Submission No. 1

Joint Select Committee on Cyber-Safety

Submission by the Australian Communications Consumer Action Network to the Joint Select Committee on Cyber-Safety

April 2010

The Australian Communications Consumer Action Network (ACCAN) is the peak body that represents all consumers on communications issues including telecommunications, broadband and emerging new services. ACCAN provides a strong unified voice to industry and government as consumers work towards availability, accessibility and affordability of communications services for all Australians.

Consumers need ACCAN to promote better consumer protection outcomes ensuring speedy responses to complaints and issues. ACCAN aims to empower consumers so that they are well informed and can make good choices about products and services. As a peak body, ACCAN will activate its broad and diverse membership base to campaign to get a better deal for all communications consumers.

Contact:
Elissa Freeman, Director, Policy and Campaigns

Suite 402, Level 4
55 Mountain Street
Ultimo NSW, 2007
Email: info@accan.org.au
Phone: (02) 9288 4000
Fax: (02) 9288 4019
TTY: 9281 5322

Introduction

ACCAN welcomes the opportunity to provide comments in relation to issues raised in the Terms of Reference (ToR). ACCAN's primary concern is with empowering consumers to protect themselves from online security threats. We have provided comments regarding measures that are relevant to the safety of young people, older people, people with disabilities, as well as the broader Australian community.

This submission includes the following recommendations to improve cyber-safety:

- Improvement of content and reach of consumer education
- Review and enhancement of current protective measures

Response to Joint Select Committee on Cyber-Safety

1. Improved consumer education

The best way for consumers of all ages to safely navigate the online environment is to be empowered with relevant, reliable and useful cyber-safety information. To create a safer online environment, industry bodies must provide the tools and information to facilitate this.

Recommendations:

- **Development of consumer self-assessment measures**
- **Development of cyber-safety messages for young people**
- **Outreach to all segments of population**

1.1 Consumer self-assessment

Consumers should be provided with the tools to take more responsibility for their own cyber-safety. ACCAN proposes the development of an Online Competency Skills Test in Online Security (the Online Security). This test would help consumers assess how well they understand cyber-safety issues and could provide details of what steps they can take to better protect themselves and links to further online security information

To cater to the particularities of different segments of the population, the Online Security test could usefully be tailored to key audiences, such as youth, and the elderly.

1.2 Targeted cyber-safety messages for young people

The precursor to ACCAN, the Consumer Telecommunications Network, produced a tip sheet on social networking (at Appendix A). This tip sheet could be used as the basis for developing practical information for young consumers on Cyber-safety, with a particular focus on youth environments, such as social networking sites.

This could be a joint government/consumer/industry initiative. The Office of the Privacy Commissioner has a special youth portal dealing with many online issues, including social networking and identity theft, which could be usefully drawn on[1]. The information sheet could provide guidance on the following issues:

- Privacy settings;
- Considerations when accepting online friendships;
- Where and how to get help if you're being bullied or harassed;
- Respect in an online environment;
- Not to make details such as their home address, birthday or mother's maiden available online;
- Copyright and ownership; and
- Feedback and complaint services to ensure that security breaches and enquires are quickly and sufficiently followed up.

It is important that this information is communicated in a youth-friendly and accessible manner, including through the use of plain language, images and animations. It should also be distributed innovatively by leveraging key youth communication channels, such as facebook and other social media sites. In order to maximise the reach to as many young people as possible, distribution should also occur through comprehensive school, church, sport, government, consumer and industry networks.

1.3 Comprehensive outreach to all segments of population

As many older Australians do not engage with the internet due to concerns about safety or just lack of general understanding, it is essential to target them with cyber-safety messages through alternative means such as television and radio advertisements. This may involve the use of animated scenarios of real-life examples, using plain-English to explain how cyber-threats operate (detailing how best to deal with them), and where to go to for further information.

People with disabilities are another segment of consumers whose particular circumstances require specialised cyber-safety tools and support. On 7 June, ACCAN will be hosting the Cyber-Security Roundtable for People with Disabilities as part of Cyber Security Awareness Week. This will provide an important opportunity to bring together key experts to investigate the experiences of people with disabilities with cyber security and to identify areas of concern and their implications on policy and regulation.

Consumers generally should also be able to easily access an up-to-date list of confirmed e-security threats, including phishing scams.

[1] Youth – private i – your ultimate survival guide, Office of the Privacy Commissioner, available www.privacy.gov.au/topics/youth

2. Review of current protections

There are currently a large range of cyber-safety initiatives, and ACCAN is interested in how effective they are, and how they can be improved.

Recommendations:

- **Continual review of the *Spam Act* to keep up-to-date with evolving threats**
- **Review of current cyber-safety initiatives**

2.1 The *Spam Act*

The *Spam Act* has had a positive effect for consumers, reducing frustrations and risks flowing from receiving unsolicited commercial messages. It provides a strong foundation for the regulation of other cyber-safety issues, and has resulted in a number of other positive consequences, including:

- ISP's taking greater responsibility for protecting consumers from spam
- The creation of SpamMATTERS - ACMA's spam reporting system
- A number of visible and significant enforcement actions taken for breaches of the *Spam Act*
- Creation of multi and bi-lateral agreements to pursue spam originating overseas

We recommend this model be considered when thinking about how to regulate other online issues. ACCAN believes that as online threats continually evolve, tools and protective measures, such as the *Spam Act*, must be constantly updated to maximise their effectiveness. It is also important to further expand cooperation with other governments to control spam originating overseas.

2.2 Stay Smart online, E-security Awareness Week and ScamWatch initiatives

ACCAN acknowledges the Department of Broadband, Communications and the Digital Economy's (DBCDE) implementation of the Government's E-Security initiatives, including the enhancement and ongoing updating of the online security information website, *Stay Smart Online*. ACCAN also commends the DBCDE for undertaking an E-Security education package aimed at Australian school students, primarily between the ages of three and nine. There are also a number of other consumer education initiatives operating, including the E-security Awareness Week and ScamWatch.

There are many different agencies involved in promoting e-security and cyber-crime awareness – the ACCC, DBCDE, the Australian High Tech Crime Centre – and we expect these agencies will have undertaken assessments of the effectiveness of their campaigns and messages. We would recommend that the inquiry seeks details from all agencies involved in consumer education as to the successes of existing campaigns and proposals for improvement.

We note that the Communications Alliance Industry Code "Handling of Life Threatening And Unwelcome Communications"[2] is an example of co-regulation which provides consumers with robust protections in relation to one aspect of cyber-safety - unwelcome telephone calls

[2] Available at: http://www.commsalliance.com.au/Documents/Documents/codes/c525

and text message communications. This Code may be a useful reference for the committee when considering appropriate compliance models that could be adapted for other cyber-safety issues.

3. Useful research

To ascertain the nature, prevalence, implications and level of risk associated with cyber-safety threats, ACCAN has found the ACMA paper[3] "Click and Connect – Young Australians' Use of Online Social Media – July 2009" (Click and Connect) to be very useful. It indicates that a high percentage (75%) of children aged 12-18, claim to know the importance of not disclosing personal information online. They also remember key safety messages such as 'people aren't always who they say they are online' and do not reveal their address of phone number online. There is also useful data about prevalence of particular types of cyber-safety threats. For example, the incidence of cyber-bullying reportedly increases from one per cent of eight to nine-year-olds to up to 19 per cent of 16-17-year-olds, and is more prominent on the internet than on mobile phones (10 per cent of 16-17-year-olds reported experiencing cyber-bullying over a mobile phones but 17 per cent report experiencing this over the internet).

We would also recommend "Surfing on Thin Ice: Consumers and Malware, Adware, Spam and Phishing"[4] (Surfing on Thin Ice), produced by ACCAN's precursor – the Consumers' Telecommunications Network. This provides details of consumers' experiences with e-security and identifies areas of concern and their implications on telecommunications policy and regulation. ACCAN did a follow-up report in 2009 with updated figures, which was provided to the Parliamentary Inquiry into Cyber Crime[5].

ACCAN strongly supports evidence-based policy making, and believes that research such as Click and Connect and Surfing on Thin Ice are useful contributions to policy debates.

Conclusion

ACCAN strongly supports efforts to improve consumer cyber-safety. In particular, we believe that consumers should be made aware of, and be able to easily access, clear, relevant cyber-safety information and tools. Assessments of how effective the current cyber-safety initiatives being run by government departments should be made and where there are short-comings currently, these should be addressed. This may be by changes to current initiatives, such as extending the *Spam Act*, or through the creation of entirely new initiatives where necessary.

[3] Available at: http://www.acma.gov.au/WEB/STANDARD/pc=PC_311797

[4] Available at: http://www.accan.org.au/research_full.php?id=20

[5] Available at: http://accan.org.au/uploads/ACCAN_submission_Cybercrime_August_09.pdf

References

Appendix A: **CTN Fact Sheet: Basics of Social Networking**

What is Social Networking?

Social Networking involves the use of the internet to connect users with their friends, family and acquaintances. Social Networking websites are not necessarily about meeting new people online, although this does happen. Instead, they are primarily about connecting with friends, family and acquaintances you already have in real life. The most well known of these sites are Facebook, MySpace and Bebo. These sites allow you to share photos and videos, organise events, chat, download music and even play games online like Scrabble.

Often, each of your “friends” will be “friends” with several of your other “friends”. Just like in real life, the connections between people aren’t just one-on-one, but a network of connections. This online social network is very useful in spreading information, pictures and videos. For example, you can easily set up a web page with details and pictures of an event you might be planning, such as an art exhibition. The site allows you to easily send out invitations to other users of the social networking site. Then, if given the option by the host, those who are invited can send out more invites to their friends who might like to attend – hence, the network.

Just like other technology, for example mobile phones, social networking online can be a very effective tool for connecting with people. However, it requires some getting used to, so be patient while you learn the about the various features and opportunities.

Getting Started

If you are thinking about joining a social networking website, ask a friend or family member who already uses one of these sites to help set you up and show you some of the basic features. It can be complex and daunting to get started, but once you have been using the technology for a while you can fly around the websites and features easily.

Your Profile Page

When you sign up to a social networking website you need to provide your email address to verify your identity. This will automatically create your own profile page. A profile page usually allows you to post your picture and a few general details about you, your interests, some comments from you friends and a list of your favourite music. You don’t have to fill all the fields in your profile – think carefully about what you want people to know about you before you fill it in. You can usually adjust this information later on if you need to.

Friends and “Friends”

The whole point of joining social networking websites is to be in touch with your friends. “Friends” in the context of social networking has a specific meaning. For instance, for you to interact online with a friend, family member or acquaintance either one of you must first send a “friend request” via the website to the other and then for that request to be accepted. Once accepted, the technology recognises you as “friends” and you can interact with each other online, so you can view the other persons profile page, see their pictures, and send them messages.

Privacy

Social Networking sites have a variety of privacy settings you can adjust. This means you can control who sees your profile page and other information you share on the site. Some people do not mind having their personal information open for the world to see. However, we recommend that you don’t publish your home address and be mindful of posting other personal information about yourself or others, especially if you don’t have their permission.

Most people who use social networking sites prefer only to allow people they have officially become friends with to see their profile and other information. It is important to note that for most social networking sites (including Facebook and Myspace), when you sign up, the default privacy setting is *not* to hide your information. If you don’t want your profile and other information to be seen by people who you have not authorised to be your “friend”, after you sign up, you will have to check these settings and adjust them accordingly – look around the page for a link to “Privacy”.

Also, just as you wouldn’t give your mobile number or bank details to anyone who asked, you should guard access to all the details of your social networking account. For anyone who is aware of identity theft, there can be very serious consequences, even if the information seems harmless.

Safety

On the whole, nearly all the interactions that go on via Social Networking sites are safe and fulfilling, just like in real life. However, you need to be conscious of your safety and what you want people to see of yourself and your friends. Furthermore, everyone should remember these safety tips:

1) Don’t accept a friend request from someone you don’t know and don’t be afraid to refuse a friend request from someone you don’t know very well,
2) Be respectful of others if and when posting photos or videos of them or mentioning them where others might read about it,
3) If you feel that you are being bullied or harassed, be aware that you can remove someone as a “friend” and / or block them from interacting with you,
4) Change your privacy settings so that only your friends can see your profile page.

Teenagers and Parents

Parents should encourage an open dialogue with their teenagers about what they are doing online, such as by asking if they are using social networking sites. Parents shouldn’t be afraid to become involved with their children’s online activity, signing up and creating a profile for themselves is a good way to get to know how they work. Before signing up, or if concerned about something happening online, teenagers should speak to a parent or other adult.

Need more information?

Most social networking sites have more information in the Privacy/About Us sections of their sites. Bebo has set up a good page that covers these issues: http://www.bebo.com/Safety NetAlert provides practical information and advice on how to keep children, and your family, safe online: http://www.netalert.gov.au/advice.html Finally, the UK Home Office has released a comprehensive guide which can be downloaded at:

http://police.homeoffice.gov.uk/publications/operational-policing/social-networking-guidance

Last updated May 2008. If you have any comments or corrections, please email ctn@ctn.org.au or call 02 9572 6007.