FILTERING CHILDREN'S ACCESS TO THE INTERNET AT SCHOOL

Kathryn Moyle
Charles Darwin University
Australia

Abstract

Countries differ in their policy responses to the question: "Should children's access to the Internet be filtered?" Countries such as the UK, U.S. and Australia do filter online content with software on servers, and countries such as Denmark, Sweden and The Netherlands, do not. The differences between these respective countries' school policies are philosophical and political. This paper discusses intersections between the aims and purposes of schools, the political economy and the use of electronic filters on the Internet, for educational purposes. The paper concludes with a reflection of the implications of these issues for school leaders.

Introduction

The Internet presents intriguing policy and practice dilemmas. Governments around the world recognise that the Internet provides students, teachers, parents and schools with opportunities previously not possible. This paper has been prepared following discussions with policy makers in three countries that have policies that require electronically controlled, filtered access to the Internet in schools, Australia, United Kingdom (UK), and the United States of America (U.S), and with policy makers in three countries that do not have policies requiring schools to electronically filter access to the Internet, Denmark, Sweden and The Netherlands. The discussions with these policy makers occurred at an international conference, and therefore was a convenience sample. The discussions were recorded with permission, and then transcribed. These discussions have been used to inform this paper.

For some years now, young children as well as teenagers have reported that mobile phones and the Internet are very important to their educational and social lives (Green & Hannon, 2007; Moyle & Owen, 2009). For example, almost all children over the age of 12 in Australia and over 50% of Australian children younger than 12, own a mobile phone (Australian Communications & Media Authority (ACMA), 2009). It is common for school-aged children to send emails, visit social networking sites, upload photos and videos, and contribute to their friends' blogs or wikis (Green & Hannon, 2007; Project Tomorrow, 2011). Furthermore, research in the UK suggests that as children mature, they use the Internet in increasingly sophisticated ways (Green & Hannon, 2007; Office of Communications [Ofcom], 2008). This UK research shows that young people aged between 8 and 11 years of age are most likely to access the Internet to play online games, whereas 12 to 17 year-olds report using the Internet to download music, movies, and video clips, and use these

functions for both educational and recreational purposes (Green & Hannon, 2007; Ofcom, 2008). These findings are consistent with those of other comparable countries (cf. ACMA 2009; Project Tomorrow, 2011).

But how do educators and policy makers deal with the dilemmas and moral conundrums raised by children being able to access a wide range of 'good' and 'bad' sites on the Internet? Schools, school districts and educational systems have to balance the political and the policy priorities placed upon them, with the educational priorities of their students.

Some Dilemmas

Internet-related risks commonly mentioned as threats to children include the risk of exposure to sexually inappropriate content; exposure to negative or intolerant beliefs and attitudes; cyber-bullying; contact with unwanted strangers; and access to inaccurate information. One strategy used to provide children with Internet safety at school in countries such as the UK, U.S. and Australia, is to filter school networks. *Filtering* is described as the use of software to block specified files on schools' servers. Filtering of the Internet can be managed through port blocking (blocking services) as well as through URL-blacklisting (i.e., blocking content).

But are the risks to children presented by the Internet, overstated and the responses over enthusiastic? This paper discusses the policy, educational and technical dilemmas to filtering the Internet at school. As outlined above, this paper is based on evidence collected from policy-makers in the UK, U.S., Australia, Denmark, Sweden and The Netherlands about electronic filtering of children's access to the Internet at school between 2009-2011.

Policy Dilemmas

Countries around the world are concerned about the safety of children while they are accessing the Internet, but take different approaches to address child Internet safety. The propensity of young people to use a range of devices and functions to access online sites and to communicate with friends, has resulted in schools and governments becoming concerned not only with Internet safety, but also concerned about the place in educational practices of online games, handheld devices such as cell or mobile phones, and the role of social networking sites. Formulating responses to these concerns has generated policy dilemmas for educational leaders.

The implementation of school Internet safety policies raise a range of complex moral and philosophical issues, the practical settlements of which can be seen played out in schools. As such, the approach taken to issues such as Internet safety, mobile and handheld devices in schools, and the educational potential of social networking sites, provides insights into what different schools and jurisdictions think is important to emphasise in relation to the roles technologies can play in a student's education, and the perceived risks they present to students' safety.

In European countries such as Denmark, The Netherlands and Sweden, there are no national policies to filter the content on the Internet, although local

school authorities can approve filtering content. Indeed, instead of having a policy to filter content, the policy of the Ministry of Education Denmark is to not filter content. In The Netherlands, no national law enables filtering of the Internet but if a local school board wants to filter or block a specific Internet site, that can be requested from the local district office.

Indeed, in Denmark, Sweden and The Netherlands filtering the Internet is seen as a form of censorship; and censorship is not something that is generally supported by the public in these countries. The Danish constitution for example, endorses freedoms such as the freedom of the press and of religion. Furthermore, according to the Danish constitution:

> Any person shall be at liberty to publish his [sic] ideas in print, in writing, and in speech, subject to his [sic] being held responsible in a court of law. Censorship and other preventive measures shall never again be introduced. (1953, § 77)

The Netherlands and Sweden have similar constitutions. In fact, Sweden was one of the first countries to include the freedom of the press in constitutional law, and all three countries (Denmark, Sweden and The Netherlands) take seriously in practice, the freedoms enshrined in their respective constitutions.

In the U.S. in comparison however, there are several pieces of legislation, both active and inactive, aimed at protecting children from potentially harmful people or content online. The U.S. Children's Internet Protection Act (CIPA) for example, requires schools to filter for 'objectionable material' (National Conference of School Legislatures {NCSL], 2010). CIPA was enacted in 2000 as part of the Consolidated Appropriations Act, which provides funding to elementary and secondary schools; provides grants to states to support public libraries; and administers the E-rate program which provides technology funding support to schools and libraries. CIPA can require schools participating in the E-rate programs to certify that they are using computer filtering software to prevent the on-screen depiction of obscenity, pornography or other material harmful to minors. In addition, almost half of the U.S. states have their own state Internet filtering laws that apply to public schools or libraries. Some state laws also require publicly funded institutions to install filtering software on library terminals and school computers (U.S. Federal Communications Commission, 2009).

Prior to the enactment of CIPA the US introduced the Child Online Protection Act (COPA) (1998). It has as its declared purpose restricting access by minors to any online material defined as 'harmful.' The U.S. Federal Court, however, has ruled that this law violates the constitutional protection of free speech, and has blocked it from taking effect. Sometimes though, COPA is confused with COPPA, the Children's Online Privacy Protection Act (COPPA). COPPA is in force, and has been designed to limit the ability of online providers to offer services to children under the age of 12 without explicit parental consent.

In practical terms then, countries differ in their policy responses to questions such as "who should filter the Internet?" and "what, if anything, should be

filtered on the Internet?" In The Netherlands, along with Denmark and Sweden, the Internet is not filtered at all unless a school community requests a specific site to be closed, or there is a benign technical reason to filter a site. In comparison, the practice in the UK, U.S. and Australia, is to provide government schools with Internet access that sees many Internet sites already blocked, filtered on the basis of their content.

But while some might see filtering the Internet as an over-reaction, it is naïve to think there is no malicious use of the Internet. The perceptions of the extent of 'bad' content available on the Internet, however, should also not go unchallenged. U.S. Professor Philip Stark (2008) calculates for example, that of the hundreds of millions of webpages on the Internet, 1.1% is 'adult entertainment'. Furthermore, Stark (2008, p. 13) notes that much 'adult entertainment' is U.S.-centric reporting that:

> A substantial percentage of adult webpages are hosted in the U.S.: about 44% of those in the Google index, 56% of those in the MSN index, 88% of those in the sample of search results, and 87% of those in the Wordtracker search results. About 6% of AOL, MSN and Yahoo! searches and 37% of the Wordtracker searches retrieve at least one adult webpage among the first ten results.

It should be noted too, that as soon as one objectionable site is closed down, others are created. This is the way that the Internet has been designed: it is the Internet's 'self-healing' capability. This 'self-healing' characteristic however, is what makes it difficult to successfully operate electronic filtering systems. The Internet's current structure and regenerative capabilities, mean that we can never walk away from questions about online safety of minors, rub our hands, and say, "well there's a job done!" Rather, it is always the time to focus on smart solutions.

Wider philosophical questions concerning learning and the purpose of schools, however, arise from the policy dilemmas concerning the use of the Internet in schools. For example, should schools be environments that are so safe and secure, learners cannot innovate, risk-take or learn behaviours that will help them to navigate the real world when they leave the school gates? As in life, there are risks in walking out the front door, but we take risks and we learn from them.

Ensuring students are safe in cyber-space though, can be considered as one of both risk minimization and risk sharing. In Australia for example, while government schools jurisdictions filter online content, private Independent and to a lesser extent, Catholic schools are able to make decisions about whether they choose to electronically filter or not. In a private, Independent girls school in Sydney, Australia, the school leadership has chosen to use students to successfully self-regulate online behaviour rather than choosing automated, electronic filters. This school publicly articulates clear values and behavioural expectations of students, and includes the use of students' voices to influence their peers' behaviour in online environments. That is, managing risks well can assist in the avoidance of harm.

Yet, although Internet-safety legislation and associated policies are ostensibly put in place to protect students, some argue that neither students nor parents are the primary audience for such approaches. Rather than primarily being concerned about students' welfare, Internet-protection legislation and policies are instead seen by some as a risk management strategy: a way of protecting administrators, politicians and other stakeholders from potentially hazardous legal issues.

Furthermore, there are differences in the roles the media play in the politics of the respective countries reviewed for this paper. There is an apparent duplicity of the press from time to time in countries such as Australia, U.S. and UK, where the media seem to delight in reporting when students crack government filtering systems, but will also carry horrific stories about instances of cyber--bullying. Inevitably such stories lead to the simplistic solutions of 'banning' and 'filtering.' These stories also feed politicians paranoia about the 'evil' nature of the Internet. Political representatives in Australia, U.S, and UK are acutely sensitive to the nature of media reporting about the use of the Internet in schools. Filtering software is an easy policy answer to provide Government Ministers with peace of mind. But only while they have a superficial understanding of the effectiveness of Internet filters. Understanding the technical effectiveness of Internet filters is necessary if school leaders are to put in place Internet safety strategies that are appropriate to the risks being confronted.

Technical dilemmas

Placing filters on the Internet is a common response in several non-European countries aimed at protecting young people from unwanted online material. Filtering involves the use of technical blocks to stop pre-determined types of content. All developed countries have at their disposal the capacity to put technical barriers in place to filter Internet sites. Filtering software is also available for mobile phones. It is a policy decision whether this technical path is chosen.

In countries such as Australia, UK and the U.S., filters are often included among the online services provided. One of the challenges for schools of using Internet filtering systems, however, is that the filtering systems themselves are not effective in what they do, and technologically-savvy students can crack or navigate around the filtering systems reasonably easily. Furthermore, the electronic filtering software itself tends to slow down the speed of the Internet generating further frustrations for the users. As such, electronic approaches to filtering are often found by teachers and students to be restrictive.

In addition, a common complaint of online filtering systems is that they block both wanted and unwanted materials. Research by U.S. Professor Philip Stark provides some insights into why this may be so. Investigating the effectiveness of online filters he found:

> Filters that block a large percentage of adult webpages also block a sizable percentage of clean webpages in error. For example, the most

> restrictive filter blocked about 91% of the adult webpages in the Google and MSN search indexes, but also blocked about 23-24% of the clean webpages in the indexes. On average, if that filter were applied to every webpage in the Google search index, the filter would erroneously block about 22.1 clean webpages for each adult page it blocks correctly. For the MSN search index, it would block about 23.1 clean webpages erroneously for each adult webpage it blocked correctly. Less restrictive filters blocked as little as 40% of the adult webpages in the indexes. Those filters blocked fewer clean pages in error. (Stark, 2008, p. 13)

The lack of accurate identification of 'adult pages' and 'clean pages' by electronic filtering systems can be frustrating for all concerned. As a result, some schools choose to avoid electronic solutions. Furthermore, the shift to mobile and 'in the cloud' services, which are more difficult to filter, and are available through devices such as the IPad, IPod and mobile phones, is seeing the locus of control shifting back to the users: students, parents and teachers. These mobile devices can be used in the educational environments without the owners necessarily conceding control to the system, and thereby enable students and teachers to bypass the school or jurisdiction's filtering system.

Finding Solutions

Educational jurisdictions that do not use filtering systems to block pre-determined content in schools, can provide some insights into the sorts of issues that can be taught to build students capabilities in online environments that ensure students exercise responsible online behaviours. In countries such as Denmark, Sweden and The Netherlands educators are encouraged to use social networking sites in ways that model safe and appropriate online behaviour. There is an emphasis placed on the concept of teachers building 'trust' with their students in ways that emphasise the development of students as creators of knowledge rather than simply consumers of information (Downes, 2007), and where the use of the Internet enhances students' learning by facilitating collaboration, innovation and creativity (Moyle, 2010). But one of the dilemmas facing educators is the place of the Internet and computers when it comes to student assessments and examinations.

In Denmark, the education system has introduced online examinations. Connected computers have replaced examination papers for every student. The final exams for high school are undertaken on a laptop, and some schools also offer students access to a wireless Internet network. But many countries do not see value in moving to using online assessments. One of the reasons why educators shy away from conducting examinations on computers with access to the Internet is the ease with which students can 'cheat' or plagiarize in such circumstances. To counter this possibility, along with the capacity to use computers and the Internet in examinations, the Danish Education Ministry has also put together a strict policy against cheating. Any student who is caught cheating is required to re-sit the examination, and the earliest this can occur is one year later (Zemer, 2009).

While the Internet may potentially provide better opportunities for cheating, meaning, cheating by copying and pasting, the same electronic system also allows for the closer supervision of cheating. Thus, for instance, if a student writes a sentence that was already written on some website, the IT system can identify this. It should also be noted however, that when students do their homework they could be copying from a friend, or their big brother or their parents could be doing their work for them (Zemer, 2009). As such, 'cheating' is not necessarily an outcome from access to the Internet, but rather a consequence of the stakes placed on the outcomes from school education.

As such, a fundamental issue that arises from this Danish approach is the bigger question: "What is cheating?' This question is one that has resonance for educators around the world. 'Cheating' is often considered a moral issue, where cheating is constructed as being 'bad'. But the capacity to use the Internet to check facts online, and the concept of 'cheating' during artificially constructed times called 'examinations', have become blended together with many education authorities deciding that access to the Internet during examinations is not appropriate.

Another way of thinking about the interfaces between examinations and the use of the Internet in examinations, however, is that students, rather than 'cheating', are accessing existing knowledge and applying that knowledge within their particular own circumstances. Furthermore, while it is well acknowledged that the Internet offers the potential for positive impacts on the nature of how and what students learn (cf. Farren, 2008; Wilson & Wright, 2007), and that those benefits associated with the using technologies in education include the capacity to build collaborative approaches to learning (Redecker, Ala-Mutka, Bacigalupo, Ferrari, & Punie, 2009), it is the very collaborative nature of learning that is actively forbidden in examinations. Hence computers and the Internet do not have a place in the testing regimes of many educational jurisdictions. But perhaps it is time to reconsider the role and purpose of examinations in school education, and to challenge the sorts of questions that should be included in examinations. Should examinations more closely approximate the life circumstances in which knowing something is important? How can knowledge be applied in meaningful ways to new circumstances? Should examination questions require students to go beyond providing factual answers to simple questions that can be answered through rote learning?

Partnerships for 21st Century Skills (2009), argues that it is no longer appropriate to prepare students for their lives beyond school, by teaching facts that are then regurgitated. One of the challenges for educators today, is how to construct approaches to learning that include both formative and summative assessment items, and that allow students to use technologies, and to apply and question their knowledge in different settings.

The policy, educational and technical dilemmas that arise from a consideration of Internet safety issues then, raise dilemmas for the work of school leaders. The nature of these dilemmas varies, depending on the policy, technical and educational approaches taken within a given jurisdiction. As such, this paper

concludes with a reflection on the implications of filtering and Internet safety issues for school leaders.

Implications For School Leadership

It is challenging for policy and decision makers to determine what they believe is of value in teaching and learning in the 21st century, and to develop curriculum and assessment approaches that match both students' and society's requirements. Different national government policy approaches seem to vary according to the weight placed on certain Internet safety strategies, over others. In countries such as the U.S., UK, Ireland and Australia, filtering of content on the Internet in schools is common practice, whereas the opposite is the case in European countries such as The Netherlands, Sweden and Denmark. There are also policy and practice tensions between the educational objectives of using the Internet and sites such as social networking environments for teaching and learning purposes, and the use of filtering systems as an Internet safety strategy.

Understanding the implications of Internet safety policies and practices for teaching and learning and students' development, and how these policies interact with the educational and technical developments occurring, are important for educational leaders to understand so they can provide leadership about these issues in ways that are both informed and sympathetic to the school communities within which they work. There are concurrent, symbiotic relationships between what is possible in schools; the policy approaches to Internet safety, their context and background; and the interactions between technical issues and developments operating at systemic and personal levels.

As clusters of schools are networked through a shared intranet and IT infrastructure and the resultant '24x7' access is made available to teachers and students, one of the challenges for educational leaders is to understand the changing boundaries between home and school. Practical responses to Internet safety to date have focused upon policy, technical and educational responses to moral and philosophical issues that are informed by culture. In some countries, these approaches focus on 'filtering the content'; while in others there is an emphasis on 'managing the bandwidth'.

Although this paper has focused on electronic Internet filtering and Internet safety, it is nonetheless important to muse about whether there is in fact a case for filtering content in schools. School jurisdictions around the world avoid the use of 'harmful' or 'objectionable' materials with students. Teachers and librarians have always selected materials suitable for their cohorts of students, and so, educators in one sense, have always filtered content. But in that case, what is different now?

With automated Internet filtering systems, Stark (2008) has highlighted the unintended consequences arising from filtering, resulting in the blocking of wanted content along with those pages that are unwanted. This practice is frustrating to the education enterprise for both teachers and students. More worrying, however, is that the boundaries between censorship and freedom of speech are also being blurred as a result of using automated electronic filtering

systems. So the question for school leaders in countries such as the U.S., UK and Australia becomes, to what extent are school communities of these countries willing to trade-off freedom of speech in order to apply Internet filtering systems to protect their children? The challenge and debate ought to be before us, but discussing Internet safety policies requires first acknowledging there is room for such debate. May this paper go some way to opening up spaces for such dialogue.

References

Australian Communications & Media Authority (ACMA). (2009). *Click & connect: Young Australian's use of online social media. 02: Quantitative research report.* Sydney: Commonwealth of Australia. Retrieved from http://www.acma.gov.au/webwr/aba/about/recruitment/click_and_connect-02_ quantitative_report.pdf

Australian Government, Department of Broadband, Communication and Digital Economy (DBCDE), (2010). *Cybersafety Plan,* DBCDE, Canberra, Australia. Retrieved from http://www.dbcde.gov.au/online_safety_and_security/cybersafety_plan

British Educational Communications and Technology Agency (BECTA). (2007.) *Signposts to safety: Teaching e-safety to Key Stages 1 and 2.* Coventry, UK. Accessed on 21 May 2011 from http://www.mmiweb.org.uk/publications/ict/esafetyks1and2.pdf

Downes, S. (2007) *Learning networks in practice. Emerging Technologies for Learning,* Volume 2, British Educational Communications and Technology Agency (BECTA), UK. Retrieved from http://partners.becta.org.uk/page_documents/research/emerging_technologies07_chapter2.pdf

Farren, M. (2008). *e-Learning and action research as transformative practice* . Innovate 5 (1). Nova Southeastern University, U.S. Retrieved from http://www.innovateonline.info/index.php?view=article&id=543

Green, H. & Hannon, C. (2007). *Their Space: Education for a digital revolution,* DEMOS, London. Retrieved from http://www.demos.co.uk/files/Their%20space%20-%20web.pdf?1240939425

Moyle, K. (2010). *Australian Education Review: Building innovation – learning with technologies,* Australian Council for Educational Research, Melbourne, Australia

Moyle, K. & Owen, S. (2009). *Listening to students' and educators' voices: The views of students and early career educators about learning with technologies in Australian education and training, Research findings.* Department of Education, Employment and Workplace Relations (DEEWR), Canberra. Retrieved from http://www.deewr.gov.au/Schooling/DigitalEducationRevolution/Resources/Pages/Resources.aspx#stuvoice

National Conference of School Legislatures (NCSL). (2010). *Children and the Internet Laws Relating to Filtering, Blocking and Usage Policies in Schools and Libraries.* U.S. Federal Government. Retrieved from http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/StateInternetFilteringLaws/tabid/13491/Default.aspx#COURT

Office of Communications (Ofcom). (2008). *UK children's media literacy, Ofcom,* UK. Retrieved from http://stakeholders.ofcom.org.uk/market-data-research/media-literacy/medlitpub/medlitpubrss/ukchildrensml/

Partnership for 21st Century Skills. (2009). *Assessment. A 21st century skills implementation guide*, Partnership for 21st Century Skills. Retrieved from http://p21.org/documents/p21-stateimp_assessment.pdf

Project Tomorrow. (2011). *The New 3 E's of Education: Enabled, Engaged and Empowered How Today's Students are Leveraging Emerging Technologies for Learning,* Project Tomorrow, California. Retrieved from http://www.tomorrow.org/speakup/pdfs/SU10_3EofEducation(Students).pdf

Redecker, C. Ala-Mutka, K. Bacigalupo, M. Ferrari, A., & Punie, Y. (2009). *Learning 2.0: The Impact of Web 2.0 Innovations on Education and Training in Europe*. Final Report, Institute for Prospective Technological Studies, Joint Research Centre, European Commission, Europe

Stark, P. (2008). The effectiveness of Internet content filters, *A Journal of Law and Policy for the Information Society*, 4, 411–429.

The Constitutional Act of Denmark. (1953). Retrieved from http://www.folketinget.dk/pdf/constitution.pdf

U.S. Federal Communications Commission. (2009). *Children's Internet Protection Act,* US Federal Government, Washington DC, USA. Retrieved from http://www.fcc.gov/cgb/consumerfacts/cipa.html

Wilson, E. & Wright, V. (2007). *Teacher Use of Technology: From the Teacher Education Program to the Classroom*, International Society for Technology in Education, USA. Retrieved from http://www.iste.org/Content/NavigationMenu/Research/NECC_Research_Paper_Archives/NECC_2007/Wilson_Elizabeth_N07.pdf

Zemer, E. (2009). *The Magazine*, IFAT Media Information, Israel.