AMTA

Australian Mobile
Telecommunications
Association

Department of Prime Minister and Cabinet

A public discussion paper:

Connecting with Confidence

AMTA Submission – November 2011

Introduction

The Australian Mobile Telecommunications Association (**AMTA**) is the peak industry body representing Australia's mobile telecommunications industry. Its mission is to promote an environmentally, socially and economically responsible, successful and sustainable mobile telecommunications industry in Australia, with members including the mobile Carriage Service Providers (CSPs), handset manufacturers, network equipment suppliers, retail outlets and other suppliers to the industry. For more details about AMTA, see http://www.amta.org.au.

The rapid advances in mobile technology supported by product and service innovation and, most recently, convergence with other media, particularly the internet, have further confirmed mobile telecommunications as a central part of everyday life. Keeping pace with evolving mobile technologies and services and the implications for safety and security in cyberspace is a significant policy challenge.

AMTA's Cybersafety Program

In terms of cybersafety, AMTA believes that education for parents, carers, teachers, children and young people is the best means of ensuring the protection of our children and young people. Software based filtering programs, industry codes of practice and network blocks are all tools that are available to parents and carers for managing and monitoring their child's online safety. AMTA, however, maintains that the best protection for children, adults and parents alike is being well-informed. It is particularly important for parents and other carers to seek to provide adequate supervision of children's use of mobile phones as well as computers and other devices capable of accessing the on-line environment.

AMTA made a submission (117) to the Joint Select Committee's Inquiry on Cyber Safety in July 2010. Our submission provided background to the recent growth, development and impacts of mobile telecommunications, and also made specific comments regarding cyber safety, including mobile industry initiatives and perspectives.

AMTA understands the concerns of Australian parents, carers and children themselves and has undertaken several information initiatives in the area of cybersafety.

AMTA's website contains information and fact sheets on the topic of cybersafety and also includes a link to the ACMA's Cybersmart website which is a valuable resource. AMTA is currently updating its website information to better reflect the rapid adoption of new technologies such as smartphones as well as new social networking platforms that are increasingly popular. AMTA's website includes tips relating to cyberbullying for parents and carers as well as teens. It also includes important consumer information relating to location based services which are also pertinent to personal safety issues for young people as well as adults.

AMTA is also a member of the Consultative Working Group on Cyber Safety. The group is a key initiative of the Australian Government's cyber safety plan. It has the important role of providing advice to the Australian Government on measures to protect Australian children from cybersafety risks including cyberbullying, exposure to illegal content and privacy breaches.

AMTA has also formed partnerships with the Australian Council of State School Organisations (ACSSO), the peak council of government school parents and citizens and school community governing bodies, and the Alannah and Madeline Foundation, a national charity keeping children safe from violence.

AMTA's highly successful Mobile Muster program (an industry funded recycling program for mobiles) partnered with the Alannah and Madeline Foundation in a campaign run throughout the first half of 2011. The Alannah and Madeline Foundation's eSmart initiative is a world-first system that helps schools deal with the serious issues of bullying, cyberbullying, cybersafety, and equips students with the skills and knowledge they need for smart, safe and responsible use of technology. There are currently over 380 Australian schools that are participants in AMTA's Mobile Muster program.

Cybercrime and Cyber security

AMTA responded to the Department of the Attorney-General's study into protecting consumers, businesses and the community from cybercrime and provided answers to the study questionnaire in February 2011.

AMTA has generally supported the Government's policy to accede to the Council of Europe's Convention on Cybercrime. AMTA's members support the Government's intention to accede to the Convention but have expressed strong concerns about some of the proposed legislative amendments relating to the timeframes for implementing compliance.

AMTA participates in industry forums that track and disseminate information relating to cybercrime, such as, the ACMA's Communications and Security Enforcement Roundtable (CSER) that provides a liaison between Australian law enforcement and security agencies and the telecommunications industry. Similarly, as an industry organisation, it is part of AMTA's role to stay abreast of a regulatory policy and industry issues and facilitate the exchange of information between industry members.

AMTA's website includes a detailed consumer tips section that covers issues relating to mobile phone viruses, scam and spam messages, location based services as well as general security tips to prevent loss or theft, such as using PIN codes to secure a mobile phone and SIM.

AMTA runs a world-leading anti-theft program at no cost to consumers. It works by detecting a mobile phone's electronic serial number, known as the International Mobile Equipment Identity (IMEI) number, then sharing this information with carriers to block handsets across all networks in Australia. Consumers contact their mobile service provider to request that their phone be blocked or unblocked. Approximately 150 000 IMEIs are blocked every year on the AMTA Lost and Stolen database, with around 50 000 later being unblocked at the owners request.

It should be noted that the loss or theft of a mobile handset can mean significant financial and personal loss for the mobile user. Not only is the value of the handset lost, but the user can have ongoing liabilities under a mobile phone contract. Australians have been quick to adopt smartphones. With over 37% of Australians now owning a smartphone the potential loss involved in losing a handset are magnified.[1] With a smartphone they may also lose

[1] "Australia's White Hot Smartphone Revolution" SMH 8 Sept 2011 by Asher Moses.

valuable personal or business data (including photos, videos, social networking account, financial and banking information) that was stored on the handset if they have not secured it with a PIN.

AMTA's MobileMuster program recently conducted some research to determine whether concerns about data stored on smartphones prevents people from recycling their mobiles. The research found that 47% of those surveyed store work emails on their mobiles, 28% store passwords and 15% store bank details.[2]

AMTA welcomes the opportunity to participate in the discussion surrounding the release of Australia's first Cyber White Paper and has provided answers to selected questions from the *Connecting with Confidence* discussion paper below.

Digital Citizenship in a Networked Society

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.

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?

Recognising that a concept of digital citizenship is fairly new to the Australian public, AMTA suggests that initiatives such as the ACMA's Cybersmart program provide a foundation of public awareness building on which to build a concept of digital citizenship. School programs and curriculums are also clearly vital in ensuring that the concept of digital citizenship is firmly established in the minds of young Australians. Digital Education Revolution will clearly pay a key role in implementing curriculum based programs in schools across Australia.

To promote the concept of digitial citizenship beyond the school system would require an overall education campaign across Australia. AMTA suggests that any such campaign should build upon and draw together current government initiatives such as the ACMA's Cybersmart and DBCDE's Stay Smart Online. The ACCC's Scam Watch is another important resource in this area.

As part of its own cybersafey program and outreach to schools, AMTA has formed partnerships with the Australian Council of State School Organisations (ACSSO), the peak council of government school parents and citizens and school community governing bodies, and the Alannah and Madeline Foundation, a national charity keeping children safe from violence.

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.

[2] http://www.mobilemuster.com.au/articles/Australians.want.to.recycle.their.old.mobiles.but.worry.about.protecting.their.data

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?

AMTA suggests that governments have a primary role to play in ensuring that such offensive behaviour is made illegal where necessary (if not already covered by legislation) or otherwise discouraged by public policy. The mobile telecommunications sector has a role in co-operating with law enforcement agencies as clearly set out in the relevant legislative requirements and obligations that exist.

AMTA suggests that closer consultation between government and industry at the policy-making, rather than implementation, stage will help industry and government to work together to prevent malicious online behaviour. For example, AMTA suggests that while there have been government reviews announced that touch on cybercrime and cyber security issues there are yet to be any outcomes from these processes. For example**,** the Council of Australian Governments review of the 2005 counter-terrorism legislation was due to begin in Dec 2010. This was originally announced 27 Sept 2005 with the review date of December 2010 (announced COAG dated 10.2.06) but has yet to commence. Similarly, the Independent Review of the Intelligence Community 2011 has not released any recommendations despite the final report being filed with the Department of Prime Minister and Cabinet in July 2011.

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.

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

AMTA believes that education is the best means of empowering parents and carers with the appropriate tools to protect children and young people online. Schools and educational institutions provide an excellent network for disseminating information to parents and carers.

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

As per the answer above, AMTA has partnered with ACSSO and the Alannah and Madeline Foundation as part of an outreach program to schools. There are currently over 380 Australian schools that are participants in AMTA's Mobile Muster program (which partnered with the Alannah and Madeline Foundation during the first half of 2011 for a joint campaign).

The Alannah and Madeline Foundation's eSmart initiative is a world-first system that helps schools deal with the serious issues of bullying, cyberbullying, cybersafety, and equips students with the skills and knowledge they need for smart, safe and responsible use of technology.

Education programs such as these are an effective means of promoting social responsibility and encouragement to young people who may be affected by cyberbullying.

The ACMA's Cybersmart progam is an example of an effective outreach program to schools and AMTA suggests that it should provide the foundation for any further government initiatives regarding cyberbullying and young people.

Protecting and Promoting Australia's Digital Economy

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.

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

Promotion of commercial online opportunities must be coupled with awareness campaigns about the potential risks involved. AMTA suggests industry organisations and bodies are well placed to distribute information and run awareness programs relating to online commerce as well as the risks involved.

AMTA suggests that the online world is a global world and government and industry must therefore also have regard to international developments – both in terms of opportunities and threats. Any co-ordinated and integrated regulatory framework for cyber issues must also incorporate the sharing of information with other countries and global corporations. The Digital Economy is a world-wide economy.

How can governments, industry, NFPs and consumer groups boost consumers' confidence to engage in e-commerce?

AMTA suggests that consumers' confidence will build as their experience with e-commerce grows. It is necessary that Government, industry and consumer groups all work closely together to ensure that the appropriate consumer safeguards are considered and put into place as new products or services are launched.

AMTA suggests that industry associations, such as AMTA and Communications Alliance can play a key role in the mobile telecommunications industry in ensuring that this happens. For example, Communications Alliance currently has an industry working group that is investigating potential regulatory issues and consumer concerns surrounding mobile commerce and potential mobile payments models.

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.

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?

As stated above, AMTA believes that consumer confidence will develop with experience. Industry and Government need to work closely together to ensure that awareness of cyber threats is promoted and maintained. AMTA suggests that industry organisations such as AMTA or the IIA (Internet Association of Australia) are well placed to promote such awareness amongst consumers and also industry members.

To achieve higher levels of small business awareness of potential cyber threats would require a targeted and well-co-ordinated education campaign by government.

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

AMTA suggests that having an online reporting mechanism is important and that a "one-stop shop*"* may also potentially improve reporting levels. As suggested in the two concept papers:

- *Integrated Awareness-Raising and Educational Initiatives for Cyber Issues*
- *Establishing a Central Referral and Support Service for Cyber Issues*

an integrated and centralised referral and support service for all cyber issues is a concept worth exploring further.

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?

AMTA suggests that an industry code of practice (for example, the ePayments code administered by ASIC) could possibly provide a framework for such sharing of experiences between online traders.

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.

What options are there for increasing consumers' trust in conducting business online?

As per the answer above, experience will bring greater consumer confidence. Industry codes of practice and a strong self-regulatory framework can also be instrumental in building consumer confidence in online transactions.

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

It is a challenge for industry and Government alike to encourage consumers to take more responsibility to protect their information. Robust systems that require strong passwords and frequent password changes can encourage consumers to take such responsibility.

A more integrated and co-ordinated framework of government initiatives and education programs could deliver better outcomes in terms of consumer education and awareness levels.

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?

Industry's options include education of customers and provision of good customer experiences that will build trust and confidence in the security and privacy of online transactions. Industry Codes can play a key role in establishing and maintaining good business practices that create an environment in which consumers can place their trust and confidence.

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

AMTA suggests that the issue is not about what information consumers need. This is simple technical knowledge that can easily be supplied – for example use PINs on mobiles, install firewalls on PCs. The issue lies in how to deliver the information so that consumers will act upon it. From a consumer perspective there needs to be more widely understood information about where to go to find out about cybersecurity and how to protect themselves from cybercrime. A centralised referral and support service that is clearly branded and marketed to consumers and small business would clearly be helpful here.

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

Consultation between governments and industry needs to be co-ordinated, regular and consistent with regard to cybercrime.

Also, due to the international nature of cybercrime there needs to be co-ordination with foreign governments and law enforcement agencies as well as industry.

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.

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

While the potential impact of a widespread individual security lapse could involve high costs to Australia, AMTA notes that industry and government are both working effectively to achieve improvements to cybersecurity and prevent any such lapses.

Business and industry must be involved in and kept informed of any initiatives to ensure Australia's cybersecurity.

It is also important to have feedback between the agencies receiving and dealing with reports of cybercrime or cybersecurity breaches and those agencies involved in consumer and business education and awareness. This ensures the public and industry receive timely warnings regarding cyber threats. It also allows for cyber threats to be better tracked and understood as the knowledge base is developed.

Security and Resilience in the Online Environment

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.

How can the Commonwealth, states and territories and industry effectively communicate the interdependent nature of individual and national cyber security?

AMTA agrees that an integrated and centralised referral and support service for cyber issues could be more effective in communicating the interdependent nature of individual and national cyber security.

The multiple and sometimes overlapping programs currently in place do create a level of confusion for consumers and businesses alike. Having a single point referral point could also simplify awareness campaigns.

While the “Help” button initiative of the Department of Broadband, Communications and the Digital Economy is valuable it also exists in the context of several similar initiatives. AMTA suggests that the “Help” button could be extended to apply to other platforms and media and used as the basis for promotion of a single referral point for consumers and businesses.

How can the importance of individual behaviour be highlighted in creating a secure, trusted and resilient online environment for all Australians?

This would require a co-ordinated and consistent education campaign across Australia.

Investing in Australia’s Digital Future

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.

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?

AMTA suggests that it should be a priority to expand the workforce which has the cyber security skills to maintain the safety, stability and interoperability of the internet no matter where the workforce is located. The numbers and skill levels of the relevant workforce need to be increased in order to minimise the risks to national, business and personal (online) security and critical infrastructure and commercial business systems. These skills should “*include the skills needed to incorporate cyber security into the industrial control systems used to manage critical infrastructure*”(Cyber Security Two Years Later, A Report of the CSIS Commission on Cybersecurity for the 44th Presidency.)

The Australian governments should also support strategies in conjunction with industry and academia to ensure that there are adequate levels of domestic expertise to develop, operate and maintain the safety (physical and logical), stability and interoperability of the networks

Australia needs to connect to the worldwide internet. For example, submarine cables, broadband capable mobile networks, satellite earth stations, transmission equipment and the infrastructure that is needed to provide power to these technologies.

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.

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?

In some of the responses above AMTA has stressed the importance of education campaigns that focus on schools. It is, of course, important to also target other sectors of the community such as older Australians and those who may be more vulnerable.

As many Government services migrate to online systems for interacting with clients there is opportunity to educate and assist those who use such services as part of the process of migration. The NBN roll-out also provides a unique opportunity to reach out to more Australians who may not have previously had any experience with online transactions and provide online tutorials or education programs.

Some older Australians and some more vulnerable consumers may be overwhelmed by making an online transaction. It is only pragmatic to accept that there will be some people who may either require assistance in their online dealings or need to be provided with other methods to conduct transactions and this should not be forgotten as more services move online. Some people are overwhelmed by the number of online passwords they have to keep track of and some older Australians may find it difficult to keep up with all of the many technological changes that have occurred over their lifetime. Recognition of these limitations should in no way limit attempts to optimise and share the benefits of the digital economy with all Australians, but rather challenge us to find a way to ensure that as many as possible can share in 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.

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?

There is evidence of past and predictions of future significant economic productivity benefits arising from investment in mobile network infrastructure.

A 2010 Access Economics report commissioned by AMTA found that the industry contributed $17.4 billion to the Australian economy in 2008-09.3 This includes $6.7 billion in direct contribution and $10.7 billion in indirect contribution. A recent industry report found that convergence and the availability of high-speed broadband networks (fixed and mobile)

[3] Access Economics Report, *Economic Contribution of Mobile Telecommunications in Australia,* June 2010.

is driving investment in the media and communications sector with investment levels predicted to reach $6.4 billion by 2014.[4]

The growth of mobile broadband is widely recognised as central and increasingly influential component of our evolving digital economy with significant capability to contribute to economic productivity and social connectivity.

The Australian Communications and Media Authority (ACMA) notes:

***There is widespread recognition that mobile broadband services are an economic enabler within society and the provision of these services, technologies and applications in the wider community is in the public interest**.*[5]

This is supported by a study conducted by Ericsson and Arthur D. Little that found that for every 10 percentage point increase in broadband (fixed and mobile) penetration, GDP increases 1 percent. The study also confirmed the correlation between faster broadband speeds and increases to GDP. [6]

As the usage and service expectations of consumers rises there is increasing pressure on the mobile network operators to ensure they have the capacity to meet an ever increasing demand for faster speed and bandwidth-hungry mobile data applications and services. The mobile network operators' capacity to adequately meet this demand and deliver productivity benefits associated with mobile broadband will depend directly upon the timely availability of spectrum resources and deployment of next generation mobile networks.

AMTA strongly believes that continued investment in infrastructure and innovation must be encouraged and fostered by the government's policy and regulatory framework so that the benefits of mobile broadband and a digitised economy can be realised by all Australians.

Conclusion

AMTA welcomes the opportunity to participate in further consultation on the Cyber White Paper.

Please contact Lisa Brown, Policy Manager, AMTA on 0405 57 00 59 or at lisa.brown@amta.org.au if you have any questions relating to this submission.

[4] "Comms and Media Sector spend to grow to A$6.4 billion by 2014:IDC" Communications Day 18 Oct 2011

[5] 2011 ACMA "***Towards 2020—Future spectrum requirements for mobile broadband"***

[6] Ericsson *New study quantifies the impact of broadband speed on GDP 27* Sept 2011