SUBMISSION No. 123

Roger Clarke's Web-Site © Xamax Consultancy Pty Ltd, 1995-2011

Search

Home eBusiness Information Infrastructure Dataveillance & Privacy Identity Matters Other Topics Waltzing Matilda What's New

Advanced Site-Search

Cyber-Safety

Evidence to the Joint Select Committee on Cyber-Safety's
Inquiry into Cyber-Safety Issues Affecting Children and Young People

Monday 21 March 2011, 11:30-12:00

Roger Clarke **

The version of this document at http://www.rogerclarke.com/II/CS-Evidence-1103.html contains links to online documents that provide further information on many aspects of cyber-safety issues

1. Introduction

The Joint Parliamentary Committee's Terms of Reference has broad scope. It encompasses such cyber-safety threats 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**.

Importantly, it is oriented towards responses to cyber-safety threats, with specific mentions of education, filtering, regulation and enforcement.

The Committee did not publish an Issues Paper. The Inquiry received a great many submissions (121 and 7 supplementaries by mid-March), and held a number of hearings (7 by mid-March). No digest of submissions, hearings or key issues was available as at mid-March. This created considerable challenges in working out what to focus on within such a wide field of view.

2. My Background

I am a consultant in strategic and policy aspects of information technology. I have spent 40 years in and around the IT industry, and am a Visiting Professor in both Computer Science at the ANU and Cyberspace Law & Policy at UNSW. I have been a user of the Internet since it became available in Australia in 1989 and have written one of very few histories of the Internet in Australia. More relevantly, I have been an observer and analyst of behaviour in cyberspace since 1990. I have published papers on many aspects of behaviour in cyberspace, with key examples listed at the end of this document.

I have been Chair of the Economic, Legal and Social Implications Committee of the Australian Computer Society (ACS, 1985-95) and a Board member of Electronic Frontiers Australia (EFA, 2001-2005), and I continue as a Board member of the Australian Privacy Foundation (APF 1987-, Chair 2006-), and as a Director of the Internet Society of Australia (ISOC-AU, 2010-).

I accordingly observe cyber-safety issues from multiple perspectives, particularly those of professional, researcher and public interest advocate, but also those of the consumer, citizen, father and grandfather.

3. The Need for Internet-Specific Measures

The present generations of Australians have available to them information infrastructure, and information and computing services, that enable effective access to and reticulation of information and other content, efficient utilisation of information and other content, and a great deal of communication with other human beings. Moreover, Australians look forward to progressive enhancements to the information infrastructure, and trust that the Parliament will ensure that access will be on a reasonably equitable basis.

During the last two decades, only quite limited stimulation of Internet usage has been needed. In the words of a sci-fi novellist, 'the street finds its uses for things', and successive generations of 'newbies' to the information infrastructure have found successive waves of things to do that have been interesting, and in some cases also valuable.

It was inevitable that, as Internet services matured and diversified, they would come to resemble the real world in terms of the mix of uplifting, useful, banal, seedy and downright unpleasant behaviour, communications and content.

Throughout the last 20 years, there have been discussions about whether the Internet was, would remain, and should be, a law-free zone. The reality is that it is a zone with very different characterics from geographically-based jurisdictions. The regulation of human behaviour in shared zones, such as the earth's atmosphere, space, the ocean floors and Antarctica, has demanded approaches different from those that provide a degree of control over behaviour in the streets.

The Internet in general, and cyber-safety in particular, present distinct regulatory challenges. The measures adopted therefore need to be devised in order to reflect the realities of this very particular zone.

Some government agencies may seek to invoke the mantra that 'legislation should be technologically neutral'. Within tight limits, the assertion has some merit; but generally it's wrong, and a dangerous excuse for public servants not to do their homework and not to consult the public. (For example, events in Japan this week have amply demonstrated the need for technology-specific regulation of the operation of nuclear power-stations). Internet behaviour needs to be subject to carefully-considered and specific regulation, but regulation nonetheless.

4. General Comments

The process of assessing potential measures to address cyber-safety issues needs to have a number of characteristics.

(1) Be Realistic about the Nature and Extent of Cyber-Threats

It is understandable that discussions about the safety of children involve the emotions. However, the Parliament has a responsibility to temper emotion with logic. In particular, anecdotes must not be generalised into pseudo-facts or even worse into pseudo-statistics, and sensationalised accounts of rare instances must not be thought of as being generally true.

It is important to understand both the nature and the actual incidence of such behaviours as cyber-bullying, cyber-stalking and the online 'promotion' of undesirable activities, and not to just assume them to be of epidemic proportions

(2) Be Practical about the Measures Adopted

Measures must not be adopted for merely symbolic reasons. They must be demonstrably capable of being applied in the settings they are intended for.

Measures must also be demonstrably capable of making significant contributions to the achievement of cyber-safety objectives. But cyber-safety measures will only be effective if they are grounded in an appreciation of:

- contemporary technological realities
- contemporary social realities
- the rapidity of technological change
- the rapidity of social change

(3) Avoid Unjustified Collateral Damage

Many initiatives can more harm than good. One example of an ill-judged attempt at cyber-safety has been the demonisation, and even criminalisation, of sexual experimentation by minors. Another example is the creation of offences of possession of digital content, which do not require criminal intent (*mens rea*), and which in some cases are declared to be criminal behaviour even if the person had no knowledge that they were in possession of the offensive material. This brings the law into disrepute, and causes law enforcement agencies to be unenthustiastic about investigating and prosecuting offences.

Where a possible cyber-safety measure has identifiable downsides, it is important that the justification for its adoption is prepared and analysed very carefully. This is particularly important where the negative impact will be felt by the very people it is intended to assist.

5. Specific Comments

In the current context, I believe there are a number of specific mistakes that need to be avoided, and a number of specific measures that need to be adopted.

(4) Avoid Dependence on Superficially Attractive but Ineffective Measures

Cyber-safety threats are real, and measures to address them must not be mere window-dressing but must have real impact. An important example of an attractive but ineffectual measure is content filtering. The problem is that it can only ever catch a small proportion of the material that the user would like to be blocked.

The use of filtering by an individual, or by a parent or a teaching institution on behalf of young children, can achieve a reduction in the arrival of unwanted material. It can also have signalling value. In particular, its existence, and its weaknesses, provide an opportunity for parents and teachers to make young people aware of the nature of cyber-threats.

For these reasons, there is widespread support for individuals to be able to apply filtering tools to their own data-flows, and to those of their young children. Moreover, government funding to ensure the availability of such filters to parents has enjoyed widespread support and will probably continue to do so. Because of its weaknesses, however, filtering alone is not enough. Complementary measures are highlighted below.

(5) Avoid Ineffective Measures that Seriously Harm Other Values

If a measure is not only ineffective in its primary purpose but also has side-effects that are harmful, then it should not be implemented. An important example of this is mandatory content filtering. I have briefly summarised at the end of this document the key reasons why mandatory filtering is such a dreadful idea.

The notion of a mandatory content filter should be accorded no credibility. By focussing energy instead on measures that are capable of being effective in addressing cyber-threats, much more progress is possible.

(6) Focus on Awareness and Education

Maintenance of the moral fabric of society is not achieved by preaching or teaching ('do as I say'). It arises from behaviour and witness ('do as I do'), and from learning.

Parents in particular must be encouraged and assisted to help their children to be aware of, and to have sufficient understanding about, the dangers that exist in both the physical and digital worlds. It is valuable to suppress information from the very young; but that must be complemented by progressive relaxation of the suppression as the child matures into the teenager.

Openness needs to be achieved sufficiently early in a young person's life that harmful taboos are avoided. It is counter-productive to tempt adolescents into thinking that gaining illicit access to prohibited information is part of an inevitable pattern of youthful rebellion and a rite of passage to adulthood.

(7) Focus on Channels, Voices and Content Appropriate to the Target-Audience

Recent generations have become less trustful of authoritarian figures. Instead, they pay much more credence to the thoughts and actions of respected peers. Young people also have relatively low literacy in the old-world sense of 'reading and writing'. On the other hand, they are highly functionally literate in their own, new-world ways.

The design of awareness and education programs must reflect the characteristics of the young people who the communications are being aimed at. In particular:

- rather than responding to preaching and teaching by authority figures, young people will adapt as a result of comments and behaviour by respected peers
- rather than responding to old dialects and written form, young people will adapt as a result of communication in their own dialects, and in aural form, and in visual and performative languages (particularly video and animation)
- rather than responding to old media (such as newspapers, radio, TV, and even advertisements), young people will be reached through a diverse array of contemporary channels
- rather than appreciating the cyber-threats described by grown-ups, and the cyber-safety measures invented by them, young people will respond to reinforcement of archetypes, signals and processes that are already part of their world

This topic is discussed in recent short papers on The iGeneration and The Privacy Attitudes of the Millennial Generation.

Efforts to assist parents and teachers to contribute to young people's cyber-safety are very likely to be ineffective, unless older people have access to awareness, education and training about the technological and social realities that are experienced by young people.

(8) Emphasise the Empowerment of Individuals

There is a role for formal regulatory measures, and these are discussed below. On the other hand, a great deal of the counterbalance against many cyber-threats needs to arise through self-reliance by individual young people, through mutual assistance within groups of young people, and from within existing social institutions.

For example, a primary antidote to cyber-bullying is communication to those young people who are subjected to it that they should not subscribe to the 'victimhood' pattern, but should stand up to the bullies. They should not perceive it as shameful on their own part that they should be picked on. They should understand that bringing it into the open shames the bully, not them, particularly if they enlist the assistance of their peers first, and go to the relevant authority-figures only as the last resort.

(9) Enhance Consumer Protections

Many international services-providers are consumer-hostile. For an analysis of the Terms of Service of six major international corporations and three Australian ISPs, see Clarke (2010). A broader analysis arising from the same project is in Clarke (2011).

The two largest and best-known actors are Facebook and Google. These corporations have developed their business models in ways that expressly exploit people, and particularly young people. Facebook's interests lie in having its users indulge in self-exposure and voyeurism. Google's interests lie in the accumulation into its own archives of vast quantities of personal data. Many other corporations that offer content services and social networking services have adopted the same rapacious business models.

In order to counter the imbalance of power between individuals and large corporations, baseline consumer and privacy rights are essential. This applies to adults, but in a number of cases even moreso to young people. This is because the absence of those rights lies at the heart of various cyber-safety issues. Young people are naturally less risk-averse than adults (and in some cases simply reckless), and are more prone to becoming caught up in excitement and fashion and overlooking the downsides of the deal that's on offer.

Consumer and privacy rights extend over a broad field. Checklists of consumer needs are provided in Clarke (2008) and Clarke (2011). A list of the privacy terms that people need is in Clarke (2005).

For the last two decades, Australian legislatures have failed the Australian public by importing the American notion of 'self-regulation' and permitting industry associations to write and administer their own codes of conduct. As part of its response to cyber-safety issues, it is necessary for this Parliament to pass genuine regulation into law, and to not just empower and resource regulatory agencies, but also to require them to prosecute offending corporations and their senior executives.

Formal legal requirements need to be imposed on international corporations that provide services in Australia in relation to key aspects of their Terms of Service. The Parliament needs to amend the newly-renamed Competition and Consumer Act to impose minimum conditions and override exploitative Terms. The following are specific aspects of the Terms of Service that organisations such as Facebook and Google define in ways that serve those corporations' interests but are harmful to consumers and especially to young people:

- visibility and clarity of the Terms
- consent
- use and disclosure of personal data by the provider for its own purposes
- accessibility of personal data by other parties
- clarity in 'privacy settings'
- data retention and destruction
- availability of pseudonymity
- changes to Terms
- changes to the meaning of privacy settings
- recourse
- redress

International corporations may of course seek to avoid compliance with domestic laws, in particular by claiming that the services are provided in a jurisdiction that has laws that permit consumer-hostile behaviour by corporations. This is not a sufficient justification for inaction by the Australian Parliament. Consumers protections need to be established, and enforced to the extent that is constitutionally practicable.

(10) Empower Law Enforcement Agencies, but do so Appropriately

There are many aspects of cyber-safety that need to be addressed by individuals, by groups, and through social institutions, with no involvement by law enforcement agencies.

When serious matters arise, however, law enforcement agencies need the requisite powers to investigate and prosecute. This includes the efficient acquisition of judicial warrants. Linked with that are efficient processes for presenting the agency's grounds for believing that access to particular locations or data will be important to the investigation or prosecution of a criminal offence.

On the other hand, excessive powers must be avoided. The last decade has seen serious erosion of standards in this area, through uncontrolled authorities and self-issued warrants. The enthusiasm to protect children must not extend to gross over-reactions such as those that have given rise to 40 inappropriate and as yet unrescinded statutes passed by Parliaments under the pretext that they were necessary to address the threat of terrorism.

(11) Impose Discovery Obligations on All Corporations

Australian corporations have generally worked with law enforcement agencies to ensure that systems are in place to ensure compliance with judicial warrants.

Some corporations, but particularly Facebook, have been less responsible, and, if media reports are to be believed, have been obstructionist and slow. The Parliament must impose on foreign corporations the responsibility to have processes in place to deal promptly with judicially authorised requests for information, and must make non-compliance a criminal offence. The question of extra-territorial reach is an issue for courts to consider, not an excuse for the Parliament not to legislate the rules of play in Australia.

The Parliament must also make abundantly clear to Australian government agencies that they have a responsibility to pursue breaches of the law by corporations, nomatter how powerful those corporations may be. The Australian Federal Police failed the test in relation to the breach of the Telecommunications Interception and Access Act (TIAA) by Google - which was an act clearly performed within the jurisdiction of Australian courts. The AFP and other agencies must be left in no doubt by the Australian Parliament that they have an obligation to apply laws relating to cyber-safety.

Brief Summary of Key Points re Mandatory Filtering

Ineffectiveness

- Blocking URLs that contain material that would be refused classification under Australian censorship law is **an exercise in futility**. There are very large numbers of pages, and hence it is financially infeasible to find and register them all. Moreover, anyone who is actively trying to distribute infringing material can change the URLs frequently or obscure the source-URL (e.g. by means of redirects and proxy-servers)
- Filtering is **readily circumvented** by the young people it is intended to protect, and they are supported and encouraged to do so by peers who they respect. To some extent they do this in order to gain access to the material, but much of this behaviour is motivated simply by the desire to challenge and bypass authority
- A great deal of the material that would be refused classification under Australian censorship law is not transmitted over the Web, but over **other channels**. A Web-specific filter cannot detect that content and cannot block it. These channels include IRC, many other chat and Instant Messaging (IM) protocols and peer-to-peer (P2P) networks
- **Filtering based on text analysis** fails to identify, and hence fails to block, the large majority of targeted material
- It is essentially impossible to conduct **filtering based on patterns in image and video**, and that will continue to be true for the foreseeable future (despite the optimism of research grant applicants)

Significant Harm to Other Interests

- Blocking URLs that contain material that would not be refused classification under Australian censorship law (i.e. material that is regarded as objectionable by some people) is indefensible in a free nation, because it imposes **the tastes of one group** on the entire population
- Blocking whole domains or even sub-directories where one or more URLs within them contain material that would be refused classification under Australian censorship law constitutes the **denial of access** to potentially

large numbers of pages that are not in breach
- Filtering based on text analysis inevitably generates a significant number of **false positives**, resulting in the blockage of material that should not be blocked. This has social and economic costs
- If the information infrastructure is perverted in order to provide a **facility for the inspection of content** for any one purpose, then it will be **available for other purposes in the future**, in particular for the detection of political speech unpopular with the government of the day, or indeed with any agency that can gain access to the facility. That would in turn undermine the vital freedoms of expression and of association
- If the information infrastructure is perverted in order to provide a **facility for censorship** for any one purpose, then it will be **available for other purposes in the future**, in particular for political censorship. That would in turn undermine democracy itself

References

Public Seminar on the Regulation of Bulletin Board Systems (1995, for the Senate Select Committee on Community Standards Relevant to the Supply of Services Utilising Electronic Technologies)

Net-Ethiquette: Mini Case Studies of Dysfunctional Human Behaviour on the Net (1995)

Virtual Chewing Gum on Virtual Library Seats? Human Behaviour in Electronic Communities (1996)

How Do You Cope With Censorship? An Analysis for IT Services Executives (1996)

PICS - The W3 Platform for Internet Content Selection (1996)

The Neighbourhood (1997)

Encouraging Cyberculture (1997)

Ethics and the Internet: The Cyberspace Behaviour of People, Communities and Organisations (1999)

Cyberculture: Towards the Analysis That Internet Participants Need (1997)

Public Interests on the Electronic Frontier: Their Relevance to Policy-Formation for I.T. Security Techniques (1997)

Technological Aspects of Internet Crime Prevention (1998)

The Technical Feasibility of Regulating Gambling on the Internet (1998)

Information Privacy On the Internet: Cyberspace Invades Personal Space (1998)

A Prosecution for Child Pornography in the A.C.T. (1998)

Freedom of Information? The Internet as Harbinger of the New Dark Ages (1999)

Introduction to Information Security (2001)

Introducing PITs and PETs: Technologies Affecting Privacy (2001)

Paradise Gained, Paradise Re-lost: How the Internet is being Changed from a Means of Liberation to a Tool of Authoritarianism (2001)

Defamation on the Web (2001)

Defamation on the Web: Gutnick v. Dow Jones (2002)

Origins and Nature of the Internet in Australia (1998, 2001, 2004)

Peer-to-Peer (P2P) - An Overview (2004)

Very Black 'Little Black Books - Social Networking Services' (2004)

Privacy Statement Template (2005)

Employee Dismissal on the Basis of Offending Images on Their Workstation (2006)

The Feasibility of Consumer Device Security (2007)

What Consumers Need in the Terms of Service for Online Services (2008)

The iGeneration (2010)

The Privacy Attitudes of the Millennial Generation (2010)

Vignettes of Corporate Privacy Disasters: FaceBook - 2004-2010 (2010)

Google - 2004- and Google Buzz and WiFi - 2009-10 (2010)

APF Submission to the Senate Online Privacy Inquiry (2010)

Internet Users' Second-Party Exposure (2010)

The Cloudy Future of Consumer Computing (2011)

Acknowledgements

This document benefited greatly from the author's various affiliations, and particularly from the ongoing contributions of many members of the 'link' Internet policy watchers' community and of the ISOC-AU members list. A number of members of those communities provided specific feedback on aspects of the draft version of this evidence. The judgements are mine alone, however, and my views may or may not be shared by organisations with which I have affiliations or for which I play public roles.

Author Affiliations

Roger Clarke is Principal of Xamax Consultancy Pty Ltd, Canberra.

He is also a Visiting Professor in the Cyberspace Law & Policy Centre at the University of N.S.W., and a Visiting Professor in the Research School of Computer Science at the Australian National University.

He is also currently Chair of the Australian Privacy Foundation (APF), and a Director of the Internet Society of Australia (ISOC-AU).

Personalia **Photographs** **Access Statistics**

The content and infrastructure for these community service pages are provided by Roger Clarke through his consultancy company, Xamax.

From the site's beginnings in August 1994 until February 2009, the infrastructure was provided by the Australian National University. During that time, the site accumulated close to 30 million hits.

Sponsored by Bunhybee Grasslands, the extended Clarke Family and Knights of the Spatchcock

Xamax Consultancy Pty Ltd
ACN: 002 360 456
78 Sidaway St,
Chapman ACT 2611
AUSTRALIA
Tel: +61 2 6288 1472, 6288 6916

Created: 17 March 2011 - Last Amended: 20 March 2011 by Roger Clarke - Site Last Verified: 15 February 2009
This document is at www.rogerclarke.com/II/CS-Evidence-1103.html