC guidelines in consultation with various experts but it at its most basic could include ensuring the computer's operating system, if Microsoft, is at least running Windows XP SP2 as this provides a level of security that is superior than earlier versions such as Windows 98 or Windows NT.

If organisations with privacy obligations are more proactive and attempt to detect when such crimes occur, then more can be done to detect this type of crime earlier and once detected, help victims mitigate the potential impacts.

AusCERT has identified some, albeit limited, ways to help detect when these types of crimes occur for e-government providers[31] but recognises that the suggestions will not be practical in all situations. Please note that e-banking providers have other more reliable options available to them to help detect when PII may be compromised, in near real time. Even when detection measures are put in place, they will not always reliably detect the presence of a system compromise.

4. Achieving National Consistency

Proposal 4-1 The *Privacy Act* should be amended to provide that the Act is intended to apply to the exclusion of state and territory laws dealing specifically with the handling of personal information by organisations.

AusCERT comment

Any proposed changes to the *Privacy Act* should ensure that the scope of a party's responsibilities under the *Act* are extended to include not only how that party (agency or organisation) handles personal information *in its possession* but how it is collected or made accessible through online or electronic means. In other words, agencies and organisations should be mindful of their privacy obligations for the entire online channel which is established to collect or provide access to PII, over the Internet. The entire channel includes the security of both computers involved in the communication – not just the security of the transport of the communication between the computers.

This is an important distinction because the scope of the *Privacy Act* and its principles (NPPs, IPPs and proposed UPPs) currently focus on how organisations handle PII *in their possession*.

Many organisations engage in practices which increase the risk of exposure of PII when collected *via online mechanisms. S*imilarly, *by giving access to individual's PII via online mechanisms, individuals' PII faces an increase risk of exposure once it reaches the remote computer system,* ie after it is no longer in the possession of the organisation.

Current provisions of the *Privacy Act* appear to be deficient in that organisations do not have to address or even consider these risks, or organisation's potential role in contributing

[31] AusCERT, 2005, Managing risk associated with online ID theft for government and providers of e-government services, page 16, www.auscert.org.au/egov

to these risks even though many organisations are conduits to facilitate the collection of PII or accessing or PII *online*.

Part B – Developing Technology

Proposal 7–1 The *Privacy Act* should be technologically neutral.

AusCERT comment

AusCERT agrees that the *Privacy Act* should be technologically neutral but significant changes have occurred in the way PII is accessed, collected and made available online and in electronic form in the last 20 years. These changes are less to do with the particular technologies or information systems being used and more to do with PII sharing frameworks being used to deliver e-government, e-commerce and e-banking services.

As such, organisations' responsibilities under the *Act*, in particular the privacy principles, need to also address how organisations manage privacy and data security of PII when the organisation is acting as a conduit for PII, ie not limit their responsibilities to PII they actually hold.

Proposal 7–2 The *Privacy Act* should be amended to empower the Minister responsible for the *Privacy Act*, in consultation with the Office of the Privacy Commissioner, to determine which privacy and security standards for relevant technologies should be mandated by legislative instrument.

Proposal 7–3 In exercising its research and monitoring functions, the Office of the Privacy Commissioner should consider technologies that can be deployed in a privacy enhancing way by individuals, agencies and organisations.

Proposal 7–4 The Office of the Privacy Commissioner should educate individuals, agencies and organisations about specific privacy enhancing technologies and the privacy enhancing ways in which technologies can be deployed.

AusCERT comment

Because knowledge of security technologies, their strengths, weaknesses and how various technologies or information systems' security can be defeated or bypassed is a specialist area, AusCERT recommends that the Minister and OPC consult a committee of experts before determining which privacy and security standards for relevant technologies should be mandated by legislation (Proposal 7-2).

It is AusCERT's experience that often incorrect assumptions are made about the relative strength or security of various systems and technologies when in fact these systems and technologies are not able to withstand known attack methods that are in common use for systems connected to the Internet.

For example, understanding the relative strengths of a particular cryptographic algorithm or key length being used for confidentiality or non-repudiation purposes is important when applied in certain contexts but may not be worthwhile if the computer systems using these cryptographic security mechanisms are insecure and can be easily compromised. This would in effect allow an attacker to have the same privileges of the system owner – including reading all communications whether the security provided by this cryptographic technology was in use or not.

For the reasons stated, AusCERT recommends that before providing such advice (Proposal 7-3 and 7-4), the OPC ensures that it has consulted with a wide range of experts as there is often a discrepancy between the perceived security of certain privacy enhancing technologies and their actual security (and privacy).

As information systems and security technologies change as rapidly as the threat environment changes, it is also recommended that the consultative expert review process occur at least on an annual basis to ensure that the advice being provided remains as up to date as possible.

8. Individuals, the Internet and Generally Available Publications

Question 8–1 Should the online content regulation scheme set out in the *Broadcasting Services Act 1992* (Cth), and in particular the ability to issue take down notices, be expanded beyond the *National Classification Code* and decisions of the Classification Board to cover a wider range of content that may constitute an invasion of an individual's privacy? If so, what criteria should be used to determine when a take down notice should be issued? What is the appropriate body to deal with a complaint and issue the take down notice?

AusCERT comment

As noted in previous paragraphs discussing the threat environment and its impact on online identity theft, it is difficult to achieve high levels of security on many remote client systems – thus efforts to prevent online identity theft fail. When prevention fails, it is imperative that improved arrangements exist for detecting breaches and responding to breaches so the impact of the theft is minimised.

As noted in AusCERT's submission to auDA,[32] AusCERT is actively involved in seeking the take down of a variety of sites hosted in Australia and around the world that are used to facilitate (directly or indirectly) the theft of PII against Australian Internet users, analyse

[32] AusCERT, 2007, Review of .au domain name policy submission, www.auscert.org.au/8396

the malware in use and, where Australia PII is at risk retrieve and redistribute log files of captured PII to trusted parties to help mitigate the impact of the attack.

Depending on the circumstances, AusCERT directs requests for assistance to take down these sites to either:

a) An ISP who operates the network where the computer is hosted if only an IP address is known;

b) Various abuse contacts and whois records where it appears that a legitimate domain has been compromised and is hosting content that facilitates ID theft; and/or

c) A domain name registrar where it appears that a domain has been specially registered to host the attack or aspects of the attack and each domain is being rotated to resolve to many IP addresses (botnet-hosted).[33]

As the national CERT, AusCERT has been actively performing this role in Australia for these types of attacks since early 2003 and often relies on the good will of various parties to assist. Sometimes parties will comply with the request because the site is in breach of specific laws (eg copyright infringement for phishing sites); or the content is against the Acceptable Use Policies of the ISP; or the attacker used stolen credit card details to register the domain and the registrar is likely to incur a financial loss; or in some cases on the basis of trust in AusCERT's own analysis, when the person/organisation complying with the request does not have the expertise to identify the presence of malware on the site themselves.

On many occasions, including the latter, when the ISP, domain name registrar or legitimate site owner has no expertise to safely read and interpret the web site's code to recognise that connections made to the site may result in the download of malware, then action may not be taken at all, or result in unnecessary delays in taking the site down. In these situations, having specific legislation and criteria which makes it an offence to host these types of sites will assist mitigate the impact of theft of PII.

What criteria should be used to determine when a take-down notice should be issued?

To help mitigate the impact of compromised PII affecting Australians that has been acquired illegally and given the difficulties that AusCERT and others continue to face in Australia (and elsewhere) seeking the timely closure of such sites in order to mitigate further harm to potential victims, AusCERT supports an extension of the 'take down' provisions in the *Broadcasting Services Act 1992* (Cth).

AusCERT recommends the criteria to be used to take-down include :

[33] In this situation, because of the huge number of changing IP addresses (ie separately compromised computers being used to participate in the attack) involved, it is not feasible or practical to contact each and every ISP about each IP address as the domain will simply be moved, generally within a short period of time, to a new IP address. Without suspending the domain name, the effect is that the phishing or malware site is able to remain accessible over the Internet.

- For ISPs: disconnect any computer in Australia connected to the Internet which poses an actual or reasonable risk of compromising PII; and/or
- For abuse contacts: Remove any affected pages or directories from any computer in Australia connected to the Internet which poses an actual or reasonable risk of compromising PII; and/or
- For domain name registrars: Suspend the domain name registration for any computer in the world with a domain registered in Australia which poses an actual or reasonable risk of compromising PII (regardless of the number of IP addresses that resolve to the domain or where those IP addresses are located).

An actual risk would include any logging site which contains the captured PII data, inter alia, from phishing and malware sites.

A reasonable risk would include phishing sites, malware sites and sites which redirect computers to either phishing or malware site for the purposes of fraudulently capturing PII, inter alia. Please note the redirect site may involve multiple redirect paths before a connection is made to the primary phishing or malware site necessary to launch the attack. Similarly, one or more malware download sites may exist within a given attack as a sequentially-staged compromise process. These techniques are used by attackers to make it more difficult to identify and hence take action against the primary sites that will facilitate the attack.

Reciprocity

In order to set best practice standards and eventually achieve reciprocity of arrangements in other countries, the take-down provisions should also apply to sites hosted in Australia but which contain PII belonging to persons who may not be Australians or are not based in Australia. Many attacks hosted in Australia target non-Australians just as most attacks of this type which target Australian Internet users are hosted overseas in other legal jurisdictions.

Preservation and responsible distribution of compromised PII

To most effectively mitigate online attacks designed to capture PII, it is not sufficient to simply issue take-down requests. Certainly this may stop an attack in progress but it does not prevent mitigation for PII already captured and does not help AusCERT, other information security experts or the government understand the technical nature of the attack and develop approaches to defeating these types of attacks in future. Therefore, take-down provisions should be accompanied by preservation of data requests – at the very least this should seek to pass copies of the captured PII to appropriate trusted parties to redistribute to help affected networks and individuals mitigate the attack.

Retrieving and responsibly redistributing log files of data captured PII to trusted third parties from phishing and malware attacks may help mitigate the impact of the stolen PII. These log files can range in size from a few MB to many GB and contain a range of PII, including various account access credentials, passwords and other captured data about

users' online activities. Sometimes it is possible to easily identify persons; at other times they may include logon access credentials.

Log files of system connections and other files stored by the attacker in the site's directories may provide forensic evidence useful to law enforcement or affected corporate or government entities that could help identify the attacker and/or the attacker's modus operandi. In some cases captured banking access credentials have been used fraudulently used within hours of the initial capture occurring – hence the timely retrieval of this information is essential for effective mitigation.

Malware artefacts are important to help identify all phases of the attack in order to seek additional site take down requests – which may not be readily apparent through other means. Malware artefacts are also important to understand the technical aspects of the attack – understand the full extent of functions the malware performs – from how it disables or circumvents security features, what type of data it is seeking to capture (eg, PII, digital certificates, access credentials, form data, protected store, etc) and where it reports to (attacker controlled web or email address). Obtaining a copy of all malware associated with a single attack is also vital to check its level of detectability using anti-virus products and where known to only have low levels of detectability among vendors, ensure it is distributed to as many anti-virus vendors as possible so they may develop signatures for the malware.[34]

Who should the provisions apply to?

If such take down provisions are to apply they must apply to any stakeholder in a position to most reasonably take action. This includes ISPs, domain name registrars or the abuse contacts listed on the web site. Suspending a domain name that has been registered solely to help facilitate a malware or phishing attack is the only effective method of mitigating the attack when the attacker is hosting elements of the attack via a botnet (ie resolving the domain name to multiple IP addresses for short time intervals each).

What is the appropriate body to deal with a complaint and issue the take down notice?

A range of parties are currently involved in take down requests for these types of Internet attacks – national CERTs, financial institutions whose customers are being potentially impacted, outsourced security organisations responding on behalf of financial institutions, and sometimes law enforcement – the latter, generally used only when other attempts via other means have failed. As noted in AusCERT's submission to auDA, law enforcement are often not skilled or resourced to identify if a site is hosting malware that facilitates ID theft, or is being used to redirect users to sites that are hosting malware or are in any other way part of a broader attack that is designed to compromise users' computers and download malware that will facilitate the theft of various types of PII. Therefore, it is not

[34] In its role as the national CERT, AusCERT analyses and seeks to mitigate the impact of malware designed to capture PII in the manner described in this paragraph.

appropriate in terms of skill or resources to rely upon them to issue take-down requests in a timely manner.

AusCERT supports a distributed approach to issuing take down requests. If the requesting party is a trusted and expert party or organisation – such as the main groups described above – then Australian based stakeholders should be obliged to respond to their take-down requests directly under the Act.

Part of the reluctance on the behalf of some ISPs and domain name registrars to take timely action is that by responding to the request, they perceive they may face legal liability by the computer owner or the domain name registrant. Therefore, if the take-down notice process is be fully effective, then the Act should confer "good Samaritan" protection to ISPs and domain name registrars and those who issue the take-down requests who act in good faith based on their expertise.

ACMA could also have a role under the Act to investigate and deal with cases of stakeholder non-compliance to take-down requests. [35] Similarly to ensure an accountable and transparent process, ACMA could investigate allegations by stakeholders (ISPs or domain name registrars) of improper use of the take-down provisions by the group of trusted parties which may not comply with the stated criteria.

In order for the legislation to be effective, it is not enough to simply specify the criteria when the stakeholder (ISP, domain name registrar or legitimate web site owner) should respond but also the legislation must identify a generic group of trusted parties whose advice these stakeholders should be obliged to accept even if they themselves are unable to verify the claims.

For example, if AusCERT identifies a computer hosted from a domain name registered in Australia serving malware capable of stealing PII and makes a request for domain suspension to the registrar, the request will not mitigate the impact of the attack if the registrar is unable to verify[36] this claim independently and hence refuses to comply with the request.[37] The registrar must know which trusted parties it is obliged to respond to 'take-down' requests from. Obviously, from AusCERT's perspective AusCERT as the national CERT would be one such party given AusCERT's role to mitigate Internet based attacks, expertise and extensive experience in this area.

---

[35] Many trojan attacks capture a whole range of data, which may include data that is not PII. Typically this type of malware captures form data, protected stores (passwords stored), sometimes digital certificates, user input via keyboard or mouse, computer output via screen or printer.

[36] The nature of these attacks is such that much of the malware being used is undetectable by many anti-virus software products at the time it is released.

[37] Some registrars have expressed concern about being held liable if AusCERT mistakenly issues a request for a legitimate site that is not hosting malware.

The generic group of trusted parties who are authorised under the Act to issue take-down requests – in accordance with the aforementioned criteria – to Australian stakeholders could be the subject of periodic review and consensus by the group of security experts reviewing the efficacy of various security technologies and systems.

UPP 8. Data Security

An agency or organisation must take reasonable steps to:

(a) protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure;

(b) destroy or render non-identifiable personal information if it is no longer needed for any purpose permitted by the UPPs; and

(c) ensure that personal information it discloses to a person pursuant to a contract, or otherwise in connection with the provision of a service to the agency or organisation, is protected from being used or disclosed by that person otherwise than in accordance with the UPPs.[38]

AusCERT comment

AusCERT considers the existing wording of UPP8 not sufficient to meet the demands of the current threat environment nor the way PII is exchanged online over the Internet while providing e-government, e-commerce and e-banking services. AusCERT recommends UPP8 (a) be amended to read (new paragraphs in bold):

> An agency or organisation must take reasonable steps to:
>
> (a) protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure;
>
> (b) **minimise how much PII can be collected or accessed over the Internet from third party computers (third party computers are those which do not belong nor are managed by the agency or organisation directly or indirectly);**
>
> **(c) implement strategies commensurate with the risk to help prevent, detect and mitigate harm arising from the compromise of PII collected or accessed via third party computers. In doing so, assume that third party computers may be compromised;**
>
> (d) **advise parties who submit or access PII online of the risks and limitations of technology to protect this data from potential capture and misuse.**
>
> (e) destroy or render non-identifiable personal information if it is no longer needed for any purpose permitted by the UPPs; and
>
> (f) ensure that personal information it discloses to a person pursuant to a contract, or otherwise in connection with the provision of a service to the agency or organisation, is protected from being used or disclosed by that person otherwise than in accordance with the UPPs.[39]

[38] DP72, page 753
[39] DP72, page 753

Understandably, in some situations it is difficult to implement security controls when communication occurs with computers the agency/organisation has no control or authority over. In this regard, what is reasonable in one situation may not be reasonable or possible in another. The key is to be mindful of the threat environment, the vulnerabilities within the channel and the real risks that exist to PII when e-government and e-commerce services are being used and to encourage organisations to be more proactive than some perhaps are.

Indeed, if organisations/agencies assume that these computers may already be compromised, or are vulnerable to compromise – which many are – then their approaches to how they collect and/or provide access to PII online and the data security arrangements may be improved.

Note, for the purposes of satisfying (d) above, it would not be considered sufficient to advise or imply that the use of encryption through the use of SSL/TLS addresses these online risks. The vulnerabilities and the threats described are in no way mitigated by the use of SSL in the current threat environment, even though the use of this technology remains important to mitigate other potential threats.

It is noted that advising users of risks associated with online services has been a recommendation of the OPC in the past. However, given its importance, AusCERT considers it should be part of the UPPs.