SUBMISSION NO. 26

CIS
Centre for Internet Safety

MARCH 2012

Inquiry into Cyber Safety for Senior Australians

Foreword

The Centre for Internet Safety at the University of Canberra appreciates the opportunity to make this submission to the Parliament of Australia's Joint Committee on Cyber Safety Inquiry into Cyber Safety for Senior Australians.

It is our view that most of the issues faced by senior Australians online are common to other online demographics. As a consequence, much of the content of this document is taken from the Centre for Internet Safety's November 2011 submission to the Cyber White Paper process coordinated by the Department of Prime Minister and Cabinet.

We have also chosen to focus on the third and fourth aspects of the Committee's terms of reference, namely:

3. *the adequacy and effectiveness of current government and industry initiatives to respond to those threats, including education initiatives aimed at senior Australians;*

4. *best practice safeguards, and any possible changes to Australian law, policy or practice that will strengthen the cybersafety of senior Australians.*

We would be very happy to provide further information and details on the issues we raise.

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. Education of end-users is a difficult task that requires repetition to have any effect. And the effect should not be over-relied upon to create a safe environment. Structural and technical issues of the Internet will be just as important to improving the cyber safety of senior Australians.
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. A more robust stance from the Australian Government towards online content providers in relation to demanding acceptable behaviours and reduced criminality on their networks.
5. 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
6. The Commonwealth Government implements recommendations of the 2008 Australian Law Reform Commission review of the Privacy Act regarding mandatory data breach notification legislation.
7. The Commonwealth Government continues engaging ISPs in relation to strengthening and expanding the existing iCode.
8. 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.
9. Existing Internet safety, security and scam public-private education efforts be amalgamated under one organisation for the purposes of efficiency and effectiveness.
10. Offline product liability regimes be applied to online services and software.
11. Governments should consider mandating standards like ISO 27001 if industry does not improve.
12. The iCode should be expanded and strengthened to increase the protective and intervention role for ISPs.
13. 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.
14. Commonwealth policy departments adopt a “network” interconnected approach to understanding and assessing cybercrime.

Our philosophy on creating Internet environments encouraging pro-social 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, threaten us, help us.

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.
- Education of end-users is a difficult task that requires repetition to have any effect. And the effect should not be over-relied upon to create a safe environment. Structural and technical issues of the Internet will be just as important to improving the cyber safety of senior Australians.

<u>We recommend:</u>

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. Education of end-users is a difficult task that requires repetition to have any effect. And the effect should not be over-relied upon to create a safe environment. Structural and technical issues of the Internet will be just as important to improving the cyber safety of senior Australians.

Perceptions of anonymity decrease cyber safety

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 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.

Creating a safer online environment

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 anti-social 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.

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.

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.

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 and end users 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 "wildebeest" mentality: while recognising online threats exist, the shear 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.

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.[1] 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

[1] "Let's Go Shopping...Online" http://engage.acma.gov.au/commsreport/e-commerce/ accessed November 2011

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, afterall, 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:

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

5. 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

6. The Commonwealth Government implements recommendations of the 2008 Australian Law Reform Commission review of the Privacy Act regarding mandatory data breach notification legislation.

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

Helping senior Australians report incidents

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 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 demonstrable 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.

As previously stated, in 2012 the Centre for Internet Safety will launch its *Surf Between the Flags Internet Safety Roadshow* specifically targeting regional and rural SMEs and end users to help improve online trust and safety in those audiences. This will help augment government efforts that - to date - have not scaled sufficiently to impact online user behaviour.

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.

<u>We recommend:</u>

8. 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.
9. Existing Internet safety, security and scam public-private education efforts be amalgamated under one organisation for the purposes of efficiency and effectiveness.

Improving end user security and safety

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.[2]

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.

<u>End user responsibility</u>

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

[2] http://www.accc.gov.au/content/index.phtml/itemId/1009862/fromItemId/ACCC#presentation accessed November 2011

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
- Use unique strong passwords that contain letters, numbers and characters for every service they use - and change them regularly[3]
- 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, 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

[3]

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:

10. Offline product liability regimes be applied to online services and software.
11. Governments should consider mandating standards like ISO 27001 if industry does not improve.
12. The iCode should be expanded and strengthened to increase the protective and intervention role for ISPs.
13. 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.

A "network" approach to prioritising Government efforts

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 belonging to a senior Australian through to full scale cyber warfare on the other. In fact they should viewed as a network: the compromised home computer belonging to the senior Australian 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

14. Commonwealth policy departments adopt a "network" interconnected approach to understanding and assessing cybercrime.