The Australian Council for Computers in Education

Submission to the Joint Standing Committee on Cyber-Safety

The Australian Council for Computers in Education (ACCE) recognises the importance of the work being undertaken by the Joint Standing Committee on Cybersafety and would like to contribute. ACCE, http://www.acce.edu.au , is the national professional body for those involved in the use of information and communications technology in education. ACCE has representation from all states and territories plus international affiliations in many countries.

While we agree that it is important to investigate the issues surrounding young people and cybersafety it is equally important to consider this in light of the ecology within which those young people live. This includes their peers (including virtual networks) but also their families, educators, and others. Not only are these people in need of education surrounding cybersafety to make informed choices for themselves and as role models. In a world of networked social media online practices are often made public. Any attempt at implementing cybersafety education with youth without also educating their wider networks/communities, especially those online, would inevitably fail. It is noted that the Terms of Reference include an intent to "encouraging schools to work with the broader school community," (ToR, a.vi.) however this intent is effectively limited to identifying school based policy and strategies. The Joint Standing Committee on Cybersafety needs to directly face the issue of educating the wider community, without inadvertently laying an unreasonable expectation on a school system which is under-resourced, time-poor, and consequently already generally struggling with effective community engagement. We encourage the Joint Standing Committee on Cybersafety to approach this problem with an ecology perspective, wherein the entire system needs to be leveraged, not just one component.

ACCE firmly supports the potential educational affordances of online communication, including social media. Teachers at all levels are demonstrating innovative and educationally rewarding uses of online media including social networking. Unilateral policies regarding removal, or blocking, of technologies such as mobile phones, or services such as social networking sites, would not recognise the potentially valuable educational outcomes (for students and teachers) they may afford. Similarly, such an action would be, in our opinion, almost impossible. Consequently we agree with other submissions to Joint Standing Committee on Cybersafety that educational responses are preferable. However, as previously noted, ACCE takes a holistic perspective and sees that educational initiatives across a broad spectrum of cybersafety issues and strategies need to be instigated at all levels within the school and wider community. For instance school based strategies could be coupled with traditional mass media, website and social media campaigns.

We also recommend to the Joint Standing Committee on Cybersafety that the Terms of Reference should also consider wider risks, including legal risks arising from the use of social networking media. ACCE has recently supported the launch of a report entitled: Teenagers, Legal Risks and Social Networking Sites (http://newmediaresearch.educ.monash.edu.au/SNSrisks).

The researchers included senior academics from education (Dr Michael Henderson) and law (Dr Melissa deZwart and Dr David Lindsay). This 18 month study surveyed 1004 middle school students (years 7-10), 204 middle school teachers and 49 parents of middle school students. In addition focus group interviews were conducted with 58 middle school students and 21 middle school teachers. The data was collected from 17 Victorian secondary schools from state (government run), Catholic and independent systems as well as metropolitan and rural locations. In addition to collecting this empirical data, the authors conducted a comprehensive review of the literature, SNS Terms of Service, and the Australian and International regulatory environment. The findings of this report are considered valuable and as such the report and its accompanying educational resources are recommended to the Joint Standing Committee on Cybersafety for consideration. The remainder of this submission uses excerpts from the executive summary of the report with permission from the authors.

The project identified the following as the main areas of the law that give rise to possible legal liability for young people using SNS:

- Privacy, disclosure and breach of confidence;
- Intellectual property rights, especially copyright infringement;
- Defamation; and
- Criminal laws, including harassment and offensive material.

The report provides considerable empirical evidence of the complexity and extent of risks. In brief, the project found that young people, their parents, and teachers were generally aware that the use of SNS can give rise to risks that must be managed; however there was a worrying lack of understanding of the nature of the legal risks. In addition, there was surprisingly little ongoing conversation about SNS use between parents and their children, on the one hand, or teachers and their students, on the other. In this respect, almost half of the surveyed students (46.1%) reported that they did not talk with their parents about SNS use, while almost three quarters of the students (74.6%) reported that they did not talk with their teachers about SNS use. One of several explanations was that adults were not sufficiently experienced or knowledgeable to be taken seriously.

The researchers also canvassed a broad range of domestic and international regulatory responses to the risks encountered by young people in their use of SNS. It was found that while these responses reflected varying cultural contexts, they placed a common emphasis on the importance of educating young people, their parents and teachers about the safe use of SNS and the broader internet environment. Recognising that the need to equip young users with the skills necessary to take advantage of online resources and participate fully in modern society, must be balanced against the potential risks outlined above, regulators need to emphasise skill development, education and information sharing as key aspects of any regulatory infrastructure.

In addition, the development of a self-regulatory system, such as the *Safer Social Networking Principles for the EU*, would provide a useful baseline of practice for SNS providers, against which their dealings with users, including young people, could be assessed.

Lessons to be learnt from the studies and the regulatory responses to date include:

- The adoption of an approach based on appropriately managing risks, not inhibiting use.
- Any policy response to the problems arising from the risks of using SNS must involve multiple stakeholders, including governments, SNS operators, parents, teachers and students. The US Joint Statement on Key Principles of Social Networking Safety and the EU

Safer Social Networking Principles provide good examples of processes that engage SNS service providers in working towards best practices.

- There is no 'one size fits all' regulatory response.
- Any regulation must incorporate a combination of modalities, including education, technologies, self-regulatory codes, and policies implemented through SNS terms of use.
- To date, police responses to risks associated with SNS use in all jurisdictions studied for this report have tended to be fragmented and insufficiently coordinated.

In conclusion, the key recommendations arising from this project are as follows:

1. In order to enhance the benefits of SNS use, and minimise the disadvantages, it is important for children and young people to be equipped with the necessary information to empower them to effectively manage risks associated with the everyday use of SNS. The best way to do this is through specifically tailored educational activities. As children and young people must be primarily responsible for managing their own risks, it is essential that educational activities focus on providing clear and accurate information about all risks associated with SNS use, including legal risks. These educational activities should be aimed primarily at equipping children and young people with the skills required to be effective digital citizens, and not focussed on rare or hypothetical fears.
2. Education about the full range of legal risks potentially encountered by the use of SNS should be part of a fully integrated cybersafety school curricula. This means that attention that is properly given to more dramatic issues, such as cyber-bullying and 'sexting', should be balanced with attention to other potential areas of legal liability. This strategy should also assist in promoting awareness of, and debates about, the Australian legal system as it applies to online activities. While acknowledging the crowded nature of school curricula, the importance of SNS in the lives of students, and the potential significance of social media for future digital citizenship, suggests that room should be found for these issues to be directly addressed.
3. The best way to approach the teaching of legal literacy in the digital environment is by the use of practical examples drawn from real life case studies. With this objective in view, one of the outcomes of this project is the Education Resource Book, which includes a series of classroom exercises aimed at promoting understanding and discussion of specific legal issues. The researchers for this project encourage the production and use of this and similar resource material for the use of teachers of middle school students.
4. The reported prevalence of posting of photographs of students to SNS, suggests that the legal and ethical issues involved with the posting of photographs – which include privacy, confidentiality, defamation and copyright – merit specific attention in any cybersafety curriculum. The significance of understanding these issues is emphasised by the incidents involving a Melbourne teenager posting naked photos of AFL footballers to her Facebook site.
5. The potential disparities in the approaches to, and understandings of, legal risks associated with SNS use between parents, teachers and students, as well as the reported paucity of communication using SNS between students and parents and teachers, suggests that there is some need for education and training of teachers and parents, as well as students. Much can be gained by the community from greater informed discussion of the implications of SNS use, including legal implications, among parents, teachers and students.

6. Consideration should be given by Commonwealth, State and Territory authorities to encouraging SNS service providers operating in Australia to enter into a self-regulatory agreement similar to the Safer Social Networking Principles for the EU. This would provide baseline commitments against which practices of SNS service providers in their dealings with young people could be periodically assessed.

7. Given the concerns expressed by teachers interviewed for this project, there appears to be an identified need for further guidance to be provided to teachers about the use of SNS, especially in the pedagogical context. In particular, there is a pressing need for research and policy work to be undertaken in determining the extent of the 'duty of care' owed by teachers in any interactions with students via SNS. In this respect, it is important that the salient differences between interactions via SNS, and interactions offline, including the different legal implications, are fully taken into account.

8. There is a need to promote holistic policy responses to the full range of risks associated with the use of SNS by young people. Any responses should be coordinated so as to minimize the risk of fragmented, inconsistent, and potentially contradictory, policy initiatives at the Commonwealth, State and Territory levels. If... the Commonwealth Joint Standing Committee on Cyber-Safety... establish[es] an Online Ombudsman, the Ombudsman's portfolio should extend to promoting education about the full range of legal risks associated with the use of SNS. In doing so, the Ombudsman should coordinate with Commonwealth, State and Territory Privacy Commissioners.

ACCE, wishes to thank the Joint Standing Committee for the opportunity to contribute to the conversation.

Tony Brandenburg
President of the Australian Council for Computers in Education.

ACCE acknowledges the work of Dr Michael Henderson (Monash University) in the preparation of this submission.