SUBMISSION No. 96

Web Management
inter@ctive technologies
Building Communities and Relationships

Submission to

Joint Select Committee

on

Cyber-Safety

July 2010

Web Management InterActive Technologies Pty Ltd
P.O. Box 1073, Capalaba, Qld, 4157
Voice Phone: 07-3823-5150
Fax Phone: 07-3245-1717
Email: info@wmit.net

1. Introducing Web Management InterActive Technologies Pty Ltd

Web Management InterActive Technologies Pty Ltd has, since 2002, been the vehicle that James Collins has been using to provide Management & Control systems so that users of the Internet can better manage their Web experience.

Prior to that, since 1985, James developed online communication systems, providing online security systems to protect against electronic intruders, dangerous and unsolicited electronic mail, dangerous web sites, and providing individuals and companies large and small, with technical advice and implementation plans to manage their online facilities.

He introduced many Australian companies to the use of Electronic mail in the early days of online services. He has continued to produce systems which build online communities and relationships essential for the success of anyone involved in the business world of today.

The below information block is the Mission Statement from our web site, and it has been consistent since the founding of the company.

Within an Online, Network connected environment;

1. Deliver Web and Data Management services to empower average users with the ability to manage Emails, DNS Records, Web pages, and other Electronic/Network related services.
2. Ensure that data can be stored and retrieved across the Internet, safely and easily.
3. Provide a safe and secure Anti-Spam/Porn/Virus environment to browse web pages and to send and receive Electronic Mail.
4. Offer a level of support and security within their Home or Work network environment which they should expect. To provide it intuitively, before they even know they need it.
5. Connect Online People with the Products, Services and Information which they seek from their online experience.
6. Achieve all the above points by providing Communities of both Users and Suppliers and creating Relationships between both these groups.

Having been there at the birth of the Commercial Internet in Australia, and before that involved in all the many aspects of Online Communications, James Collins and his company remain in a unique position to provide guidance and advice on this exciting and cutting edge environment.

2. Products and Services previously developed.

- Online Management systems for Web Site design and maintenance.

- Controls for Dynamic setting of Internet communication protocols.

- Alternative Online funding models for ISPs and Web sites.

- Search and Reporting systems including one initial introduction of Google search services via a managed system.

- Children's Games, Learning Environments, Competitions and Puzzles in an online environment which is both Fun and InterActive.

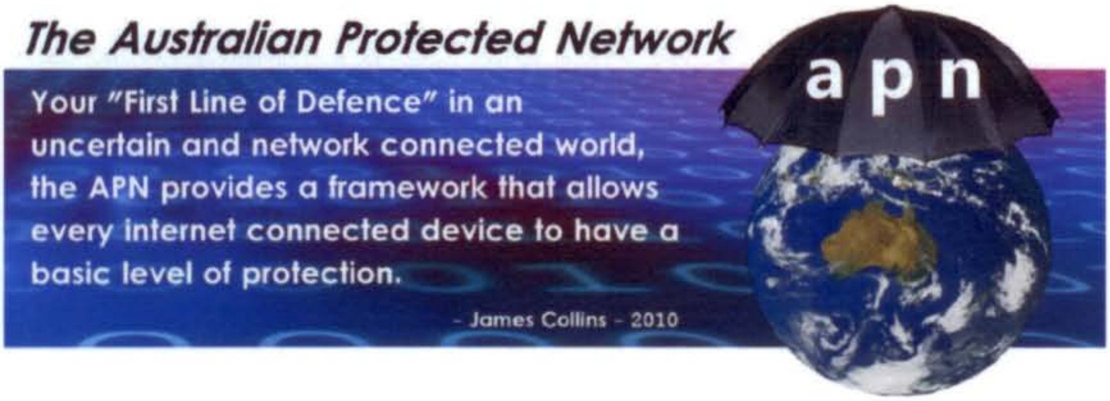
- Computer Operating on Resource Advantage. A system which draws data from various sources and makes predictive and collaborative decisions.

- An InterActive Information Window which endorses positive G rated content.

- Communities and Conversational group systems which allow support of Intranets and exchange of data systems.

- The Australian Protected Network. A Prototype of this system is available for the Committee to evaluate.

The Australian Protected Network



Your "First Line of Defence" in an uncertain and network connected world, the APN provides a framework that allows every internet connected device to have a basic level of protection.

- James Collins - 2010

Gizmo connects you
With the Wonderful WorldWide Web

3. Addressing the issues upon which the committee is inquiring.

(a) That a Joint Select Committee on Cyber-Safety be appointed to inquire into and report on:

I. the online environment in which Australian children currently engage, including key physical points of access (schools, libraries, internet cafes, homes, mobiles) and stakeholders controlling or able to influence that engagement (governments, parents, teachers, traders, internet service providers, content service providers);

This, like many of the issues being considered by the committee, has been well answered by other submissions. However, there is little uniformity or longevity in any of the current solutions employed. To be effective, measures must be well integrated and become the accepted norm, rather than a one off government program.

This is something the Australian Protected Network will be able to achieve by providing a central point from which to allow this standard to flow. It is not an additional service; it is part of the knock-on effect of having the APN framework in place. Some consideration should probably be given as to what are minimum access standards for certain key points of access. Note that the APN is extremely flexible in this area, allowing schools to engage in the creation of their own personalised security profile, and Internet Cafes to use a standard that might already exist. One should imagine that would be at least to block dangerous content.

There is no doubt that Government has a responsibility to provide a guiding hand in this arena. However the form that hand takes must be one of community participation rather than strict control, and be executed by Government funding rather than direct departmental operation. The APN is an entity which is designed for exactly this purpose, to provide protection on a national level while maintaining privacy standards that many commercial operators simply can not achieve.

II. the nature, prevalence, implications of and level of risk associated with cyber-safety threats, such as:

- *abuse of children online (cyber-bullying, cyber-stalking and sexual grooming);*
- *exposure to illegal and inappropriate content;*
- *inappropriate social and health behaviours in an online environment (e.g. technology addiction, online promotion of anorexia, drug usage, underage drinking and smoking);*
- *identity theft; and*
- *breaches of privacy;*

Children in today's world are growing up more technology-savvy than their parents. They are able to easily access more information than people of previous generations. They have more knowledge of things that are beyond their own immediate scope of existence. No longer are the backyard and the local creek the focal point of their weekends and holidays. Now they spend more time on the Internet, not only learning more useful information, but also being exposed to more experiences over which their parents have no control, simply because their parents lack full understanding of the technology and its capabilities.

Once upon a time, children learnt from their parents. They learnt social interaction, knowledge, practical skills, and respect. Because parents are being left behind by the technology that their children grasp so much more easily, they are losing this respect, and losing their position as guides and mentors for young minds. Children are more technology-savvy than their parents.

Technology-savvy does not necessarily mean that children are smarter. It does not mean they have more skills to recognise how advertising can influence them positively or negatively. They still need guidance from their parents as to what is appropriate or inappropriate. Children need to be taught how to respond to these new experiences. Parents, therefore, need to be educated about what their children already know, so that they can guide them in the proper direction. Parents need to be shown how to help their children use the Internet as a positive tool for learning and social interaction.

According to an ABC news report, Inspire Foundation, a mental health organisation, says "*parents should learn how to use social media to stop their children from being cyber-bullied.*"

http://www.abc.net.au/news/stories/2009/07/23/2634545.htm

III. Australian and international responses to current cyber-safety threats (education, filtering, regulation, enforcement) their effectiveness and costs to stakeholders, including business;

While Digital Literacy is a valid ongoing problem in our society, there are some basic protections which are lacking from the infrastructure which has built up over the past 15 years, since the release of Windows 95 fuelled an explosion in Internet usage. They can be summarised by the phrase "Setting a good example". At present, the Internet sets the example of "Anything goes", and while this is something it does well, if it becomes the central theme of our society, it can cause the erosion of our societal values. This prediction is coming true in all these areas listed. On the one hand, it is becoming more common to access materials which are inappropriate in a civilised setting, and on the other hand Governments are over-reacting with measures which are simply draconian in their application.

Towards the end of providing a good example, the Australian Protected Network proposes to put controls in the hands of parents that allow them to set limits for their children on the Internet. Rather than throttling Internet access, the APN can put in place a Basic level of protection, and then allow the users to modify their approach as per their individual requirements.

IV. opportunities for cooperation across Australian stakeholders and with international stakeholders in dealing with cyber-safety issues;

There is a great deal that can be done in the area of collaborative work. The principle behind the Australian Protected Network is that of providing a framework that engenders an environment of cooperation. The Australian Protected Network is designed to be the first of many such endeavours around the world, as we become more aware of the need for protection from criminal elements. Resources "pushed" through the "InterActive Window" are connections to information both local to Australia and contained around the world. This is especially important when you consider the influx of people who use English as a second language, and may feel more comfortable viewing information from another cultural perspective than that of our Australian/English heritage. While Australia has many good initiatives that can be exploited, there are sources of information and education that already form part of the operational Australian Protected Network Prototype system.

One of the "Basic" things that the APN blocks access to is the Command and Control servers of certain Botnets. Reduce the influence of the Botnets and you reduce the criminal influence of the Spam that they produce in ever increasing amounts. That alone will make a significant impact on Cyber-Safety.

V. *examining the need to ensure that the opportunities presented by, and economic benefits of, new technologies are maximised;*

Towards the topic of "new technologies" it is important to elucidate on Web Management's design of an "Australian Protected Network". The APN is a framework which allows users to control and shape their online view. For the purposes of this enquiry it should be noted that it -:

- Allows or disallows access to different classes of product or web site. i.e.: One selection could be the blocking of all direct external IP access and disallowing Web access to Chat web sites. Another selection might simply block criminal/fraud activity and gambling.

- Aggregates data from other services that provide information on compromised equipment and prevents access to that equipment.

- Seeks out compromised equipment and as far as possible attempts to inform owners of their problems, as well as providing links to possible solution providers. i.e.: Anti-Virus solutions or patches for their Operating System.

- Via the same system that allows users to "choose their own way to view the Web" they are able to securely use the Web Management InterActive Window to communicate with others via Moderator/Monitor controlled forums and to safely exchange files and links. Everything is also automatically checked against classification tests (i.e.: Files are checked for viruses as required, etc)

- The system uses the Computer Operating on Resource Advantage to constantly derive new sources of content to classify and scans the internet reading and processing web based information as it goes.

- Uses all of the above functions in collaboration with the Moderators/Monitors to prove the veracity of information about Internet based content and correct errors as they arise.

- By anticipating threats, being able to react quickly and decisively to put preventative measures in place against potential fraudulent/criminal behaviour. This is especially true when it comes to security advisories.

- The safety and security of user information is maintained at all times. Users have full access to all data they supply into the system and are able to maintain or remove their information at any time. Under no circumstances is personally identifiable information collected or used without the full acknowledgement of the user. This means that Proxy server access logs are *not* used as part of normal system operations at any time.

VI. *ways to support schools to change their culture to reduce the incidence and harmful effects of cyber-bullying including by:*

- *increasing awareness of cyber-safety good practice;*
- *encouraging schools to work with the broader school community, especially parents, to develop consistent, whole school approaches; and*
- *analysing best practice approaches to training and professional development programs and resources that are available to enable school staff to effectively respond to cyber-bullying;*

Cyber-bullying is an increasing problem for youth, and has been known to result in youth suicide. If parents learn more about the nature of the dangers facing their children, they can better deal with the problem.

The problem is reflected by the opinion of a writer for the Irish Times, who states, "*With no diaries to read, parents now need an IT expert to find out what their children are up to.*"

http://www.irishtimes.com/newspaper/opinion/2009/0116/1231974458097.html

4Parents.gov is one parenting site that highlights the dangers to children using the Internet unsupervised and without sufficient parental understanding of the dangers.

http://www.4parents.gov/sexrisky/risky/tech_dangers/tech_dangers.html

And, according to Parent Guide News, "*the family approach to technology and the continuing exploration of the Internet is still the best way to set standards and help your kids get on the right track.*"

http://www.parentguidenews.com/Catalog/Parenting/WantToBecomeATechSavvyParent/

Providing good examples to our children is a simple thing in a home environment. While our children are interacting with others we pass our values on to them in the form of encouragement and admonishment based on their behaviour. And there are literally hundreds of parenting courses available which are specifically designed to help struggling parents.

To provide that same environment online is just as easily addressed. Parents can provide a good example and encourage good behaviour while discouraging bad behaviour. This must happen *in* the online environment. The Australian Protected Network approach of Moderators and Monitors engenders an environment of earning trust and providing leadership examples. Leaders who are able to take on these roles are seen as good examples to follow, and users who attain greater acknowledgement by becoming Monitors or even Moderators themselves, are rewarded.

VII. analysing information on achieving and continuing world's best practice safeguards;

It is a matter of record that we must educate and continue to guide Internet users towards taking greater care on the Net. It is an environment where there is a great deal of good and a not insignificant amount of evil as well. No matter how much care and attention to detail is made from within the Australian Protected Network environment, there are some basic protections which will always remain the responsibility of the user. We can improve the Internet environment, provide structure, guidance and training, but in the end, if they are determined to ignore advice, they will learn the hard way. Users who have machines that become compromised because of this will, of course, also be advised of how to correct their problem, and put into a position that allows them to correct their problems, but not harm others at the same time.

Something that the APN does is to put information in front of the user that they can use to assist them in keeping up to date on what safeguards are available, and what they should be doing. As advisories regarding vulnerabilities in Operating Systems and Programs appear, the APN provides a central nexus from which to disseminate that information. After all, if the APN is the location of their controls to access the Internet, it is the best place from which to *know* that they are being informed.

VIII. the merit of establishing an Online Ombudsman to investigate, advocate and act on cyber-safety issues;

This is similar to a recommendation that came out of the Cyber-Crime enquiry, and I am still working on a response to that expansive document that the Communications Committee produced. While it is hard to summarise a response in time to get this document before the Joint Select Committee, I will make the following point. Creating such a position is something that may eventually become a requirement, but like so many of the recommendations that have been made over the years, there is just so much more to be done before we reach that point. Until there is a framework which encourages a Protective environment, any such position would run the risk of holding a great deal of responsibility and yet have little in the way of mechanisms in which to achieve any real goals. It would be a little like putting a policeman in the middle of the highway with no uniform, no tools of the trade and no respect from the passing traffic. There is much more to do before we reach the point of establishing that position.

4. The question of Mandatory ISP Filtering.

There has also been a lot of discussion surrounding the Mandatory Filtering regime planned by the Labor Government. There have been many reasons given for implementing it, and a quite vocal anti-filtering brigade who have spoken against it. Web Management has written literally dozens of papers on this topic over the past 3 years and about Protective Networking for even longer.

I think we would all agree that the stated "Aims" of Labor's "Mandatory ISP Level Filter" are quite reasonable. After all, who of us would say that we want to "Opt-in" to the viewing of Child Pornography? But those of us "in the know" realise that the current approach is simply confrontational and abusive of the people and technology that could be used to protect us.

The truths are buried in both sides of the argument. If we stop to think about it for a minute, we can find a path through this minefield to a reasonable outcome.

So, what is the goal of the Mandatory ISP Filtering system? Simply put, to prevent access to Child Pornography. The Government realises that this will only apply to Web pages, and it realises people will get around their filter. So a simple and quickly achievable goal would be to "limit" access to these resources.

The question that everyone asks is; "What is on the current list of sites planned to be blocked?" There was a Boarding Kennel, a Tourism Operator and a Dentist.

So how do innocent sites get on the list? Simply put, the criminal elements hack into vulnerable websites and exploit them to spam anything from illegal drugs to child pornography. There are literally millions of options for them to use out there, and without an adaptive system, there is simply no way to block them. The methods they use are tied up in the hacking underworld and the spread of virus and Botnet systems. The "Australian Protected Network" solution not only limits damage quickly – but provides a path for remedy and redemption for the infected equipment.

We are all faced with a situation where the net, which is a fantastic resource, is infected with this undesirable material. How do we sensibly approach this problem? We could block all the Dentists, Kennels, and Tourism sites. Or we could attack the problem at its source. We could protect ourselves from the Virus and Botnet infections that start the process.

Monitoring the changing landscape of dangerous sites and indeed RC sites on the net is a function of the Protected Network as it seeks to maintain a lock on where that content is at any given time. Just because a compromised host is delivering suspect content today, doesn't mean it won't be moved to another location tomorrow.

If we now approach the solution not as enforced censorship of content, but as a desired protection from materials that would harm us, the entire project takes on a new and positive light. Just changing the approach doesn't resolve the technical issues involved, but it does put those who are involved on the ground in a more tenable position, that of providing protection, rather than censorship. The technology we are offering exists and makes what was previously impossible, possible.

Now we can approach the problem of what is technically feasible in this arena, and what is not. How much we can protect ourselves, and what resources must we draw on to achieve this. If we can reach this stage, then a "Protected Network" is definitely in Australia's future.

James Collins

Managing Director,
Web Management InterActive Technologies Pty Ltd.