Cyber White Paper Submission

Foreword

The Centre for Internet Safety at the University of Canberra appreciates the opportunity to make this submission to the Cyber White Paper process.

We would be very happy to provide further information and details on issues contained within this document.

Alastair MacGibbon
Director

Nigel Phair
Director
About the Authors

Alastair MacGibbon is an internationally-respected authority on cybercrime, including Internet fraud, consumer victimisation and a range of Internet security and safety issues. For almost 5 years Alastair headed Trust & Safety at eBay Australia and later eBay Asia Pacific. He was a Federal Agent with the Australian Federal Police for 15 years, his final assignment as the founding Director of the Australian High Tech CrimeCentre.

Nigel Phair is an influential analyst on the intersection of technology, crime and society. He has published two acclaimed books on the international impact of cybercrime, is a regular media commentator and provides executive advice on cyber security issues. In a 21 year career with the Australian Federal Police he achieved the rank of Detective Superintendent and headed up investigations at the Australian High Tech Crime Centre for four years.

About the Centre for Internet Safety

The Centre for Internet Safety at the University of Canberra was created to foster a safer, more trusted Internet by providing thought leadership and policy advice on the social, legal, political and economic impacts of cybercrime and threats to cyber security.

The Centre for Internet Safety is hosted within the Faculty of Law at the University of Canberra. The University of Canberra is Australia’s capital university and focuses on preparing students for a successful and rewarding career.

www.canberra.edu.au/cis
Consolidated Recommendations

1. When engaging the online community on these matters government and businesses need to talk about consequences and effects of behaviours rather than safety and risk.

2. Engagement, particularly of young people, needs to start at an early age and be repeated many times. Preferably this should be built into curriculum, combined with additional visits by experts to reinforce messages over the school life of a young person.

3. Relevant Commonwealth departments collaborate with universities to undertake robust studies into perceptions of Internet anonymity and aggression and honesty as well as what cues may deter that anti-social behaviour.

4. The ACMA and OFLC consider user-generated classification systems where the user ratings would determine classification, similar to eCommerce companies like eBay, or venue review sites like Yelp. Even an entity like Common Sense Media [www.commonsense.org](http://www.commonsense.org) where parents can subscribe to privately-curated lists from like-minded people.

5. As part of schools outreach programs conducted by ACMA, parent/guardian/carer information on effective use of technology be strengthened in the materials.

6. A more robust stance from the Australian Government towards online content providers in relation to demanding acceptable behaviours and reduced criminality on their networks.

7. Public sector agencies contact the Centre for Internet Safety to actively involve themselves in the Growing the Digital Economy Safety Working Group so that they may engage with their private sector counterparts.

8. The Australian Government explore online credentials in light of the US Government’s NSTIC.


10. The Commonwealth Government continues engaging ISPs in relation to strengthening and expanding the existing iCode.

11. A cybercrime reporting capability take a broad definition of cybercrime to include all aspects of the misuse of online technology, including Internet frauds and scams.

12. Existing Internet safety, security and scam public-private education efforts be amalgamated under one organisation for the purposes of efficiency and effectiveness.

13. State, territory and Federal police consider operating procedures, training and structural reform in light of the Australia community’s wholesale adoption of Internet and mobile devices so that they can better respond to cybercrime complaints.

14. Victims of crime should be treated in a “channel of victimisation” agnostic way: all victims of a similar offence receive similar, respectful, manner.

15. A modest clearinghouse be established to ensure online crime complaints are directed efficiently to appropriate agencies.

16. Offline product liability regimes be applied to online services and software.

17. Governments should consider mandating standards like ISO 27001 if industry does not improve.

18. The iCode should be expanded and strengthened to increase the protective and intervention role for ISPs.

19. Government should ensure there are adequate “safe harbour” legal provisions in place to protect ISPs, financial institutions and other businesses to take action, sometimes against the instructions of their customers in order to protect the customer or other customers.

20. The iCode should be tightened to give ISPs less latitude in the actions they take when an infected device is detected.
21. Australian police should seek to engage major tech companies who invest in overall Internet health and seek genuine investigative partnerships.

22. Commonwealth policy departments adopt a “network” interconnected approach to understanding and assessing cybercrime.

23. Efforts to improve cyber safety and cyber security for the benefit of the broader community be carried out in a manner that preserves as far as possible the freedoms and values we expect offline in Australia.

24. The Government exercise its sovereignty over Australian networks in a manner that protects and preserves society just as the government aims to do in offline situations, reducing its “light touch” approach.

25. In relation to offshore crime and broader Internet governance, the Australian government must rely upon bilateral, multilateral and international agreements.

26. The Australian Government engage with multinational corporations offering services to Australians to outline government expectations.

27. In relation to offshore crime and broader Internet governance, the Australian government must rely upon bilateral, multilateral and international agreements.

28. The Australian government should consistently and significantly play a part in Internet governance bodies such as ICANN and the Internet Governance Forum.

29. The Australian Government enhance existing Aid programs to include aspects of cyber security for developing nations to increase governance and productivity.

30. The Government take the view that acceptable behaviour online should be no different to acceptable behaviour offline.

31. Government should avoid legislation specifically centered on technology, instead applying offline laws and regulations online.

32. Government should consider programs to encourage Australian nationals to undertake IT security studies with a “return of service obligation” within national security, policing and defence agencies.

33. Government backing for formation of centres of excellence around key IT security and investigative capabilities should also be considered.

Structure of this Document

We address several of the specific questions raised in the discussion paper. The format of this document is that we will list the question or questions, and our response appears below. Since some of the questions are similar, there is some repetition in this document.
Question: How can we promote a concept of digital citizenship, reach agreement on acceptable online behaviour and encourage people to assume greater responsibility for that behaviour?

The Internet traverses political, cultural and geographic boundaries within and between countries. It brings people and their views and behaviours closer together - and allows them to interact - in a speed and manner never seen before. The Internet exposes us to views and behaviours that reinforce and challenge our beliefs, threatens us, help us.

The globalised nature of the Internet was enhanced in October 2009 with a decision by the Internet Corporation for Assigned Names and Numbers (ICANN) to introduce the first non-latin character top level domains, which will increasingly see people from around the world able to use their own script to enter unique URLs: an Internet no longer dominated by English speakers, or even people with languages that use Latin charters.

The Internet has opened international trade to consumers with person-to-person online financial transactions, eCommerce and classified ad platforms. It has reunited old friends - and helped us find new ones - via social networks, dating websites and computer-to-computer telephony and messaging. It has helped enable individuals to become publishers, commentators and journalists via blogs, video sites and social networks.

And it has brought offenders closer to victims all around the world.

As society struggles to rationalise the size and scope of online sexual predation, child exploitation, hate, bullying, scams and hacking, one of the dominant views is the Internet is somehow different from “real” society: it is “virtual”. But nothing could be further from the truth. The Internet is - whether we like it or not - a (albeit imperfect) reflection of society and what we see happening on the Internet should force us to pause for thought.

What is different is the scale of the anti-social and criminal behaviour, which is amplified because offenders can use tools and services that increase the cadence and reach of their activities.

Encouraging pro-social behaviour (our Australian version of it at least) amongst those users of the Internet inside Australia and interacting with Australians requires multiple inputs:

- This is not solely a technical problem, and cannot be fixed by software and hardware alone.
- Solutions for creating pro-social and discouraging anti-social behaviour must come from the many mechanisms societies deploy today for other offline issues.
- Internet users need to understand they are not anonymous online: we may not necessarily be identified by name and we may not be physically seen while acting, but we are not anonymous (most of the time).
- When engaging the online community on these matters we need to talk about consequences and effects of behaviours rather than safety and risk.
- Engagement, particularly of young people, needs to start at an early age and be repeated many times. Preferably this should be built into curriculum, with messaging for each stage of maturity and online involvement and if additional visits by experts are undertaken (such as the Australian Communications and Media Authority (ACMA) Internet Safety Awareness program) they need to be repeated rather than a one-off lecture.
We recommend:

1. When engaging the online community on these matters government and businesses need to talk about consequences and effects of behaviours rather than safety and risk.

2. Engagement, particularly of young people, needs to start at an early age and be repeated many times. Preferably this should be built into curriculum, combined with additional visits by experts to reinforce messages over the school life of a young person.
**Issue:** The online environment can create a sense of dislocation from our actions; the ability to act anonymously online can embolden bullies and sometimes abusive, offensive or illegal behaviour can go unchecked.

**Question:** How can governments, the private sector, the NFP sector and the broader Australian community work together to promote responsible and accountable digital citizenship and reduce harassing and malicious online behaviour?

There is a misconception that we are totally anonymous while using Internet and mobile devices. We mistake the solitary situation we may find ourselves in with technology and equate that to anonymity. While we may not be aware of it, every action taken online, every key-stroke, can shed digital evidence, and major online corporations (many of them providing a “free” service) are making billions of dollars per year analysing our actions, data mining, selling advertising to us based on our actions. In fact, we are in many respects more anonymous walking down the street or standing in a crowd. There are many reasons why Internet users should use their real identity whilst online, however whilst always acting legally, sometimes we may want our web surfing to be unattributed and allowance needs to be made for this.

The assumption of anonymity has emboldened outright crime from some who might otherwise not been criminals, and girded others into anti-social behaviour. In the 1970s there were experiments conducted by psychologists such as Zimbardo into anonymity and aggression and by Diener, Fraser, Beaman and Kelem into anonymity and honesty. The role of the Internet's perceived anonymity on behaviour is worthy of significant further study.

**We recommend:**

3. Relevant Commonwealth departments collaborate with universities to undertake robust studies into perceptions of Internet anonymity and aggression and honesty as well as what cues may deter that anti-social behaviour.
Issue: Children and young adults are prolific users of social networking sites and as a result can be exposed to a range of online risks, including abusive behaviour.

Question: How can we help carers and parents to appropriately supervise young people and minimise these online risks?

Question: How can we promote social responsibility and encourage young people to protect themselves and each other by speaking out against cyberbullying?

Computers, gaming consoles and mobile telephones are not the “baby-sitting” devices that televisions, VCRs and landline telephones were for the previous generation. Being Internet connected devices they are by their nature interactive, and can expose young people to unwanted and dangerous people, communications, content and products.

Parents and guardians can’t dispose of their requirement to teach children to act respectably, ethically and lawfully, by assuming such activity is the role of a school. Parents and guardians also can’t use the excuse they don’t understand technology as a reason for not guiding their children to act properly online.

The use of these devices requires the following:

- Active supervision and participation of the parent/guardian/carer
- Discussion and understanding around consequences of behaviour
- An “open door” relationship allowing the child to talk about issues that concern them, and to seek advice
- Consideration to purchase, install or turn on - but not overly rely upon - “Net Nanny” type software

The nature of content creation (publishing/broadcasting) and consumption (viewing/reading) has changed dramatically, and it is important that the Government, through the auspices of the responsible entities, the ACMA (for Internet content) and the Office of Film and Literature Classification (OFLC), seriously consider the long term viability of the classification rating system. As more content can be directly accessed from overseas that is rated (or not) under different systems, the efficacy of the Australian regime will rapidly diminish.

We recommend:

4. The ACMA and OFLC consider user-generated classification systems where the user ratings would determine classification, similar to eCommerce companies like eBay, or venue review sites like Yelp. Even an entity like Common Sense Media [www.commonsense.org](http://www.commonsense.org) where parents can subscribe to privately-curated lists from like-minded people.

5. As part of schools outreach programs conducted by ACMA, parent/guardian/carer information on effective use of technology be strengthened in the materials.
**Issue:** Social networking sites are almost entirely facilitated by the private sector. Although many of the larger sites have some capacity to monitor and limit abusive behaviour, some others do not.

**Question:** How can the owners of social networking sites be more engaged in meeting community expectations that their platforms will not be used for abusive or illegal activities?

Operators of websites and Internet services need to tread a line between legitimate protection of the creativity, free expression and privacy of people using their services, and deterring those who abuse the service. Like other social activities most people on the Internet will do the right thing most of the time, but a few people doing the wrong thing can cause significant harm to many, quickly.

It is in the interest of many of the operators of social networks to develop (and continue to evolve and harden) acceptable use policies and other rules, as well as to build out rule enforcement capabilities. This is especially so for social networks that are profitable.

Rather than being a generic “global village” as the Internet is often referred to, users of social networks tend to gravitate to places where they feel most comfortable, where their friends are and where the behaviour most closely matches their expectations. And it is in the interests of the social network operator to try to maintain that balance. There is a saying in Internet businesses that you are “only one click away from your competition”. When users no longer see a site as relevant they leave. MySpace’s rapid demise illustrates this.

It is logical - even if frustrating to regulators - that such rules and capabilities will often develop after a service has reached a certain level of activity, and only after significant antisocial behaviour has occurred that the company now perceives to either damage the profitability of the company, and/or, possibly exposes the company to regulatory intervention or litigation. Added to this problem is many overseas based services don’t have Australian (or even Asia-Pacific) contact points for trust and safety issues. From our long term interaction with these companies, the timelines for product changes to fix problems and appease governments can be many months due to the complexity of code and the availability of developer resources. And that is assuming there has been buy-in at a high level at headquarters: a difficult task even if there is intense government attention in a country outside headquarters.

Facebook provides a good example of this asynchronous capacity development.

Most multinationals, even if they believe domestic laws do not apply to them, will subject themselves to domestic laws as a sign of good faith, especially those with satellite offices located inside Australia. However, many will suffer “conflict of laws”, where due to their global footprints, laws of many states will pull them in different directions. [see breakout box]
Australian regulators need to remember that although in Internet terms Australia is only a small player due to population size, it is a profitable market for its size, so most multinationals will do the right thing where possible, and will certainly change behaviour if legislation requires it, even if legislation is only actively considered. Websites can tailor experiences (roughly) to geographic blocs, and they can have country-specific user agreements. This is just a cost of doing business that they will try to avoid, but they will not forgo the (possibly slightly diminished) profits associated with mandated change.

We recommend:

6. A more robust stance from the Australian Government towards online content providers in relation to demanding acceptable behaviours and reduced criminality on their networks.

Hypothetical

A US-based social network which stores data in that country, but has a sales and marketing office in Australia, has a French national as a customer who is believed to have broken Australian law.

An Australian Federal Police officer needs the account information and messages sent and received by the French national.

She obtains a search warrant and executes it on the Melbourne office of the social network. No data is stored in Australia, but office staff can access the data via their work computers. The police officer knows that the search warrant gives her authority to compel that data to be brought electronically to Australia. She exercises that authority.

The data, stored in the United States, is protected under US law. It does not allow the removal of data via any other nation’s compulsive powers. To do so could see the company breach criminal and civil laws there. The company will, however, accept the authority of US law enforcement and their search warrants.

The company representatives in Melbourne comply with the Australian search warrant, as they risk criminal charges if they don’t.

The data pertaining to the French national is protected under European Union and French law. The US-based company should not have had the French citizen’s information on US servers: that information should have stayed within the boundaries of the European Union.
Issue: Governments are progressively implementing online services in response to community expectations. However, many individuals do not trust their private data will be appropriately managed.

Question: How can governments improve citizens’ and businesses’ trust that their private data will be secured and only used for agreed purposes?

We believe the bigger questions that need addressing are:

- How do traditional government-issued offline credentials fare in an online world as a means of verifying identity?
- Should governments issue a new form of online identity?
- What role does multi-factor authentication play?

In short, current government-issued identity credentials are highly unreliable in terms of helping businesses establish the identity of their online customers. The online environment has proven a fertile place for the theft of government-issued (and financial) credentials which are then reused by criminals. As all tiers of government increasingly offer online transactional services to citizens, governments too will find that their own identity systems have failed them as a way of verifying the identity - and intent - of the person they are transacting with.

Establishing identity online

Businesses operating online often collect identity information in an effort to reduce the likelihood of fraud, and sometimes because of legislative requirements to “know your customer”. That identity information includes collecting and “verifying” similar information to the bank “100 point” system. There are online identity verification services that match supplied details against government lists, offering a “green light/red light” if the document details match those supplied by government. What these services can’t tell their customers is that the person presenting the credentials as the rightful owner, and not an unrelated third party.

Hypothetical:

A company offering an online financial service asks a prospective client for their full name, date of birth, Medicare number, passport number and place of issue, and driver’s licence details.

The business uses an online verification service, which makes a data call to various government agencies querying if a passport with the number and place of issue in the customer’s name was, indeed, issued. Same applies with the other credentials provided. All come back “green”: there were documents issued in that name with the same details provided.

This does not prove that the person presenting the credentials is the person they claim to be: that information can be obtained via phishing (where victims are tricked into giving away identity information); stolen from end user computers via malware; intercepted during legitimate transactions online via “man in the middle” or “man in the browser” attacks; or stolen, sold, lost or “hacked” from businesses who hold that identity data from previous interactions with the person.

The customer who appears to have presented “good” information may not be who they claim they are.

The business about to provide the goods or service as no idea from this information what the intentions of the customer are.
In fact, stolen credentials are actively traded online by criminals. Analysis of the prices demanded for identity information (like credit cards) shows that the price of data online has dropped rapidly. This is a simple supply and demand issue: criminals have been very successful at stealing data and the market is saturated. In fact, higher prices on identity data is only commanded now when the data thief can provide a basket of identity information, like, credit card number, expiry date, CCV2, mobile phone number, documents showing address on a utility bill, etc. Governments need to realise their ‘brand’ is susceptible to phishing attacks the same as any private sector organisation. They need to look beyond conventional IT security practices and procedures for securing their online services and creating a more trustworthy experience for citizens.

As governments offer greater online transaction engagement with the community they will increasingly see identity problems emerging: especially when there is a financial benefit involved, or another credential to be issued. It would be beneficial for government departments who are starting to engage in online transactions to learn from their peers in the private sector. Lessons learned faster will save the Australian economy significant budget losses. There is also a requirement to accurately address the issue of authenticating an online user in addition to the identity of such a user. Though similar terms, authentication requires proof that cannot be refuted, where identification relies on a simple match between data sets. For example you do not prove identity when using an ATM, only knowledge of the PIN.

In 2012 the Centre for Internet Safety will establish the Growing the Digital Economy Safely Working Group to help bring government and private sector leaders together to address structural issues impeding the growth of the digital economy, including trust in online identities.

Government issued identities in a web 2.0 world

If the Australian Government wants to realise its desire to see the digital economy continue to grow, it needs to start actively considering the issue of more secure online credentials, just as the US has entered the discussion with the National Strategy for Trusted Identification in Cyberspace (NSTIC).

We recommend:

7. Public sector agencies contact the Centre for Internet Safety to actively involve themselves in the Growing the Digital Economy Safely Working Group so that they may engage with their private sector counterparts

8. The Australian Government explore online credentials in light of the US Government’s NSTIC.

Case study:

A young man seeking work applied for a job advertised on a prominent online jobs site. The job advertiser sent him a pre-employment document to fill in to vet him for the job, which included his personal identity information and Tax File Number. The job never eventuated.

Later in the year the young man submitted an income tax return, expecting a refund, only to be informed by the Australian Taxation Office that the refund had been paid out some time earlier to “him”.

**Issue:** The digital economy presents both wide-ranging opportunities for increased productivity and innovation across the Australian economy and the risk of the loss of sensitive commercial data.

**Question:** How can small business awareness of commercial online opportunities be balanced with awareness of potential online risks and mitigation strategies?

**Question:** How can governments, industry, NFPs and consumer groups boost consumers’ confidence in engaging in e-commerce?

Clearly, the sky is not falling online, but there are behavioural and structural issues that should be addressed in the near and medium term to ensure Australia can maximise the benefits of the nascent digital economy. This should involve improving trust and confidence in the online channel, and creating an environment that enables people to go about their business peacefully, safely and unhindered online, much as they can offline in Australia.

**Behavioural issues**

It is difficult to talk about online crime without being seen as fear-mongering, but unless consumers and businesses are cognisant of the risks and consequences of those risks to their wellbeing and profitability, they are unlikely to take steps to minimise those risks.

In 2012 the Centre for Internet Safety will launch its *Surf Between the Flags Internet Safety Roadshow* specifically targeting regional and rural SMEs, parents, guardians and children to help improve online trust and safety in those audiences.

To date the dominant attitude of many businesses and consumers has been what we refer to as the "wildesteest" mentality: while recognising online threats exist, the sheer weight of numbers of users means that - statistically - they are unlikely to be targeted by criminals. While that theory held true in the early yeas of the Internet, automated and scaled attacks using social engineering and malicious code means that all end point devices are now targets.

Online transactional businesses run the risk of payment fraud (particularly card not present fraud), which has, anecdotally, been a significant barrier to entry for many smaller operations. Businesses run the risk of data theft pertaining to their IP, customers, and finances. The situation for SMEs is difficult: they do not possess the in-house expertise to look after sophisticated financial fraud nor IT security, and they generally cannot afford (or wish to prioritise spending) on outsourced solutions, many of which are priced for larger enterprises.

Our view is that scalable remote outsourced security and fraud services for SMEs will eventually grow to fill this void, possibly supplied by Internet Service Providers (ISPs). Increased adoption of software-as-a-service (the cloud) may also present an opportunity for improved security.

Successful online businesses know consumer activity is driven by three factors: value, convenience and choice. This was recently supported by a survey published by the ACMA.² Lack of confidence in the online channel acts as a dampener for consumers whereas a more confident consumer will engage more, use more services and spend more.

The best way to build confidence is for a consumer to engage in activities and for nothing untoward to happen to them.

Our economy would be healthier if consumer confidence was based on a more transparent knowledge of the threat environment and of the security incidents that occur. One enabler for such knowledge would be for Australia to implement the data breach notification recommendations contained in the Australian Law Reform Commission’s 2008 Privacy Act review. This would bring Australia in line with many other Western nations.

---

Structural matters
The “light touch” regulatory regime originally applied to telephone companies to encourage competition and growth and later transferred to Internet Service Providers by virtue of the fact that telephone companies tended to operate the first Internet services available to the public has not succeeded in delivering the appropriate safety and security necessary for long term sustained development. The market has failed to deliver safety, which could to a significant degree be delivered by ISPs stopping threats before they get to end point computers. They, after all, run the “pipes” that carry the traffic between computers. And they have a reasonably clear picture of what those pipes are carrying and what the end point computer is up to. Much of this knowledge is already captured for customer billing purposes.

The ability of ISPs to do this was highlighted by the formation of the iCode in consultation with the Commonwealth Government, where in a voluntary agreement ISPs undertook to identify compromised “zombie” end point computers that form part of botnets, and notify the customer to reduce the threat posed by that compromised computer.

We believe that while the iCode is a good first step, it needs to be substantially strengthened so that action taken by ISPs is more decisive, and expanded so that the code is mandatory for all ISPs in Australia. In addition, we believe the iCode highlights the future increased role that ISPs should play in overall Internet health, and that in time they should throttle malicious code and other illegal activities occurring across their networks.

We recommend:

10. the Commonwealth Government continues engaging ISPs in relation to strengthening and expanding the existing iCode.
**Issue:** Industry and governments need to strike the right balance between improving awareness of and protecting against cyber threats, while also encouraging consumers to take advantage of the benefits of the digital economy.

**Question:** How can governments and the private sector continue to build and maintain confidence in the digital economy while also raising awareness among consumers and small businesses of the nature of cyber threats?

**Question:** How can governments and the private sector continue to build and maintain confidence in the digital economy while also raising awareness among consumers and small businesses of the nature of cyber threats?

**Question:** How can we improve and encourage the reporting of data breaches in Australia?

**Question:** How can e-businesses more effectively work together to develop a self regulatory feedback system that provides a way of sharing their experiences with other online traders?

We understand that the Government is currently investigating the feasibility of implementing an online crime reporting capacity so that victims of online crime can report matters more easily to police and regulators.

We have strongly supported this initiative for some time.

We trust that the focus of this capacity has not been unduly narrowed to “cybercrime” as defined by the Cybercrime Act 2001 (unlawful access to, modification or impairment of data, ie, hacking, denial of service, etc) but rather kept broad to include crimes that are significantly enabled by online technologies as well, such as investment and romance scams, and Internet auction fraud. It would be a pity if government got the message that victims should not have to understand the bureaucratic jurisdictional maze of police and regulatory agencies only to be replaced by the frustration of an equally bureaucratic demarcation of crime definitions.

In terms of online safety and security messaging supported by government, we believe amalgamating and more closely coordinating the various public-private partnerships would be more efficient and effective. Thus the cyber safety activities of the ACMA, the cyber security activities of the Department of Broadband Communications and the Digital Economy, and the online consumer fraud awareness efforts of the Australian Competition and Consumer Commission should be amalgamated.

Should an Office of Cyber Security be created within the Commonwealth, we believe that would be the best custodian of the combined effort. Should no such body be created, we believe one of the aforementioned agencies would be next best placed to carry on the task. Proper metrics should be developed to assess the success or otherwise of such programs. This should be based on demonstratable user behavioural change of a period, rather than ‘hits’ on a website, or number of media mentions.

All such messaging would be less effective without the continued participation of the private sector, as they own the majority of Internet-facing systems and also maintain close relationships with their customers.

We hope that in time government-led safety initiatives will be evidence-based, just as public health campaigns are: with a sound understanding of the economic, behavioural and environmental factors that need to change in order to affect base-line statistics.

**We recommend:**

11. A cybercrime reporting capability take a broad definition of cybercrime to include all aspects of the misuse of online technology, including Internet frauds and scams.

12. Existing Internet safety, security and scam public-private education efforts be amalgamated under one organisation for the purposes of efficiency and effectiveness.
**Issue:** Police resources are finite and cybercrime investigations are inherently time and resource intensive. Consequently, the growth in cybercrime activity poses significant challenges to Australia’s state and territory and federal police services.

**Question:** What does the Australian public expect from policing and consumer protection agencies in relation to preventing and investigating cyber crimes?

While we acknowledge many of the difficulties to investigating online crimes, such as the involvement of overseas jurisdictions and high volume, we believe the level of difficulty is over-played: this is a matter of prioritisation and effort on the part of law enforcement agencies. If the same effort was applied to many of these crimes as, say, drug interdiction and investigation, we would be in a very different situation.

In many respects law enforcement has vacated the field before the fight has been had.

Law enforcement agencies need to fundamentally change the way they think about online crimes and digital evidence. For too long it has been seen as the domain of technical analysts to deal with such matters. The analogy of how traffic enforcement is conducted needs to be parlayed in the online environment. Presently, all uniformed police officers are trained and have the equipment to conduct traffic stops and random breath testing; they competently enforce a wide range of laws; travel in marked and un-marked vehicles; conduct school education campaigns; are more visible in high impact times and locations; and dedicate significant advertising spend in the mainstream media. All these aspects can be mirrored for enforcement of online crime.

State and territory governments need to take the online environment much more seriously, by appropriately funding law enforcement and related agencies to detect and dismantle such criminal activity.

Victims of online crime need to be treated as victims, with dignity and respect, regardless of the channel of their victimisation. A victim of online identity theft is as much harmed as the victim of a traditional identity theft. Having $100,000 stolen from a business offline is as damaging to a business losing $100,000 online.

If law enforcement agencies consistently refuse to take complaints, we believe the public will have diminished respect for those institutions. Certainly criminals will. We hope the current Commonwealth scoping of an online crime reporting capacity will address this issue.

Such a reporting capability will mean that victims need not know the internal bureaucratic divisions between agencies, they need not report multiple times. A modest clearing house needs to be created with the reporting portal to accurately and quickly forward consumer complaints to the appropriate organisation, even though much of this can be automated. There will be a greater chance this information fits into a bigger crime picture, leading to more effective criminal investigations, disruption and crime prevention.

We also believe that the act alone of taking the complaint will satisfy a significant proportion of victims, many of whom are rational about the likelihood of justice being served, but who feel the need to tell their story.

**We recommend:**

13. State, territory and Federal police consider operating procedures, training and structural reform in light of the Australia community’s wholesale adoption of Internet and mobile devices so that they can better respond to cybercrime complaints.

14. Victims of crime should be treated in a “channel of victimisation” agnostic way: all victims of a similar offence receive similar, respectful, manner.
15. A modest clearinghouse be established to ensure online crime complaints are directed efficiently to appropriate agencies.
**Issue:** One of the primary impediments to e-commerce is consumers' fear that their financial or personal details may be at risk when conducting business online. Anonymity will remain a key part of the Internet, but trust and confidence in the digital economy may be undermined if people’s financial and personal details remain at risk of being stolen by criminals.

**Question:** What options are there for increasing consumers’ trust in conducting business online?

**Question:** How can consumers be encouraged to take more responsibility to protect their information?

**Question:** What are the options for broadening industry's efforts to provide customers with a greater level of trust and confidence in the security and privacy of their online transactions?

**Question:** What information would help consumers and small businesses better protect themselves and enhance their trust and confidence online?

**Question:** What do consumers and small businesses expect from their Internet Service Providers (ISPs), software and hardware providers and the government to assist them to maintain or enhance their confidence online?

**Question:** How can governments and industry work together to make Australia a difficult place for cyber criminals to target?

Failure to improve end user and business safety and security online will, in effect, “poison the well” for all online: overall trust and confidence in the channel is at stake.

In our extensive experience dealing with Internet businesses from a government regulatory viewpoint, there is an over-reliance in government on the effect stronger “warning” messages will have on consumer behaviour on websites. While we firmly believe consumer education, including warning messages play a role, we are not convinced they have tangible cut-through most of the time. For example, the Australian Competition and Consumer Commission has worked with key dating industry websites to insert stronger “warning” messages on their websites as part of a three point strategy to reduce dating and romance scams.³

It is actually the second point in their strategy that will have the highest impact: “internal verification processes and procedures in relation to profiles on dating websites to detect and disrupt the activities of those seeking to engage in fraud.” Designing out risk is the key, but it is also the hardest and most expensive thing for companies to do. Unfortunately it is easier for companies to placate government with the messaging than to achieve meaningful structural reforms.

**End user responsibility**

Our society is built on the premise that end users are largely responsible for their actions. There is no doubt that in terms of Internet safety and security, end users can influence their level of risk. But we believe there has been an over-emphasis on the role of the end user that has allowed policy and operational areas in government to shift the burden too far in that direction.

Just as the public can reduce the spread of flu viruses via simple processes like washing hands and covering mouthes when coughing, so too can end users of computers. It is sensible, for example, that end users

- Automatically “patch” their operating system and applications running on their devices
- Run anti-virus and firewall programs, and automatically update them

---

³ [http://www.accc.gov.au/content/index.phtml/itemId/1009862/fromItemId/ACCC#presentation](http://www.accc.gov.au/content/index.phtml/itemId/1009862/fromItemId/ACCC#presentation) accessed November 2011
Use unique strong passwords that contain letters, numbers and characters for every service they use - and change them regularly

Exercise discretion in relation to how much personal information they expose online, particularly via social networking sites, and how widely they share that information

Pay for goods and services online with care, preferably using a payment service that does not share your personal financial information (like credit card details) with the person you are transacting with

The list goes on.

But what seems sensible on paper is not always how people actually act. For example, reading user agreements for Internet services seems sensible, but we believe only a very very small fraction of the community reads such material and service providers know this, which is why the option to acknowledge you have read and understood the terms and conditions of a website or service or software invariably appears as a check box at the start of the user agreement. Indeed the length, use of small fonts and legalistic content of such agreements makes it almost impossible for users to comprehend them.

End users have also been the subject of sustained and often clever "social engineering" (phishing) and malicious code attacks on an industrial scale since the early 2000's. Phishing remains viable today because education and awareness has not had the behavioural-changing cut through we would have hoped. Even if it did, we would see a shift to more sophisticated malicious code attacks which would be even harder to defeat. Rather, operators of businesses online, as well as hardware and software manufacturers, along with governments, can and should do more to protect people and businesses operating online.

Goods and services offered online should be fit for purpose, just as we expect offline goods and services to be. Companies need to tighten offerings and not ship when significant flaws are known to exist in a product. We should apply offline product liability regimes to online services and software.

While they are still evolving, and will not provide 100% protection, that a standards-based approach to online offerings would greatly enhance end user and business protections. If industry fails to apply meaningful voluntary standards like ISO 27001 on a wide scale basis, governments should consider mandating, just as they have in the banking and finance sector.

ISPs have a far greater role to play than they are comfortable with taking: they know a great deal of what happens on their networks and should not knowingly serve (nor be willfully blind to) harmful code or actions for end-point devices.

The iCode, that came into effect in December 2010 is both a step-change and only a first step: it is significant because ISPs acknowledge they can actually help improve security broadly for the community and have agreed in a voluntary, non-binding, and unfortunately loose way that they may act. It is a first step because ISPs can and should do more.

One pre-condition for greater "network" level proactive protection is to ensure their are adequate "safe harbour" legal provisions in place to protect ISPs, financial institutions and other businesses to take action, sometimes against the instructions of their customers to protect the customer or other customers, much like a publican's role in the "responsible service of alcohol": if they act in good faith to stop delivering their service they are protected against litigation.
We recommend:

16. Offline product liability regimes be applied to online services and software.

17. Governments should consider mandating standards like ISO 27001 if industry does not improve.

18. The iCode should be expanded and strengthened to increase the protective and intervention role for ISPs.

19. Government should ensure there are adequate “safe harbour” legal provisions in place to protect ISPs, financial institutions and other businesses to take action, sometimes against the instructions of their customers in order to protect the customer or other customers.
Issue: Damaging criminal activities are often aided by the use of botnets, built as a result of many individuals unwittingly operating virus-infected computers. The AFP estimates that the overall risk of cyber crime to the Australian economy is more than a billion dollars a year. This is likely to grow substantially as Australia’s digital economy expands.

Question: What are the options for limiting the collective economic and societal costs of widespread individual security lapses?

Question: What role do individuals, businesses and, more specifically, ISPs and large online companies, have in limiting the collective harm compromised computers have on the Australian economy and to the broader well-being of the Australian community?

We applaud the iCode initiative that was the result of consultations between Government and the Internet Industry Association but believe it could go further and have less latitude regarding the actions of ISPs once an infected end point computer is discovered. Placing the computer in a virtual “walled garden” until the operator can successfully demonstrate the device is “clean” would be the most effective option.

There are also examples of sound police work by some agencies offshore that should be replicated from time-to-time by Australian police like the FBI working with Estonian police and private sector companies to take down the Esthost botnet of some 4,000,000 compromised end points.5

To their credit, several significant companies operating online invest in efforts to keep the Internet as a whole safer. Foremost among those is Microsoft, through the activities of their Digital Crime Unit.5

We recommend:

20. The iCode should be tightened to give ISPs less latitude in the actions they take when an infected device is detected.

21. Australian police should seek to engage major tech companies who invest in overall internet health and seek investigative partnerships.

6 http://www.facebook.com/MicrosoftDCU
**Issue**: The effects of cybercrime and scams often extend beyond the immediate financial impacts. Many instances of online crime go unreported, so the full extent of the problem is not known.

**Question**: How can Commonwealth and state and territory governments encourage victims to report incidences of cybercrime and scams and better assist them with support and advice?

**Question**: How can Commonwealth and state and territory governments obtain the information and data required to form a more precise assessment of the extent of the economic and social harm caused by cyber crime?

As discussed previously, we understand that the Government is currently investigating the feasibility of implementing an online crime reporting capacity so that victims of online crime can report matters more easily to police and regulators.

We have strongly supported this initiative for some time.

We trust that the focus of this capacity has not just been unduly narrowed to “cybercrime” as defined by the Cybercrime Act 2001 (unlawful access to, modification or impairment of data, ie, hacking, denial of service, etc) but rather kept broad to include crimes that are significantly enabled by online technologies as well such as investment and romance scams, and Internet auction fraud. It would be a pity if government got the message that victims should not have to understand the bureaucratic jurisdictional maze of police and regulatory agencies only to be replaced by the frustration of an equally bureaucratic demarcation of crime definitions.

Once governments have a better understanding of reported victimisation via efforts to make online crime reporting possible, they will be able to more effectively engage industry to access further information, and to work with industry on disrupting trends. Our dealings with industry over many years from a government, corporate and consulting perspective indicates to us that industry is willing to assist government, within legal and proper privacy boundaries, of course.
**Issue:** Small businesses often lack access to the security controls employed by government or other larger enterprises, yet consumers expect small businesses to secure their data and transaction appropriately.

**Question:** How can government, ISPs, financial institutions and small businesses collaboratively create an environment where small businesses are empowered to operate in a safe and secure manner online?

As discussed previously, online transactional businesses run the risk of payment fraud (particularly card not present fraud), which has, anecdotally, been a significant barrier to entry for many smaller operations. And all businesses run the risk of data theft pertaining to their IP, customers, and finances. The situation for SMEs is difficult: they do not possess the in-house expertise to look after sophisticated financial fraud nor IT security, and they generally cannot afford (or wish to prioritise spending) on outsourced solutions, many of which are priced for larger enterprises.

Our view is that scalable remote outsourced security and fraud services for SMEs will eventually grow to fill this void, possibly supplied by Internet Service Providers. Increased adoption of software-as-a-service (the cloud) may also provide an opportunity for improved security.
**Issue:** Much of the public discussion on cyber threats and risks to date has focused on national security issues. This important dimension has inadvertently hidden the reality that at its most basic level, security and safety online is reliant on the awareness of individuals. As a result, many businesses and consumers are not as mindful of cyber threats as they could be.

**Question:** How can the Commonwealth, states and territories and industry effectively communicate the interdependent nature of individual and national cyber security? How can the importance of individual behaviour be highlighted in creating a secure, trusted and resilient online environment for all Australians?

**Question:** How can citizens better protect themselves from cyber threats?

**Question:** Are individuals adequately aware of cyber threats and the steps they should take to protect themselves? If not, why not?

One of the reasons for a conservative Commonwealth policy in this area - which in our view is inadequate for the scale of the threat and the level of reliance the Australian economy has on digital devices - is that cyber security and cyber crime threats have been viewed on a spectrum: small “petty” crime on one end like a compromised home computer through to full scale cyber warfare on the other. In fact they should viewed as a network: the compromised home computer may concurrently be used as part of a botnet “zombie” army to launch denial of service attacks against a big online business; be draining personal and financial identity information for later exploitation against the computer owner; may be used to store child exploitation images; and to send spam emails. Where on a linear spectrum should that one compromised home computer be placed?

A Commonwealth employee may, in their own time, and quite properly, place personal information on a social networking site that may later be used to “socially engineer” them in a state-sponsored attack against a government system they use during working hours.

This is one of the reasons why we have so consistently supported the creation of an online crime reporting facility: we don’t know until an incident is correlated and cross-referenced where it may fit in the overall crime and security network.

**We recommend**

22. Commonwealth policy departments adopt a “network” interconnected approach to understanding and assessing cybercrime.
**Issue:** The attractions of the internet in terms of openness, access to information (of all qualities) and informal governance are also creating tensions with traditional government responses to community interests.

**Question:** What model of Internet governance is in the best interests of all Australians?

**Question:** How can we get the right balance between Australia’s social, economic and security needs when developing an Australian vision for the online environment?

While we are firm supporters of improving cyber safety and cyber security for the benefit of the broader community, we believe that must be carried out in a manner that preserves as far as possible the freedoms and values we expect offline in Australia. We want to ensure the Internet remains a place of creativity and (reasonably) free expression. We also understand that far from being a “global village”, the internet is actually a set of many “villages”, each encroaching on the other, and in those various villages there are different behaviours, expectations and views.

These are certainly not new tensions, merely that they are magnified somewhat online.

In terms of Internet governance, the Australian Government has sovereignty over the physical systems operating within the confines of our nation. We believe the Government has a right - and the public has an expectation - that they will exercise that sovereignty in a manner that protects and preserves society just as the government aims to do in offline situations. In order to do this effectively we believe the government needs to change form its current “light touch” approach to a more interventionist one.

That should also entail telling multinational corporations offering services to Australians what government expectations are.

In relation to offshore crime and broader Internet governance, the Australian government must rely upon its traditional mechanisms for engagement: bilateral, multilateral and international agreements to help build frameworks for acceptable behaviours, preservation of evidence, investigations, protection of data etc.

Further, the Australian government should consistently and significantly play a part in the more unique Internet governance bodies such as ICANN and the Internet Governance Forum.

Without proper security, regulation, policy and privacy arrangements in place, the gains from building an online economy, through the provision of new businesses, services and the physical infrastructure, will provide little benefit to their citizens, communities and economies. Rather, the online information and service economy will simply provide a vector for (predominantly overseas based) cyber criminals to prosper at their expense with relative impunity.

Just like Australia, South East Asia and Pacific Island nations are not immune from international organised crime groups and state sanctioned actors seeking profit, corporate proprietary information or the revelation of government secrets. Indeed, Pacific governments could be seen as a soft target to gain information, not just about their own affairs, but also their communication with other sovereign governments.

Also like Australia, each Pacific Island has its own Top Level Domain name giving it influence yet requiring prudence in its management and that of lower-level domains subsequently administered. Indeed, as the Pacific Islands have been previously targeted as havens for money laundering and as transit points for large-scale narcotic importation, they are susceptible to electronic attacks from criminals or rogue states. The Top Level Domains of many nations are favoured by criminals, further damaging the level of trust in legitimate business and government activities in those countries.
It is in Australia’s national interest for Pacific Island government, business and end user computer systems to be robust and secure. It is also in Australia’s interest for our closest neighbours to reduce the proportion of economically-marginalised people and improve their opportunities to lead a better life.

We recommend:

23. Efforts to improve cyber safety and cyber security for the benefit of the broader community be carried out in a manner that preserves as far as possible the freedoms and values we expect offline in Australia.

24. The Government exercise its sovereignty over Australian networks in a manner that protects and preserves society just as the government aims to do in offline situations, reducing its “light touch” approach.

25. In relation to offshore crime and broader Internet governance, the Australian government must rely upon bilateral, multilateral and international agreements.

26. The Australian Government engage with multinational corporations offering services to Australians to outline government expectations.

27. In relation to offshore crime and broader Internet governance, the Australian government must rely upon bilateral, multilateral and international agreements.

28. The Australian government should consistently and significantly play a part in internet governance bodies such as ICANN and the Internet Governance Forum.

29. The Australian Government enhance existing Aid programs to include aspects of cyber security for developing nations to increase governance and productivity.
**Issue:** Increasingly, policy makers have turned to discussing what agreements governing behaviour in the online environment might look like, the principles they should be based on, the boundaries they would place on behaviour and how they can be promoted. This will be a gradual and long-term process, and varying stakeholders are likely to want different outcomes from any agreement process.

**Question:** What sort of approach should be taken to developing agreements on behaviour in the online environment?

There is no reason why acceptable behaviour online should be different to acceptable behaviour offline. As such, we believe the Australian Government should pursue legislative and policy programs along those lines. As representatives of the people, Parliament - and the processes around Parliament - is best suited to determine that acceptable “Australian” behaviour.

Where possible we should avoid legislation specifically centered on technology, instead we should look to apply offline laws and regulations online. Where there is doubt, those matters should be tested in court, and deficiencies such as they may be, addressed as needed.

We recommend:

30. The Government take the view that acceptable behaviour online should be no different to acceptable behaviour offline.

31. Government should avoid legislation specifically centered on technology, instead applying offline laws and regulations online.
**Issue:** The demand for skilled cyber professionals in both the public and private sector will continue to grow at a rapid rate and it is likely that those companies - many of which will be based overseas - offering the best financial incentives will attract the best of Australia’s ICT graduates. However, a purely market-led distribution of skilled cyber workers may not meet the broader digital needs of Australia as a nation.

**Question:** What strategies should be pursued by governments, industry and academia to ensure adequate levels of domestic expertise are available to maximise the opportunities of the digital economy and address risks to Australia’s digital infrastructure?

**Question:** What new forms of government-industry cooperation and dialogue are required to ensure the Australian cyber skills base is developed to meet Australia’s broader national interests?

An area requiring immediate Government attention is the dwindling size of the cohort of young IT security professionals who may be eligible to work in sensitive national security areas of government. While there is a burgeoning IT security training industry in Australia, many students are foreign nationals, who will not be able to obtain high level security clearances for work in national security, police and defence agencies, even if they wished to do so.

Government should consider programs to encourage Australian nationals to undertake IT security studies with a “return of service obligation” within national security, policing and defence agencies.

Given the relatively small size of the Australian economy, Government backing for formation of centres of excellence around key IT security and investigative capabilities should also be considered. Fields could include cyber safety, cyber crime and cyber security, computer forensics, policy, and law.

**We recommend:**

32. Government should consider programs to encourage Australian nationals to undertake IT security studies with a “return of service obligation” within national security, policing and defence agencies.

33. Government backing for formation of centres of excellence around key IT security and investigative capabilities should also be considered.