SUBMISSION No. 60

The Secretary
Joint Select Committee on Cyber-Safety
R1-109, Parliament House
PO Box 6021 Canberra ACT 2600

This document responds to your letter of 14 May 2010 inviting a submission regarding initial consideration by the Joint Select Committee on Cyber-Safety of topics relating to children and young people.

The following paragraphs outline the background to this submission, provide overall comments regarding cyber-safety regimes and address specific topics in the Committee's terms of reference.

They are made as an individual, rather than on behalf of the University of Canberra Law Faculty. They suggest that the Committee take a cautious stance in assessing claims about 'cyber-dangers' and about potential responses such as new legislation, establishment of a 'cyber-safety czar' or further public education campaigns.

Basis

Comments in this submission reflect more than a decade's experience in government, business and academia regarding the internet, digital technologies and the use by minors of 'new media'.

I teach undergraduate and postgraduate law at the University of Canberra, lecturing in information law and intellectual property law and on defamation, family law and bullying. I have been an invited speaker at major events on use of the net (eg presenting a plenary paper on children, dangers & digital surveillance technologies at last month's *Watch This Space* Children & Privacy conference) and have served on advisory committees of auDA (the Australian domain name regulator), IIA (the Australian internet industry association) and ISOC-AU (the Australian chapter of the Internet Society). Prior to teaching I consulted in Australia and overseas regarding technical, regulatory and user aspects of cyberspace, after work as a Commonwealth public servant specializing in new technologies. As an indication of credibility my writing about the internet and digital technologies has been cited in several hundred books and peer-reviewed journal articles and in government reports.

Children, young people and cyber-safety

Senator Wortley's 14 May 2010 'New Inquiry into Cyber-Safety' media release indicates that "it is timely to review Australia's progress in keeping children safe online".

In conceptualizing online safety and progress I suggest that the Committee adopt a stance of robust skepticism, questioning the rhetoric that –

- has inhibited understanding in community debate about the online experience of Australian children and young people
- fosters simplistic solutions that are ineffective and that divert resources from areas of real need.

The notion of progress implies improvement, for example an alleviation of risk or elimination of perils. It can also imply recognition of achievement, reward for past effectiveness and funding for future effort.

In reality we do *not* know whether there has been much progress. We also do not know whether that progress is attributable to the zeal and proficiency of government agencies (typically competing with each other) and nongovernment bodies, in particular bodies that are more proficient at building a media profile than in addressing serious harms.

Anxieties expressed a decade ago about pervasive online stranger danger, cyber-addiction and other ills have *not* been substantiated.

That is unsurprising, given the history of similar – and equally unfounded – alarms about the impact of the moving picture, gramophone, commercial radio and television. None of the dark visions of hooliganism, mass murder, vandalism, large-scale school absenteeism, fare evasion, drug abuse, sexual experimentation, unplanned pregnancy, white slavery and offences by adults against children (all duly noted in a succession of parliamentary committee reports and royal commission or other inquiry reports over the past century) came to pass. Contrary to mythmaking, Australian children – along with adults – are safer now than they were in 1910 or 1960 and contemporary harms cannot be narrowly blamed on the hypertext protocol.

'Progress' in safe use of the internet is primarily due to normalization of the online population, rather than to developments in statute law, effective policing or extraordinary efforts by public/private sector bodies such as Bravehearts. Normalisation is a consequence of most Australian households and organizations going online, independent of reassurance by or incentives from governments. As a community we are 'safer' than we were ten years ago because we are more experienced online, not because there are more and better watchdogs or because there are tools such as 'kid friendly' trustmarks and on-the-fly content filtering (tools that in practice are disregarded by most parents, are often subverted by minors or – because deceptive – simply represent a breach of the *Trade Practices Act*).

Progress should not be measured in terms of the establishment of specialist agencies (which may or may not result in substantive achievements) or in bureaucratic metrics such as the number of mouse mats distributed to schools and parents and the number of media launches. A challenge facing legislators and administrators is to determine whether particular safety initiatives have had any impact in the long and short term. Do not confuse correlation with causation.

The online environment

The Committee's invitation refers to the "online environment in which Australian children currently engage, including key physical points of access (schools, libraries, internet cafes, homes, mobiles)".

It is tempting for legislators to seek 'silver bullet' solutions to intractable social problems and for government agencies and advocacy organizations to legitimate their existence (or merely gain substantial funding). There are no silver bullets.

Poverty of the policy debate regarding internet filtering, characterized by hyperbole on the part of those who claim it will not/should not work (or is grossly erosive of civil liberties) and hyperbole that filtering is imperative and readily achievable. Australia has always censored some content, in electronic and non-electronic media (eg books, films, photographs, broadcasts). The contemporary censorship regime recognizes Australia's cultural diversity and individual responsibility (eg notions of parental restriction on access by minors to 'adult content' in broadcasts, print and electronic formats). It is complemented by restrictions on personal defamation and ethno-religious or other vilification, consistent with Australia's respect for human rights.

Contrary to the assertions of internet exceptionalists, whose perceptions are predicated on the notion that the internet is fundamentally different to other media and on a misreading of United States law (which is assumed to comprehensively protect freedom of expression and provide a global norm in the form of a *lex informatica* that does/should supersede Australian Law), regulation of the internet is not necessarily objectionable *per se*. Regulation is appropriate and, as with any other media, is broadly achievable.

It is clear that the Government's proposed national internet filtering scheme, like that of its predecessor, will not exclude all offensive content and in particular will not exclude some of the most abhorrent content. Our expectations about that scheme should be modest: it will not prevent all harms. Contrary to doom-saying by some of the noisier advocacy groups, it is not unprecedented and – like restrictions on computer games – it is not the end of the world. It has some value in complementing supervision by parents/guardians of what minors view online. It should not be promoted as a substitute for parental responsibility.

Abuse of children

The Committee has asked about the 'abuse of children online, particularly cyber-bullying'.

Advocacy groups will presumably argue that cyber-bullying is prevalent, increasing and serious. Those arguments will be reflected in suggestions that governments should fund special cyber-bullying initiatives. They may also be reflected in calls, as in the United States, for new statute law that penalizes cyberbullying and that assigns responsibility to parents/guardians.

I suggest that the Committee adopt a cautious stance in considering those arguments. It is clear from authoritative studies that cyber-bullying does occur. The nature and impact of that bullying varies considerably. It is not an isolated or unprecedented phenomenon; instead it typically reflects broader individual and collective aggression among minors, in the same continuum with theft, assault and other offences within schools and other locations. A moral panic, in which uncritical media reporting of isolated incidents leads to new statute law and unwarranted anxieties, is undesirable. In particular we should be wary about criminalizing behaviour that is more effectively and more appropriately addressed through non-criminal measures, such as education and counseling. We should also be wary about radical changes to parental responsibility.

The Committee's avoidance of hyperbole regarding sexting is strongly endorsed. The harms associated with the criminalization (as child pornography) of naïve experimentation or rule-breaking on the part of minors are likely to outweigh the benefits to the community at large or to those minors. Overseas research is particularly persuasive about negative impacts associated with heavy-handed policing of sexting and with prosecutions of minors that result in inclusion on sex-offender databases. Education campaigns, such as those highlighted at the May 2010 *Watch This Space* Children & Privacy conference under the auspices of the Victorian Privacy Commissioner, are more effective than trials of 15 year olds or seizure by enthusiastic NSW police personnel of the mobile phones of teenagers who have been making and sharing 'happy snaps'.

Australia, correctly, has been slow to embrace 'online angels' groups and other cyber-vigilantes. The Committee should critical examine claims by some groups and their proponents, because the effectiveness of the groups is highly doubtful, because their activity erodes respect for the law and because – despite self-serving claims of expertise – they lack both the resources and accountability of law enforcement agencies and may not for example provide evidence that can lead to a conviction.

Inappropriate behaviours

The Committee is exploring "inappropriate social and health behaviours in an online environment (e.g. technology addiction, online promotion of eating disorders, drug usage, underage drinking, smoking and gambling)".

I note and endorse the Committee's avoidance of characterizations of the internet as promoting promiscuity, pre-marital intimacy or what some advocacy groups stigmatise as deviant behaviour. It is clear that the internet has substantial value for minors who are seeking information about health and are grappling with questions of identity and sexual affinity, for example same sex attraction. Given high rates of depression and suicide among minors who are questioning their sexual affinities (unsurprising given negative media coverage such as recent statements by Jason Akermanis, condemnations by religious figures and continuing gendered violence demonstrated in authoritative studies such as the recent *Speaking Out* by Berman & Robinson) we should welcome rather than seek to restrict access to information that assists the wellbeing of Australian youth. Potential restriction is of concern in relation to filtering at the national level and by educational institutions.

If the Committee is considering harms it might contemplate the adequacy of Australian law, at the level of principle and practice, in addressing online hate-speech. Passage of a statute will not purge every heart of the hatred or fear or incomprehension that is expressed as ethno-religious or homophobic vilification. However, law has a symbolic function in articulating the values of the Australian community. The current Government's failure to enshrine human rights in the national Constitution, ignoring the recommendations of the Human Rights Consultation and experience in Victoria and the Australian Capital Territory (where litigation has *not* exploded and public administration has not collapsed), is a major lost opportunity for a just society that fosters the growth of Australia's children.

The Committee's letter refers to 'technology addiction'. The notion of cyber-addiction has been strongly promoted by some therapists, by tabloid journalists and by totalitarian governments (with exaggerated claims of addiction legitimizing restrictions on cybercafés and educational institutions that are aimed at choking political dissent). It is clear that some minors have an over-engagement with electronic games or the internet, in the same way that children have over-engaged with cricket, football, comics, broadcast television, billycarts or stamp collecting. There is very little recognition within the medical and legal communities of 'television addiction', 'videogame addiction' or cyber-addiction. 'Internet addiction' or 'technology addiction' is essentially a phantom disorder. We should be wary about recognizing a new 'addiction' and thereby removing the responsibility of minors and parents (some of whom, as in the past, need to establish rules for their children regarding homework and bed-time or accept that not all minors are academic high achievers) and fostering the growth of a new therapeutic sector. (Using the mooted criteria for technology and communication addiction most Committee members and staff are addicts but, presumably, are not seeking therapy and indeed – like most minors – have no need to do so.)

It has been fashionable for policymakers and advocates to express concern about the internet as a source of inappropriate information or as a medium that is uniquely powerful and thus persuades minors to adopt unhealthy values. As noted above, those claims are reminiscent of claims regarding film, television and other new media that have been seen as uniquely (or unprecedentedly) powerful and therefore requiring special restrictions. Much to the chagrin of some advertising executives, television and radio advertising has not turned us into consumer automatons. There is no substantive proof that the net is uniquely persuasive. (If we *do* think that it is especially seductive, we should be consist and implement greater restrictions on for example television advertising encountered by minors.)

I would therefore encourage a realistic view of the "inappropriate social and health behaviours" attributed to the internet. Those behaviours are fostered through the mainstream media rather than just the net. Concerns regarding exposure by minors to 'pro-anorexia' sites are legitimate but are arguably offset by the proliferation of online health sites and debates. They are of course located in a media universe that, like the Australian community, strongly valorizes thin blonde women and muscular suntanned shirtless males. Self-regulation on the part of advertisers and the dominant media groups has some way to go, irrespective of what happens online.

Identity

'Identity theft' has become something of a moral panic in advanced economies, with major anxieties, misinformation and commercial opportunism.

There is no substantive evidence that appropriation of the identities of children is occurring on a large scale in online venues and is resulting in fundamental harms.

There are anecdotal reports that adults have interacted with children in online venues while pretending to be children and have for example sought to engage in grooming. Australian case law demonstrates that grooming does occur and we should abhor any sexual exploitation of a minor. Facts, however, indicate that most molestation of children is wholly independent of the internet and indeed of strangers (digital or

otherwise). The Australian child is most at risk from intimates: the parent, cousin, elder sibling, much loved parish priest or babysitter rather than the unknown 'monster behind the modem'. There are indications that when online solicitation does occur it typically involves a peer, or a somewhat older minor, rather than a fifty-something with a criminal record.

If we are concerned with physical and psychological harms to children we might sensibly disregard alarmism from fear-mongers such as Bravehearts that foster extraordinary developments such as the *Lex Ferguson* in NSW.

We might instead substantially increase funding for mediation in family law disputes. Australian children do experience harms. Rather than a campaign about 'stranger danger', new legislation or new investigation units within law enforcement agencies we can tangibly improve the well-being of minors by making sure that all get fed and housed (more than a decade after 'no child will live in poverty' some are still going to bed hungry or sleeping on riverbanks) and that the pain associated with relationship breakdowns is minimized through support for parents. That improvement requires more than ingenuity in implementing the *Access to Justice* strategy or dogwhistling about income support as equivalent to abortion. It should be undertaken on a bipartisan basis, given that all parties espouse a commitment to Australia's children.

Privacy

The Committee refers to "breaches of privacy".

Some breaches are willed by minors. Others involve misbehaviour by organizations. Some behaviour is ethically reprehensible but is currently quite legal.

Three responses are feasible and should be adopted.

The first is education. We should and can encourage awareness – through community campaigns and through the national curriculum – about the nature of privacy (as a human right), about how individuals can preserve their privacy online (eg do not gift all data to Facebook) and about how individuals can respect the privacy of their peers.

The second is activism on the part of public sector privacy watchdogs. As an institution the Federal Privacy Commission resembles a somnolent, underfed watchdog. Its bark is not loud. It does not stir from its kennel. Its teeth are not used. The performance of its European counterparts, endorsed by both business and civil society advocates, demonstrates that a more active engagement with privacy issues is quite feasible and is quite appropriate. The current watchdog system is a digital Potemkin village: nice façade, poor performance, derisory remedies.

The third response is adoption of the recommendations by the Australian Law Reform Commission in its 2008 *For Your Information* report. Those recommendations are not radical or unprecedented. They are consistent with a succession of Directives and judicial decisions in Europe (a region where commerce continues and where citizens indeed have called for stronger protection). They are also consistent with decisions in the United Kingdom, where excesses on the part of major media groups have led courts – in for

example *Mosley v News Group Newspapers* [2008] EWHC 1777 – to restrain scandal-making that it is not in the public interest. The global financial crisis has demonstrated that markets cannot be left to regulate themselves. Children cannot be expected to treat privacy seriously when Australian organisations misunderstand or choose to ignore it. Substantive law reform will foster a privacy culture that is appropriate to the digital environment experienced by adults and minors and that, contrary to claims by some advocates, does not fundamentally reduce the commercial viability of data miners such as Acxiom.

Responses

The most effective "Australian and international responses to these cyber-safety threats" are predicated on informed decision-making, rather than media grabs.

Underlying any response must be an informed assessment of risk (some threats are more likely to eventuate, some incidents will affect major populations rather than a few individuals) and the significance (some harms are trivial, others are not). Australian governments have finite resources. They should accordingly target their responses, allocating funds and skills on the basis of real need rather than on the basis of bureaucratic self-interest, deference to particular advocacy groups or opportunities for a media release.

The Committee should also be wary of quick solutions such as appointment of a 'cyber-safety czar'. Governments across the world tend to create 'czar' positions out of frustration and because appointment of the czar results in a nice media release, offer accompanied by declaration of a 'war' (on terror, drugs, people trafficking, pollution, tax evasion …). A more effective response to concerns regarding online misbehaviour would be –

- meaningful funding for the strengthening of information technology expertise within the Australian Federal Police (and the state/territory forces) – given that the thin blue line regarding child-related offences in cyberspace rather than terrorism is indeed thin – and
- an associated cultural change within that organization to ensure that 'real policing' is perceived as including sitting in front of a computer rather than sitting in a car or holding a pistol.

Cooperation

It is unclear whether there are any major new "opportunities for cooperation across Australian stakeholders and with international stakeholders in dealing with these cyber-safety issues". The Committee should be hard-headed in asking who are those stakeholders, are they performing and whether there will be substantive benefit from new/continued cooperation. Will the opportunities be more than another government/industry/NGO roundtable or another overseas trip by senior executives?

Schools

Are there "ways to support schools to change their culture to reduce the incidence and harmful effects of cyber-bullying".

In considering cyberbullying (including harassment by SMS) we should recognize that it does not occur in isolation. It is a manifestation of underlying problems (eg disengagement on the part of students, cognitive styles such as ADHD, ethno-religious disadvantage, depression, a history of being bullied) and often accompanies 'offline' bullying such as assaults in the playground or tacit endorsement by teachers of homophobic vilification in the classroom/sportsfield. Are we going to do anything about those problems apart from exhortations to students to behave and curriculum items about 'self-defence' in cyberspace, such as warnings about not sharing your password with today's 'bestest bestest mate'?

We should also be brave and acknowledge that schools are *not* families. Teachers and educational administrators can only do so much. Hateful statements from a Fred Nile, Keysar Trad, Alan Jones or Jason Akermanis may speak louder and longer than anything that is seen on a school poster between classes. We cannot expect schools to monitor all communications that take place within school precincts (eg all SMS traffic) or outside those precincts.

As a corollary we might acknowledge that the Australian community places onerous demands on its teachers. K12 educators are not particularly well paid. If we want teachers to act as surrogate parents and to address concerns about cyber-bullying or other harms we need to reward performance. We need to recognize that teaching for some people will not be a long term career (ie assist educators to move out of the profession when burnout occurs, in the same way that we assist people to move out of the armed forces). We also need to do more than engage in a digital cargo cult that takes the form of providing laptops to schoolchildren and assuming that the task of education is done.

Roles

The final topic is "the role of parents, families, carers and the community". That role should be facilitative, rather than directive. Facilitation involves recognizing that minors have different needs, circumstances and capabilities. It involves equipping them with skills (for example through the education system) and with a confidence to venture into cyberspace, a confidence ultimately based on trust that each child can seek guidance from an adult or peer without being punished for a perceived transgression or an unfortunate encounter

Government *does* have a role in cyberspace. It should foster the growth of an environment in which children can have a childhood and are able to become self-reliant, happy and capable adults. That growth involves encouraging respect for children and adults as individuals who have irreducible rights and who have agency, ie are capable of making assessments and taking decisions. Children are not puppets: if we are concerned about their flourishing in cyberspace we need to avoid wrapping them in cotton wool or imprisoning them digital handcuffs, such as technologies that allow parents to monitor every SMS message or every word typed in an online chatroom. Those technologies produce a false sense of safety, because easily subverted by minors, and more importantly encourage parents to rely on tools rather than building a relationship.

Because the internet is a global network of networks we cannot make all the dangers go away. We can however help minors to cope when dangers are encountered. Breaking rules is an innate part of childhood:

it is how children learn boundaries or skills and how they deal with inescapable boredom or frustration. Rather than criminalizing particular breaches of rules or encouraging trauma through an exaggerated response to victimization (not every 'skinned knee in the cyber-playground' needs an intervention by a therapist or inquisition by a police representative) we should as a society, as institutions and as individuals on occasion encourage victims and child/teen offenders to acknowledge that a particular action was wrong (and should not be repeated) and then move on. Not all cyber-dangers are equal. Not all require a media campaign, a statute or a talk with a professional.

Bruce Arnold
Law Faculty
University of Canberra 24 June 2010