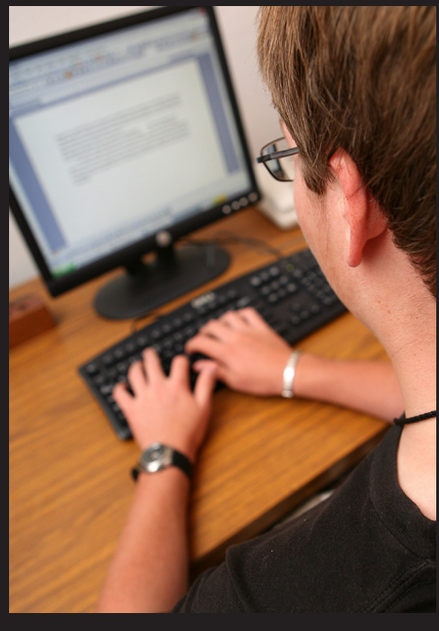
Australian Government



A PUBLIC DISCUSSION PAPER

Connecting with Confidence

Optimising Australia's Digital Future

Published by the Department of the Prime Minister and Cabinet

ISBN (PDF): 978-1-921739-49-1

ISBN (Hardcopy): 978-1-921739-48-4

ISBN (RTF): 978-1-921739-50-7

An open invitation

This discussion paper is a 'conversation starter', designed to allow all Australians to participate in an open discussion on how government, industry and the community can work together to address the challenges and risks arising from greater digital engagement and, in doing so, complement the government's vision for Australia to become a leading digital economy by 2020. The result of this conversation will be the release of Australia's first Cyber White Paper in the first half of 2012.

This discussion paper seeks your views on a wide range of issues, including how we can together minimise cyber risks so we can maximise social and economic opportunities in the digital economy. We greatly value your views on how we can get the right balance between Australia's social, economic and security needs. The discussion paper is not designed for a technical audience. However, a glossary of terms has been provided at the back of the document to assist readers unfamiliar with terms or concepts.

The Cyber White Paper website (www.cyberwhitepaper.dpmc.gov.au) will enable electronic lodgement of submissions relating to questions in the discussion paper. Written submissions can be forwarded electronically to cyberwhitepaper@pmc.gov.au or via mail to the Department of the Prime Minister and Cabinet, One National Circuit, Barton, 2600, ACT.
The White Paper team will accept written submissions from 14 September to 14 November, after which formal submissions will close.
The final White Paper will be released in the first half of 2012.

Connecting with Confidence

Optimising Australia's Digital Future

Table of Contents

Why a Cyber White Paper? 5

Digital citizenship in a networked society 7

- An engaged, participatory and networked society 7
- Online government service delivery 7
- Online behaviour – the need for a digital social contract? 8
- Safety – protecting young people online 9
- An unfettered domain 9
- Privacy and identity security 10
- What does it mean to be a digital citizen? 10
- Key issues and questions 10

Protecting and promoting Australia's digital economy 12

- The economic benefits of going digital 12
- Crime online – threatening confidence in the digital economy 13
- The vulnerability of intellectual property 14
- Consumers, NFPs and small businesses uniquely vulnerable 14
- Local police and consumer protection agencies on the front line 15
- Key issues and questions 16

Security and resilience in the online environment 18

- Increased security capabilities and societal resilience 18
- Cyber vulnerabilities and risks 18
- Mitigating the cyber threat 19
- Key issues and questions 19

International partnerships and Internet governance 21

- A new paradigm of partnerships 21
- Internet governance – the future of the digital environment 21
- International norms of behaviour in cyberspace 22
- Cooperating with partners 22
- Key issues and questions 22

Investing in Australia's digital future 23

- Growing demand for digital skills 23
- A digitally literate nation 23
- Attracting international investment 24
- Key issues and questions 24

References 26

Glossary 30

Connecting with Confidence

Optimising Australia's Digital Future

Why a Cyber White Paper?

The Internet and digital technologies are evolving and are having an increasingly powerful influence on Australia's economy, society and security. With the roll out of the National Broadband Network (NBN) gaining pace and a growing number of Australians using the Internet, Australia is increasingly 'connected' and consequently well placed to derive substantial social and economic benefits from the use of digital technologies. At the same time as digital engagement is increasing and being encouraged, so too are reports of people and businesses being exposed to and harmed by risks in the online environment. Consequently, it will be necessary to ensure there is a broad awareness of the risks associated with digital technologies so Australians have the tools and knowledge to mitigate these risks and can connect with confidence.

The government will release a Cyber White Paper in the first half of 2012 to ensure Australia is well prepared to optimise the benefits of greater online engagement. The White Paper will outline how government, industry and the community can work together to address the challenges and risks arising from greater digital engagement. This complements the government's vision for Australia to become a leading digital economy by 2020 as outlined in the *National Digital Economy Strategy*. The Strategy outlines an optimistic vision which views digital technologies driving productivity, innovation and integration across our economy; empowering citizens; increasing the reach of critical services and reducing their costs; and connecting Australians to one another and to the world. Central to achieving this vision will be ensuring confidence, trust, resilience, security and safety characterise our nation's engagement in the online environment.

As a strategic blueprint, the White Paper will place the government's existing initiatives and strategies within the context of a holistic and integrated framework and will highlight the central importance of partnerships with industry and community groups.

The cyber threat is growing

Various individuals and groups, including nation-states, sophisticated cyber criminals, politically motivated hackers and cyber bullies are making use of cyber tools to harm Australia's social wellbeing, economic prosperity and broader national interests. Cyber tools are cheap to acquire and the growing value of information that individuals, businesses and governments store online is motivating a growth in malicious cyber activity. The impact of the growing threat includes:

- The overall risk of cyber crime to the Australian economy is more than a billion dollars a year [AFP: 2010].
- In 2010 major cyber intrusions cost Australian organisations an average of $2 million per incident [Symantec: 2011].
- Reported online scam losses totaled more than $63 million in 2010, with 45 per cent of reported scams occurring online [ACCC: 2011].
- More than 50 percent of all Australian teachers had at least one cyber-safety incident directly reported to them in 2010 [IRIS: 2011].
- Over 200 cyber intrusions against the Department of Defence were investigated in 2009 [Defence: 2010].

This framework builds on the *2008 Cybersafety Plan* and *2009 Cyber Security Strategy*. It includes the establishment of the national computer emergency response team (CERT Australia) in the Attorney-General's Department, the Cyber Espionage Branch within the Australian Security Intelligence Organisation (ASIO), and the Australian Federal Police's High Tech Crimes Operations portfolio. The framework includes the establishment of the Cyber Security Operations Centre in the Department of Defence as a result of an initiative of the 2009 Defence White Paper. (For further information on the

government's existing cyber policy efforts see *Safety and Security Online: An update for all Australians*).

Such a framework will ensure Australian households, schools, businesses and regions enjoy the benefits from existing government initiatives, including the *Digital Regions Initiative, Digital Enterprises Program, Digital Communities Program* and *Digital Education Revolution* and future activities associated with the *National Digital Economy Strategy*.

By aligning and streamlining the government's broad ranging cyber policy efforts, the White Paper will maximise opportunities to find efficiencies and synergies and will highlight the areas where greater effort is required. The White Paper will emphasise the shared responsibility of government, business, not-for-profits (NFPs), and individuals, in achieving a joint vision for Australia's digital future.

An associated goal of the White Paper is to 'mainstream' cyber issues. Cyber risks and cyber opportunities are not issues just for the consideration of information, communications and technology experts. Digital technologies are now so deeply embedded into the daily lives of all Australians that they need to be considered a normal part of the activities of governments, businesses, NFPs and individuals.

This paper is structured to stimulate discussion on how government, industry and the community can work together to address risks and challenges. The purpose is to focus on those issues that may have the most important and enduring implications for the future prosperity and wellbeing of all Australians.

Australia's online engagement

An increasing number of Australians are joining the online community and are using faster speeds to do so.

- At the end of December 2010, there were 10.4 million active Internet subscribers in Australia [ABS: 2010].
- Ninety-three per cent of Internet connections are no longer dial-up and 81 per cent of connections offer a download speed of 1.5 megabits or greater [ABS: 2010].

The amount of time people spend online and the amount of data they consume is increasing.

- From June 2005 to June 2010, the number of Australians considered heavy users (online activity of more than 15 hours a week) of the Internet doubled [ABS: 2010].

Once online, data consumption is increasing.

- In December 2010, Australians downloaded 191 839 terabytes of information. This was almost twice as much as was downloaded in the 2009 June quarter [ABS: 2010].

The vast majority of data is downloaded via fixed-line broadband services (91 per cent of data downloads) [ABS: 2010].

Digital citizenship in a networked society

The daily social interactions of a growing number of Australians have been altered fundamentally by the pervasiveness of digital technologies.

As Australians gain more experience in the online world we are increasingly engaging in social and participatory activities. The roll out of the NBN, the steady migration of media and entertainment services online, and the convergence of these and other online services onto mobile devices such as smartphones and tablets is likely to see expanded social interaction through the Internet over the next decade.

Digital technologies will increasingly form the underpinnings of the full-spectrum of our social interactions. As these technologies evolve, and as we become more active participants in the online environment, we will increasingly be 'digital citizens'. Social media sites such as Facebook, Twitter and YouTube have facilitated the development of rich, complex and productive online civic spaces. Already Australians are avid users of digital technologies and the next generation of Australia's workforce, political and industry leaders and entrepreneurs will be 'digital natives'. For example, research from the Australian Communications and Media Authority (ACMA) shows 8.4 million Australians accessed social networking sites and 5.5 million accessed video streaming sites from home during December 2010.

An engaged, participatory and networked society

In general, the increased use of social networking sites by Australians and their friends, families and collaborators internationally has led to a far more productive set of social interactions. This collective and creative social action has already produced outcomes that have broader societal benefits, such as the creation of free, interactive, web-based services – like wikipedia.org. Wikipedia is now one of the most popular sources of information worldwide, with more than 3.6 million English language articles [Wikipedia: 2011]. Wikipedia has not only made information more accessible, it has also democratised the creation of knowledge, allowing relevant experts to update and research discrete topics, no matter their background, institutional affiliation or physical location.

Online government service delivery

Outside these innovative, citizen-driven, digitally enabled services, traditional government-provided services, such as public health, education and social welfare have also been augmented by digital connectivity.

Online delivery of government services and programs reduces costs and increases efficiencies. It also leads to enhanced customer services and enables greater teleworking by government employees. Importantly, governments' use of online service delivery will continue to grow.

The Australian Government Information Management Office's (AGIMO) *Interacting with Government 2009* [AGIMO: 2009] report indicates that those who contacted government by Internet have the highest level of satisfaction (91 per cent). Given a choice, most Australians would prefer to use an e-Government channel to access a government service. Consequently the National Digital Economy Strategy outlines a goal that by 2020, four out of five Australians will choose to engage with the government through the Internet or other type of online service.

The 2008 *National E-Health Strategy* highlighted both the government's intention to digitise the Australian health system and the great benefits digital technologies can bring to the health sector. A digitally enabled health sector allows a greater capacity to share and access health data, and increases collaboration and interoperability. As a consequence, the Australian health system will be able to do more with existing resources, allowing the right health resources to be deployed against real need, ultimately leading to better health outcomes for all Australians.

A more digitised health sector, particularly when high-speed broadband is more widely available, will improve the capacity of health professionals to consult with patients via teleconferencing facilities. Telemedicine will reduce travel costs and increase the reach of medical professionals, providing much needed medical support to rural and remote patients and for those with afflictions that limit mobility.

That is why the *National Digital Economy Strategy* sets a goal that by 2020, 90 percent of high priority consumers can access electronic health records, with 495,000 telehealth consultations delivered by 2015.

Similarly, education institutions are embracing the benefits of going digital. The government's *Digital Education Revolution* (DER) aims to contribute sustainable and meaningful change in teaching and learning to prepare students for further education, training, work and life in a digital world. The DER aims to support the effective integration of information and communications technology (ICT) in Australian schools, the digital proficiency of teachers and students and the use of innovative digital teaching and learning tools.

The *National Digital Economy Strategy* sets a goal to extend and develop online educational services, resources and facilities through Australian schools, universities and higher education institutions.

The government's *Cybersafety Plan* supports educators to achieve these outcomes through a range of measures including the *Cybersmart* program run by ACMA. This provides outreach and online professional development programs for teachers, trainee teachers and librarians that focus on strategies to ensure children in particular learn how to participate safely and confidently in the online world.

Online behaviour – the need for a digital social contract?

Although digital technologies and social media are driving positive social change both within Australia and globally, the increasingly networked and interconnected nature of our social interactions is challenging traditional structures that form the basis of civil society. The social contract between governments and citizens which sees citizens abide by laws in return for the security and protection provided by governments, is challenged in the online environment.

Complicating the traditional concept of the social contract is the central role the private sector plays in shaping outcomes in cyberspace and the new types of social interaction the Internet facilitates. For example the Internet provides the capacity to remain anonymous and to connect socially, unhindered by geographic distance.

However, anonymity is not always appropriate when using a financial or government service. For instance, if a person uses online social support services such as Centrelink or lodges a tax return with the Australian Tax Office, it is a requirement to be identifiable. Conversely, as more services are offered online, anonymity may be reasonably expected in those situations where

an online identity is not required. This means where sensitive or private information is stored or transmitted electronically, citizens will expect it to be appropriately secured by the parties involved.

These challenges highlight that we as a society are yet to develop an agreed view on the appropriate balance between the type of behaviour possible online and the negative effects this can have on the civility of online social interactions.

Safety – protecting young people online

The online environment has in some cases disconnected people from responsibility for their words and actions. Similarly, the near ubiquity of personal and mobile computing has broken down traditional safe havens such as the home, increasing the reach and potential impact of negative and abusive behaviour such as bullying and harassment.

The phenomenon of cyberbullying is a growing concern for students, parents, carers and teachers. Unlike traditional bullying, cyberbullying can penetrate the boundaries of the home and reach a far broader audience. As the message is usually delivered by text, it can be read over and over by the target. These factors can exacerbate victims' feelings of isolation, embarrassment and intimidation. Parents face unique challenges in protecting children from this form of bullying, as the implications of new technologies and online applications require new knowledge and responses.

A March 2011 IRIS Research report found cyberbullying was the most reported cybersafety incident in Australian schools (nearly 40 per cent of all incidents) [IRIS: 2011]. Australian Government research *Australian Covert Bullying Prevalence Study*, found that in 2009 more than 10 per cent of secondary school students had experienced some form of cyberbullying [DEEWR: 2009].

Student resilience, wellbeing and safety are essential for academic and social development. Australian students should be able to learn and develop in safe, supportive and respectful environments. Australian schools, families and communities all have a responsibility to provide safe online environments and teach children how to use technology in positive and productive ways.

A range of Commonwealth, state and territory agencies have invested substantial effort in combating online risks for children. This includes measures provided as part of the 2008 *Cybersafety Plan* such as the ACMA's national education and awareness raising programs for students, resources such as the Cybersmart and Stay Smart Online websites and consultation mechanisms to ensure young people, parents and teachers are directly involved in the design and development of cybersafety resources.

Yet no one would declare the problem solved.

An unfettered domain

Most social media sites are privately owned and operated and are often based in overseas jurisdictions which may be beyond the reach of Australian law. This challenges the ability of the Commonwealth and state and territory governments to regulate behaviour on these sites.

In addition, the main penalty used by companies to enforce their terms of service is to deny access to their site, either temporarily or permanently. Reputable operators of social media

usually enforce their terms of service, tend to cooperate with law enforcement and provide safety advice to their users. But some popular sites still have lax rules and enforcement for their user base. These 'safe havens' can be used to harass, bully, mislead or distribute offensive material to Australians.

Privacy and identity security

How we think about the online environment has clear implications for our understanding of the levels of privacy we are afforded when online. Many of us consider that because we might use an Internet-connected device in the privacy of our own home, then we are also afforded that same privacy online. However, in reality any information stored on an Internet-connected system is vulnerable to a broad range of malicious parties including cyber criminals.

Further, the storage of citizens' private information is now often outsourced to third parties by traditional holders of information, such as doctors' surgeries and banks. Consequently, the confidentiality of an individual's information is contingent not only on the security practices of the individual, but also on the security practices and awareness of the institutions holding their data. This further highlights the shared responsibility governments, businesses, NFPs and individuals have in ensuring a secure and trusted online environment.

In an era where our online identity is central to accessing information and services, ensuring the integrity of that identity is increasingly important. The loss or compromise of our online identity can have wide-ranging implications, including financial loss, emotional distress and reputational damage.

What does it mean to be a digital citizen?

To respond to these challenges, we need to consider what it means to be a digital citizen, or at least how the online environment is impacting upon our conventional understanding of citizenship and the social contract. Our online interactions are challenging traditional notions of privacy, identity and social responsibility. We may therefore need to consider a broadened or updated social contract that takes account of the growing part of our civic experience that occurs online.

In doing so, there would be value in revisiting the distribution of responsibility among individuals, businesses and governments in ensuring social cohesion and social inclusion. Developing a common understanding of a model of accountable and responsible digital citizenship – a digital social contract – may need to be part of the debate about Australia's digital future.

Key issues and questions

***Issue**: A growing portion of our lives and civic experience is conducted in the online environment. This environment has a unique set of characteristics, including anonymity, and allows people to interact socially unhindered by geographic distance.*

- **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?

***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?

***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?

***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?

***Issue**: Social networking sites and increased social connectivity provide increased opportunities for people to collaborate, share ideas and produce socially valuable outcomes.*

- **Question:** What new and innovative opportunities do social networking tools provide to improve the social wellbeing of Australians?
- **Question**: How can NFPs ensure the security of online fundraising activities conducted through social networking sites?

***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?

Protecting and promoting Australia's digital economy

Australia's future prosperity is linked increasingly to the confidence and trust businesses and consumers have in our digital economy. According to the Australian Bureau of Statistics (ABS), nearly $143 billion worth of Internet orders were received by Australian businesses in 2009-10 [ABS: 2010], up 15 per cent on the previous year. This steady growth in Australia's digital economy is consistent with global trends. The 2010 *Digital Agenda for Europe* report found that digital technologies were responsible for 50 per cent of the European Union's overall productivity growth [European Commission: 2010]. In the United Kingdom (UK), Internet-driven commerce accounted for 7.2 per cent of GDP in 2009 [Boston Consulting: 2010]. In the United States (US), online retail sales are forecast to reach in excess of $195 billion annually by 2012 [Emarketer: 2010].

Mobile commerce driving digital growth

The growing prevalence of Internet-connected mobile devices, or smartphones, is facilitating rapid increases in e-commerce. The convenience of mobile e-commerce is a primary attraction for consumers. Laura Chambers, senior director of PayPal mobile, recently told an industry conference that purchases made through PayPal using mobile devices went from $US140 million in 2009 to an expected $US2 billion in 2011 and within two years would reach $US7.5 billion. According to Chambers, in Australia PayPal is expecting to see in excess of $120 million of volume over mobile devices in 2011, a tripling from 2010.

The economic benefits of going digital

Digital technologies have the potential to drive productivity growth and transform the Australian economy. For example, research conducted by the Allen Consulting Group has forecast a 10 per cent increase in household Internet connections would increase Australia's GDP by 0.44 per cent. This translates to an estimated $5.6 billion increase in the size of the Australian economy and includes gains to the consumer, investor and government sectors.

The digital economy enables greater opportunities for innovation, as researchers and entrepreneurs are empowered to invest in new and creative research. This innovation leads to new products, more efficient business processes and better ways of interacting with customers and suppliers. Firms will also be able to add greater value to the goods and services they produce, which will continue to create new opportunities for growth and continue to drive productivity growth in the Australian economy.

Greater connectivity has already provided Australian businesses with increased reach, a broadened customer base, more efficient engagement with suppliers and reduced transaction costs. Similarly, the Internet is benefitting consumers by increasing competition, choice, convenience and by providing access to more resources that inform consumer decisions.

According to technology and economic development experts Edward Malecki and Bruno Moriset [Malecki & Moriset: 2008], digital technologies have two core functions in a modern economy: an enabling role in traditional industries, such as simplifying logistics and reducing communications and other transaction costs; and the creation of new industries that are fundamentally based on digital transactions, such as electronic commerce (e-commerce).

The challenge for Commonwealth, state and territory governments, and Australian businesses, is to maintain digital momentum and to encourage and facilitate a deeper and broader

uptake of digital technologies across the economy. Key to this is ensuring Australians maintain trust and confidence when engaging in e-commerce.

Crime online – threatening confidence in the digital economy

The Internet is becoming an integral part of Australians' everyday lives and this is only going to increase with the roll out of the NBN. There are significant benefits to Australia in developing and growing its digital economy. With these benefits also come some challenges. Criminals will look to exploit vulnerabilities for their own financial gain. All sectors of Australian society, including government, businesses, NFPs and individuals are at risk of being victims of cyber crime and scams, which will become increasingly sophisticated and targeted.

The global reach of the Internet has provided criminals with new opportunities to commit 'traditional' crimes (such as fraud) as well as high-tech crimes that did not exist until relatively recently (such as hacking). Cyber crime and other forms of malicious cyber activity represent a serious threat to the long-term prosperity of Australia's digital economy. Cyber crime is a rapidly evolving phenomenon, with the exponential growth in the global digital economy providing enormous incentives to organised criminal groups to develop cyber crime capabilities.

The Sony PlayStation hack

A recent example of the growing scale of cyber criminal activity was the April 2011 breach of Sony PlayStation's accounts database. The breach is the largest known compromise of consumers' personal information. The hackers had access to the personal details of 77 million PlayStation accounts – including 1.5 million accounts belonging to Australians – resulting in a global shutdown of the PlayStation network.

Cyber crime can undermine consumer confidence in e-commerce, with research showing consumers' security concerns are a key impediment to further growth in the digital economy. Consumers are particularly concerned about registering personal details and using credit cards for online transactions, with the 2008-2009 ABS *Household Use of Technology Survey* finding more than one million Australians refrained from purchasing goods or services online due to security or privacy concerns [ABS: 2009].

Similarly, businesses in modern digital economies are increasingly becoming victims of financially motivated cyber crimes. A 2011 UK study estimated cyber crime cost the UK economy about $42 billion a year [Detica: 2011]. Australia faces a similar threat, with the AFP estimating that the overall risk of cyber crime to the Australian economy to be in excess of a billion dollars a year.

Confidence in e-commerce is also impacted by online consumer fraud, including scams purporting to represent genuine opportunities for businesses and consumers. These activities inhibit consumers' confidence to trade online with legitimate businesses and engage with digital technologies generally.

While financial loss is the most obvious impact, other effects can include shame, self-blame and ongoing emotional distress. The 2010 *Norton Cyber Crime Report: The Human Impact* attempts to survey the emotional impacts of cyber crime. The report shows victims' strongest reactions are anger, annoyance and feeling cheated. In many cases, victims blame themselves for being attacked. Many believe 'faceless' criminals are the main perpetrators of cyber crime and nearly 80 per cent of users surveyed do not expect cyber criminals to be brought to justice [Norton: 2010]. As a result, many victims fail to report or work to remedy the damage done.

If online criminal activity goes unchecked, it has the potential to affect public trust and confidence in the Internet generally. In addition to a government role in ensuring an appropriate response to crime, businesses have a commercial interest in protecting themselves and their customers' data.

The government is doing considerable work, through the Standing Council on Law and Justice and the National Cyber Crime Working Group, to develop a national approach to cyber crime. This work includes undertaking a feasibility study on the establishment of a national online reporting facility, developing protocols to improve cooperation between law enforcement agencies on cyber crime investigation and considering the need for a national approach on cyber crime education and prevention strategies. Recognising cyber crime's transnational nature, the government is therefore pursuing its intention, announced in April 2010, to accede to the Council of Europe Convention on Cybercrime. The government aims to be a Party to the Convention by the first quarter of 2012.

The vulnerability of intellectual property

The ABS estimates intellectual property products in Australia are worth $171.5 billion [ABS: 2010]. The loss of intellectual property can lead to a reduced competitive advantage, decreased profits and returns on research and development, and damage to a company's brand and reputation. The systematic and widespread theft of intellectual property can directly reduce a national economy's competitiveness and erode the incentive for innovation.

In 2010 a number of global corporations were the targets of a large-scale and sophisticated cyber crime operation. Among the companies targeted were ICT companies including Google, energy firms and defence contractors. Experts claimed the hackers responsible sought to gain access to the most valuable information stored on these companies' networks, namely their intellectual property.

Consumers, NFPs and small businesses uniquely vulnerable

For a variety of reasons, consumers, NFPs and small businesses tend to acquire and apply fewer ICT security measures, potentially leaving them more vulnerable than government and big business. According to a 2009 survey of Australian consumers by the ACMA, less than 50 per cent of respondents had installed anti-virus software and a smaller proportion of respondents had firewalls or other protective measures on home computers [ACMA: 2009].

Individuals and businesses do not always apply the same caution and judgment to their decisions and actions online as they do in the offline world. A person who has installed a security system and diligently locks the doors

The cost of breaches

According to Symantec's *2010 Annual Study: Australian Cost of A Data Breach* report the average cost of significant data breaches reported by Australian organisations was about $2 million in 2010 [Symantec: 2011].

Scammers exploiting online dating sites

Paul, a retired grazier, recently shared his devastating encounter with scammers with the ACCC's SCAMWatch. Through an online dating website, Paul met someone named 'Selina', from Ghana, and quickly developed a relationship with her. Soon after, a man claiming to be Selina's brother contacted Paul to inform him that Selina had been in a serious accident and needed $1200 to cover medical costs. For several months, scammers continued their contact with Paul, using his relationship with Selina to convince him to help her village. Over time, Paul sent over $200,000 to the scammers, without any of this money reaching the village or 'Selina' [ACCC: 2011].

each day before leaving the house may not take equivalent precautions to protect the information they hold on a computer connected to the Internet. This is likely due to lack of knowledge of cyber risks and how to address them as well as failing to act when risks are known.

Large enterprises do not place the burden of security risk on individual employees. Instead, they employ intrusion detection systems, sophisticated firewalls, chief information officers, chief technology officers and IT security staff. Consumers and many NFPs and small businesses do not have this level of support and may lack the technical skill or interest to better secure their systems. As a result, they are susceptible to scams and having their computers compromised by malicious software. Criminal groups can form networks of compromised computers (called botnets) and use them to commit large-scale crime and scam activities that pose a collective risk to the Australian economy.

Consumers, NFPs and small businesses' low levels of awareness of online threats also make them vulnerable to online scams and frauds. The Australian Competition and Consumer Commission report, *Targeting Scams,* noted reported losses attributable to fraud and scams amounted to $63 million in 2010, with 45 per cent of reported scams occurring online [ACCC: 2011].

Consumer confidence is a critical element of all market economies. Consumers can now distribute their opinions of a business across multiple online forums in real-time and this information is increasingly being used by consumers to determine choice. Increasing consumer adoption of new technologies and the desire to seek out new products and suppliers within and outside of Australia, means a major cyber event would significantly dent consumer confidence in the digital economy.

Local police and consumer protection agencies on the front line

Although most of the world's criminal networks making use of online tools are transnational in nature and rarely based in Australia, state and territory police services and consumer protection agencies are often the primary points of contact for Australians impacted by cyber crimes. Cyber crime provides a unique challenge to local police services and consumer protection agencies, as cyber criminal offences are difficult to investigate and prosecute due to the anonymity afforded by the Internet and the trans-jurisdictional nature of the activities.

The dense and complex interdependencies that underpin the global market economy can enable adaptability and dynamism, but can also produce unexpected and contagious risks. It is therefore essential that trust, confidence and security characterise Australia's digital environment, so as to ensure Australia's digital economy will remain prosperous, innovative and resilient.

Shutting down online cons

Constantine 'Con' Barris, and his company claimed to have a secret method to predict future Powerball draws. A website was set up and thousands of leaflets were distributed promoting these claims and asking for a $59 subscription fee to receive numbers that would win. However, the predicted numbers failed to produce any winnings to subscribers. In 2010, the Federal Court ordered Mr Barris to pay $48,163 in compensation to victims of his scheme [ACCC: 2010].

Key issues and questions

***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 to engage in e-commerce?

***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 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?

***Issue**: Police resources are finite and cyber crime investigations are inherently time and resource intensive. Consequently, the growth in cyber crime 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?

***Issue**: One of the primary impediments to e-commerce is consumers' fear 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?

***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 wellbeing of the Australian community?

***Issue**: The effects of cyber crime 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 cyber crime 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?

***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 transactions 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?

Security and resilience in the online environment

Building confidence in Australia's digital economy and developing a model of responsible digital citizenship are critical elements of Australia's broader societal security and resilience. It is important to recognise that in an era of globalisation and interdependence, our economic and societal security is indivisible from our national security. This interdependence is further amplified by greater connectivity. Those who build cyber tools to exploit individual security lapses for the purposes of cyber crime activities also threaten our broader national security, as the same tools can be used to threaten our national security by targeting critical infrastructures such as power grids, transportation networks and water supplies.

Increased security capabilities and societal resilience

The successful integration of digital technologies into the Australian national security system has enhanced information sharing arrangements both domestically and internationally. It has also improved interoperability and increased the capacity of military, intelligence, and law enforcement officers to collaborate in real-time when managing security challenges. Digital technologies are now central to Australia's modern networked defence capabilities and have greatly enhanced the speed, reach and reliability of the Australian Defence Forces' command, control and communications capabilities while also improving efficiencies in logistics and supply chains.

The dependence on the Internet of other government agencies and the private sector, including critical infrastructure, is also an issue that is addressed through the government's approach to security and resilience online. The cornerstone guidance documents shaping the government's approach are the 2009 *Cyber Security Strategy* and the 2010 *Critical Infrastructure Resilience Strategy*. The aim of the *Cyber Security Strategy* is the maintenance of a secure, resilient and trusted electronic operating environment that supports Australia's national security and maximises the benefits of the digital economy. The *Critical Infrastructure Resilience Strategy* recognises that the security and resilience of Australia's critical infrastructure is inherently linked to cyber security.

Outside of government national security capabilities, the pervasiveness of digital technologies has also produced a growing resilience among citizens when responding to disasters. For example, social networking and media sites were used extensively during the Queensland floods and the Christchurch earthquakes to provide citizens with real-time access to critical resources, such as links to emergency services, news updates, maps of affected areas and information about those who were affected. These resilience-building capabilities are not government-led or even government funded; rather they are non-government sector initiatives enabled by citizens and event responders.

Cyber vulnerabilities and risks

It is, however, important to recognise that reliance on digital technologies also brings a unique set of security challenges. In addition to organised cyber crime operations, which are typically motivated by financial gain, cyber capabilities can be used to facilitate espionage, to support military operations and for more limited purposes that involve disrupting, destroying, degrading or altering information or systems, such as sabotage and deception operations.

The targets of these operations can be diverse and often unpredictable; a piece of information that seems benign to its owner can often be of critical value to another actor. For example, an email about a transport route stored on the systems of an agricultural fertiliser supplier may be of huge value to a terrorist group seeking access to key ingredients for explosives, but would seem routine and unimportant to the email sender and recipients.

Despite the unpredictable nature of cyber operations, a number of targets have enduring value for strategic competitors. These include foreign espionage operations targeting sensitive or classified Australian information stored on government or commercial systems, disruption operations against critical communication nodes and attacks against systems supporting critical national infrastructures, such as water, gas or electricity.

Mitigating the cyber threat

Cyber intrusions against Australian information systems are serious and persistent. Australian Government agencies, in particular, must be prepared for these intrusions so they can develop adequate responses to protect the information that is entrusted to them by the Australian people and our international allies and partners.

Defence's Cyber Security Operations Centre is seeing evidence of sophisticated cyber events on government networks and is developing a better capability to prevent and respond to these threats. The global community continues to experience an increase in cyber intrusions. All systems connected to the Internet are potential targets for hacking and cyber attack. Cyber threats can come from a wide range of sources, including individuals, issue motivated groups, organised criminal syndicates and nation states. The nature of the Internet makes it difficult to attribute intrusions to particular sources, but it is reasonable to assume that information held on Australian networks is attractive to intelligence services of foreign governments and criminal syndicates.

Cyber Security Operations Centre

The Cyber Security Operations Centre (CSOC) was established in the Defence Signals Directorate (DSD) as an initiative of the Australian Government's Defence White Paper to mitigate the cyber threat to Australia's national security. The CSOC identifies, analyses and responds to provide the Australian Government with protection against various cyber threats. The CSOC is a multi-agency body and has embedded representation from a number of Defence and other government agencies.

Key issues and questions

***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?

International partnerships and Internet governance

Australia cannot develop a secure and safe digital environment alone. The online environment is global in nature and, importantly, is almost entirely hosted and facilitated by businesses and private citizens. Further, in an era of cloud computing, a growing proportion of Australians' information and online services will be stored in and delivered from offshore locations. Consequently, efforts to optimise Australia's digital future must include both a series of long-term strategic partnerships with other nations, the private sector, international organisations, key transnational commercial organisations and concerted and meaningful engagement with the institutions of Internet governance.

A new paradigm of partnerships

As the Internet increasingly shapes the prosperity and wellbeing of a growing number of people, there is an expectation that governments consider their responsibility to protect and promote their citizens' online interests.

This is a new and complex task and it is challenging for governments to keep pace with the rapid changes occurring in the digital environment.

As discussed in *The Shift* by Allison Cerra and Christina James, "Governments are in an interesting predicament. On the one hand, they must respond to an increasingly collaborative constituent base and embrace transparency in communications. On the other, they must protect information central to our nation's and their citizens' security". Consequently, the institutions and instruments of the state are not always going to provide the complete solution, nor should they necessarily do so. There may be a need to explore a new set of partnerships designed to further build trust among governments and private actors.

What is cloud computing?

Cloud computing is an information and communications technology providing convenient access to a shared pool of computer resources including, but not limited to, digital networks; computer servers and storage; software and associated services. These resources can be accessed anywhere through a network connection, such as the Internet. This technology allows access to high-powered computing and services that may otherwise be unaffordable for individuals, businesses and governments.

These partnerships will need to be global in nature and underpinned by a shared vision of an open, trusted, safe and secure digital environment. Future developments in the underlying characteristics of the Internet are likely to be shaped and influenced by the interests of citizens, businesses and governments globally. Domestically, societies will need to determine the appropriate balance between security and openness. At an international level, stakeholders will have to cooperate and collaborate to shape the underlying characteristics of the Internet in ways that reflect this balance.

Internet governance – the future of the digital environment

Governments and businesses will need to be aware of the impact their efforts to achieve a safe and secure digital environment are likely to have on the Internet's underlying principles. As an open, decentralised and universally available space, the Internet in its current form is an enabler of innovation and creative and positive social action. Although it is inevitable that over time commercial, societal and political pressures will have some impact on the underlying characteristics of the Internet, liberal democracies like Australia benefit most

from an open online environment. Balancing our social, economic and security needs will be central to determining a vision for the online environment which best advances the interests of Australia and its people.

International norms of behaviour in cyberspace

International norms on cyberspace are developing rapidly in a variety of fora – in relation to cyber security, international trade, intellectual property and Internet governance.

It is essential that Australia engages actively in all relevant fora – to ensure our interests and values are reflected in the emerging international norms on cyberspace. In doing so we need to ensure Australians can take full advantage of the opportunities the digital economy offers.

Perhaps the greatest threat to an open, trusted, safe and secure digital environment is competition and conflict in cyberspace between nations. To avoid this, understandings among states governing responsible online behaviour may need to be developed.

Although there are legal principles that apply to some aspects of cyber activity, the online environment is not currently governed by an existing holistic international legal framework. There is a clear need for the international community to address what norms or "rules of the road" are needed for the online environment.

Cooperating with partners

The Australian Government will continue to engage and strengthen cooperation with other countries, including using important forums such as the Australia–United Kingdom Ministerial (AUKMIN) and the Australia–United States Ministerial (AUSMIN) meetings to further collaboration and ensure the best possible defence against cyber threats. This will position us to better act, in, and through, cyberspace in support of our national interests.

Key issues and questions

***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?

***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 different stakeholders are likely to want different outcomes from any agreement.*

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

Investing in Australia's digital future

Optimising the social and economic outcomes of any technological capability is fundamentally reliant on the humans using the technology. A strategic blueprint designed to optimise Australia's digital future must therefore consider how to ensure a long-term investment in the human capital required to drive the digital economy. In addition to specialised expertise, we need a population with strong digital skills with an awareness of the opportunities and risks of digital technologies.

As the NBN rolls out and Australia's digital economy continues to grow, a domestic workforce will be needed to maintain the digital infrastructure on which Australians rely. In particular, ICT security specialists will be critical to protecting Australia's digital infrastructure.

Growing demand for digital skills

According to a 2010 environment scan conducted by *Innovation and Business Skills Australia*, 60 per cent of Australia's ICT industry faces difficulties finding applicants with the right mix and level of skills. Demand for ICT skills is expected to increase more than 25 per cent a year to 2013 [IBSA: 2010]. Anticipated demand for technical skills will be even greater to support next generation technology developments.

In managing this growing demand for digital skills it is important that Commonwealth, state and territory governments and the private sector coordinate and prioritise skill sets critical to delivering the services and capabilities which will meet Australia's core digital needs. A key element of this should include the need to grow our cyber security skills base to meet the growing sophistication and scale of the cyber crime threat posed to Australian businesses and consumers.

A digitally literate nation

To complement a core of technically proficient ICT professionals, developing a high level of digital literacy among all Australians would both improve the nation's capacity to take full advantage of the opportunities available in the online environment and heighten awareness of the potential risks associated with operating in cyberspace.

The *Digital Education Revolution* will play a key part in building the digital literacy of young Australians, but improving older Australians' digital literacy will be important in ensuring that they too can take advantage of the opportunities of the digital age. The government's *Broadband for Seniors* program has taken important steps to improving older Australians' access to high-speed Internet services through the establishment of broadband kiosks. As the NBN rolls out and seniors have access to high-speed Internet in their homes, we will need to consider how older Australians can take full advantage of this service and are aware of and can implement the steps required to mitigate cyber risks.

Similarly, disadvantaged, disabled and vulnerable Australians are often unaware or unable to take advantage of the opportunities digital technologies provide and can be the most susceptible to online scams and other cyber crimes. Ensuring all sections of Australian society are aware of the benefits and risks inherent in the digital age will require a whole of community approach. Responsibility for this awareness raising effort must be shared by industry, governments and community groups.

An important measure to ensure all sections of Australian society are digitally literate is the government's *Digital Communities* initiative, as outlined in the *National Digital Economy Strategy*. A focus of the initiative will be to establish 'Digital Hubs' in communities, where local residents will be able to experience the NBN and receive training to develop the digital skills necessary to participate safely and securely, and have trust and confidence in the digital economy.

More broadly, the government will need to consider how to ensure all Australians can take full advantage of the opportunities the NBN presents. Taking advantage of established learning opportunities of all types, both formal and informal, can support all Australians to learn about and develop the skills required to safely and securely engage with new and emerging technologies. Learning opportunities that go beyond age and socio-economic status and focus on key learning attributes will support all Australians to engage with the digital age.

Attracting international investment

With the combination of next-generation digital infrastructure provided by the NBN, a technically proficient workforce and a technically savvy population, Australia will have in place the elements to emerge as a key hub in the global digital economy. Normalising and mainstreaming cyber security and cyber safety issues will give Australia a distinct comparative advantage over less mature digital economies, particularly in the context of increasingly sophisticated and pervasive cyber crime activity.

As the global digital economy continues to expand, Australia's capacity to emerge as a global leader in digital infrastructure, human capital, and in our approach to cyber security and cyber safety will be critical to ensuring Australia is positioned as a genuine global leader in the digital age.

Key issues and questions

***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?

***Issue**: Australians' level of digital literacy is growing, yet many elderly and vulnerable Australians are unaware of the opportunities and risks inherent in digital technologies.*

- **Question**: How can we ensure all sectors of the Australian community have the necessary skills and security awareness to optimise the benefits of the digital economy?

***Issue**: Being viewed as a world leading digital economy in the way that Singapore is in our region, is critical to attracting overseas investment, both in our ICT sector and more broadly because of the enabling role of digital technologies.*

- **Question**: Besides rolling out the NBN, what role does the government have in promoting opportunities for individuals and businesses to compete in the global information communications technology marketplace and to increase the attractiveness of Australia as a destination for digital investment?

References

Access Economics, *Household E-Commerce Activity and Trends in Australia*, 2010, http://www.accesseconomics.com.au/publicationsreports/getreport.php?report=254&id=323, viewed 28 July 2011.

The Allen Consulting Group, *Quantifying the possible economic gains of getting more Australian households online*, 2010, http://www.dbcde.gov.au/__data/assets/pdf_file/0004/135508/Quantifying_the_possible_economic_gains_of_getting_more_Australian_households_online.pdf, viewed 28 July 2011.

Attorney-General's Department (AGD), *Cyber Security Strategy*, 2009, http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(4CA02151F94FFB778ADAEC2E6EA8653D)~AG+Cyber+Security+Strategy+-+for+website.pdf/$file/AG+Cyber+Security+Strategy+-+for+website.pdf, viewed 28 July 2011.

Attorney-General's Department (AGD), *Critical Infrastructure Resilience Strategy*, 2010, http://ag.gov.au/www/agd/rwpattach.nsf/VAP/(9A5D88DBA63D32A661E6369859739356)~Australian+Government+s+Critical+Infrastructure+Resilience+Strategy.PDF/$file/Australian+Government+s+Critical+Infrastructure+Resilience+Strategy.PDF, viewed 28 July 2011.

Australian Bureau of Statistics (ABS), *Australian System of National Accounts*, 2010, http://www.ausstats.abs.gov.au/Ausstats/subscriber.nsf/0/556894E44C26469ECA2577CA00139858/$File/52040_2009-10.pdf, viewed 28 July 2011.

Australian Bureau of Statistics (ABS), *Household use of information technology*, 2009, http://www.ausstats.abs.gov.au/ausstats/subscriber.nsf/0/9B44779BD8AF6A9CCA25768D0021EEC3/$File/81460_2008-09.pdf, viewed 28 July 2011.

Australian Bureau of Statistics (ABS), *Internet Activity, Australia, December 2010*, http://www.abs.gov.au/AUSSTATS/abs@.nsf/DetailsPage/8153.0Dec%202010?OpenDocument, viewed 28 July 2011.

Australian Communications and Media Authority (ACMA), *Australia in the Digital Economy – Report 1: Trust and Confidence*, 2009, http://www.acma.gov.au/webwr/aba/about/recruitment/trust_and_confidence_aust_in_digital_economy.pdf, viewed 28 July 2011.

Australian Communications and Media Authority (ACMA), *Click and Connect: Young Australians' use of online social media*, 2009, http://www.acma.gov.au/WEB/STANDARD/pc=PC_311797, viewed 28 July 2011.

Australian Communications and Media Authority (ACMA), *Online risk and safety in the digital economy*, 2010, http://www.acma.gov.au/webwr/_assets/main/lib310554/online%20risk_safety_report_2010.pdf, viewed 28 July 2011.

Australian Communications and Media Authority (ACMA), *The internet service market and Australians in the online environment*, 2011, http://www.acma.gov.au/webwr/_assets/main/lib310665/the_internet_service_market_in_australia.pdf, viewed 28 July 2011.

Australian Competition and Consumer Commission (ACCC), *Targeting Scams: Report of the ACCC on scam activity 2010,* http://www.accc.gov.au/content/index.phtml/itemId/972476, viewed 28 July 2011.

Australian Competition and Consumer Commission (ACCC), *SCAMWatch – How online romances cost Melba and Paul more than their hearts.* http://www.scamwatch.gov.au/content/index.phtml/itemId/780314, viewed 28 July 2011.

Australian Competition and Consumer Commission (ACCC), *SCAMWatch – ACCC brings Powerball 'bogus' to halt,* http://www.accc.gov.au/content/index.phtml/itemId/925068/fromItemId/927069, viewed 28 July 2011.

Australian Government Information Management Office (AGIMO), *Interacting with Government,* 2009, http://www.finance.gov.au/publications/interacting-with-government-2009/docs/interacting-with-government-2009.pdf, viewed 28 July 2011.

The Boston Consulting Group, *Connected Kingdom,* 2010, http://www.connectedkingdom.co.uk/downloads/bcg-the-connected-kingdom-oct-10.pdf, viewed 28 July 2011.

Cerra A. & James C., 2011, *The Shift*, Alcatel-Lucent, page 212. http://www.theshiftonline.com

Consumer Reports, *Social Insecurity – what millions of online users don't know can hurt them*, 2010, http://www.consumerreports.org/cro/magazine-archive/2010/june/electronics-computers/social-insecurity/overview/index.htm, viewed 28 July 2011.

Department of Broadband, Communications and the Digital Economy (DBCDE), *Cyber Safety Plan,* 2008, http://www.dbcde.gov.au/online_safety_and_security/cybersafety_plan, viewed 8 June 2011.

Department of Broadband, Communications and the Digital Economy (DBCDE), *Digital Economy Strategy,* 2011, http://www.nbn.gov.au/wp-content/uploads/2011/05/National_Digital_Economy_Strategy.pdf, viewed 28 July 2011.

Department of Education, Employment and Workplace Relations (DEEWR), *Australian Covert Bullying Prevalence Study,* 2009 http://www.deewr.gov.au/Schooling/NationalSafeSchools/Documents/covertBullyReports/Exec_20summary.pdf, viewed 28 July 2011.

Department of Education, Employment and Workplace Relations (DEEWR), *Digital Education Revolution,* http://www.deewr.gov.au/Schooling/DigitalEducationRevolution/Pages/default.aspx, viewed 28 July 2011.

Department of Broadband, Communications and the Digital Economy (DBCDE), *Digital Enterprise Program,* 2011, http://www.dbcde.gov.au/digital_economy/programs_and_initiatives/digital_enterprise_program, viewed 28 July 2011.

Department of Broadband, Communications and the Digital Economy (DBCDE), *Digital Regions Initiative,* 2009, http://www.dbcde.gov.au/funding_and_programs/digital_regions_initiative, viewed 28 July 2011.

Department of Families, Housing, Community Services and Indigenous Affairs (FAHCSIA), *Broadband for Seniors,* 2008, http://www.fahcsia.gov.au/sa/seniors/pubs/Broadbandprogguide/Documents/BroadbandSeniorsProgramGuidelines.pdf, viewed 28 July 2011.

Department of Health and Ageing (DHA), *National E-Health Strategy,* 2008, http://www.health.gov.au/Internet/main/publishing.nsf/content/604CF066BE48789DCA25751D000C15C7/$File/National%20eHealth%20Strategy%20final.pdf, viewed 28 July 2011.

Detica, *The Cost of Cyber Crime*, 2011, http://www.detica.com/uploads/resources/THE_COST_OF_CYBER_CRIME_SUMMARY_FINAL_14_February_2011.pdf, viewed 28 July 2011.

Edith Cowan University, *Australian Covert Bullying Prevalence Study*, Child Health Promotion Research Centre, March 2009.

Emarketer.com, *US Retail Ecommerce Forecast*, 2011, http://www.emarketer.com/Reports/All/Emarketer_2000770.aspx, viewed 28 July 2011.

European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – A Digital Agenda for Europe*, 2010, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF, viewed 28 July 2011.

Healey S, *Submission to the Joint Select Committee on Cyber-Safety: The Human Faces Behind Cyberbullying Offences an Australian Case Study when "Using a carriage service to menace, harass or cause offence",* 2011, http://www.aph.gov.au/house/committee/jscc/subs/sub_136.3.pdf, viewed 28 July 2011.

Innovation and Business Skills Australia (IBSA), *Environment Scan – 2010 Information and Communications Technologies Industries,* 2010, http://www.ibsa.org.au/Portals/ibsa.org.au/docs/Research%20&%20Discussion%20Papers/Sectoral%20report%20-%20ICT%20Industry%2026%20Feb%2010.pdf, viewed 28 July 2011.

IRIS Research, *Australian Children's Cyber-safety and E-Security,* 2011, http://www.dbcde.gov.au/__data/assets/word_doc/0004/135562/Australian_Childrens_Cyber-safety_and_E-Security_Projectreport_on_the_results_of_a_teachers_survey.docx, viewed 28 July 2011.

Malecki E. & Moriset B., *The Digital economy: business organization, production process and regional development*, 2008, Routledge, New York.

Near Field Communications/Smart mCommerce, *Paypal's Mobile Plans POS payments this year and $7.5 Billion in volume by 2013,* 2011, http://nfcdata.com/blog/2011/05/24/paypal%E2%80%99s-mobile-plans-pos-payments-this-year-and-7-5-billion-in-volume-by-2013/, viewed 28 July 2011.

The Nielsen Company, *State of the Online Market*, 2011, http://au.nielsen.com/site/documents/AustralianOnlineConsumersReportMediaRelease.pdf, viewed 28 July 2011.

Norton, *2010 Cyber crime Report: The Human Impact,* 2010, http://us.norton.com/theme.jsp?themeid=cyber crime_report, viewed 28 July 2011.

Sydney Morning Herald, *PlayStation privacy breach: 77 million customer accounts exposed*, 2011, http://www.smh.com.au/digital-life/games/playstation-privacy-breach-77-million-customer-accounts-exposed-20110427-1dvhf.html, viewed 28 July 2011.

Symantec, *Cost of a Data Breach & Encryption Trends Study*, presentation by Craig Scroggie, Vice President and Managing Director, Pacific region, Symantec, May 12, 2011

Senator John Faulkner, *Opening of the Cyber Security Operations Centre,* 15 January 2010, http://www.defence.gov.au/minister/FaulknerTranscripttpl.cfm?CurrentId=9885, viewed 28 July 2011.

Wikipedia, *Wikipedia,* 2011, http://en.wikipedia.org/wiki/Wikipedia, viewed 28 July 2011.

Wired, *Google Hack attack was ultra sophisticated, new details show*, 2010, http://www.wired.com/threatlevel/2010/01/operation-aurora/, viewed 28 July 2011.

Glossary

Bot	A single compromised computer, sometimes called a zombie.
Botnet	A network of compromised computers, sometimes called a zombie army.
Cloud Computing	An information and communications technology providing convenient access to a shared pool of computer resources including, but not limited to, digital networks; computer servers and storage; software and associated services. These resources can be accessed anywhere through a network connection, such as the Internet.
Cyber bullying	Cyber bullying involves the use of information and communication technologies to support deliberate, repeated, and hostile behaviour by an individual or group, which is intended to harm others.
Cyber crime	Encompassing two categories of criminal behaviour: crimes directed at computing and telecommunications technologies (such as hacking, or denial of service attacks), and crimes where the Internet or information and communications technology is integral to the commission of the offence (such as online fraud, online child exploitation and online intellectual property infringement).
Cyber safety	Refers to a range of measures designed to: • help protect Australian families, particularly children, from online risks including cyber bullying, sexual grooming, exposure to offensive content, breaches of privacy and identity theft; • educate and promote the safe and responsible use of the Internet and all Internet enabled devices, including mobile phones; and • promote positive and responsible online behaviour as key principles for building good digital citizenship.
Cyber security	Measures relating to the confidentiality, availability and integrity of information that is processed, stored and communicated by electronic or similar means.
Cyberspace	The simplest definition of cyberspace is the 'Internet and anything connected to it'. For the purpose of the discussion paper, non-Internet connected systems, such as supervisory control and data acquisition (SCADA) and industrial control systems are also considered part of cyberspace. There are two largely complementary aspects of cyberspace: • first, cyberspace is a medium where things happen - a technological construct which supports a range of online interactions, such as social networking, online banking and gaming; and

	• second, cyberspace is also a medium through which things happen - a global conduit between private enclaves ranging from home computers to industrial control systems. It is most useful to think of cyberspace as a virtual manifestation of 'real life', which coexists in parallel with the physical world.
Digital Age	Also known as the computer age or the information age, is the concept that a key aspect of our current era is that digital technologies have greatly improved our ability to transfer and access information instantly and freely.
Digital Economy	The global network of economic and social activities that are enabled by information and communications technologies, such as the Internet, mobile and sensor networks.
E-commerce	A contraction of electronic commerce, which refers to business-to-business and business-to-consumer transactions occurring over open networks, such as the Internet.
Firewall	A device or application that protects a computer network from unauthorised access – it may be hardware, software or a combination.
Identity Security	The security of who a person is, or the evidence a person uses to prove who they are. Identity Security is a balancing act between three drivers: • confidentiality and privacy – protecting an individual's evidence of identity from being compromised (stolen, duplicated, misused etc); • integrity – maintaining the integrity or correctness of an individual's identity information; and • availability – maintaining access to the identity information to those who should have access.
Internet	The global system of interconnected computer networks.
ISP	Internet Service Provider, which is a company that you pay to provide you with access to the Internet.
Malware	Short for malicious software and is a generic term for software that is designed to specifically damage, disrupt or take control of systems.
Phishing	A type of scam, generally sent by email that will direct you to a website that looks like the real website of a retailer or financial institution. The website is designed to encourage you to reveal financial details, 'phishing' for information such as your credit card numbers, account names, passwords, and other personal information.
Privacy	The right or interest of a person in sheltering his or her life from arbitrary or unwanted interference or public scrutiny. 'Privacy', especially in a cyber security context, typically refers to being able to protect one's personal information from access, use, disclosure, copying or modification by other persons who are not authorised to do so.

Smart Phone	A mobile phone that has advanced capabilities such as being able to access the Internet.
Social Contract	The philosophical and political concept that citizens abide by laws in return for the security and protection provided by governments.
Software	A general term for various kinds of programs used to operate computers and related devices.
Spam	Unsolicited electronic messages.
Teleconference	The live transmission of audio and video information and data between various locations by ICT.
Telemedicine	An application of clinical medicine where information is transmitted, and consultations are facilitated by ICT.
Virus	A type of malware that attaches itself to a program or file, which is how it spreads from one computer to another. It can be spread by human action, such as sharing infected files or sending emails with viruses as attachments.
White Paper	An authoritative report or guide on a particular theme or problem that identifies issues of strategic importance, articulates objectives and details how to achieve those objectives.

Notes