Abstract
Whilst developing technologies such as mobile communication devices are presenting education with opportunities to generate flexible and portable solutions to teaching and learning it is clear that there are other, less desirable, outcomes occurring. The ubiquitous mobile phone has allowed the greatest flexibility with regard to mobility and communication. With the convergence of technologies, the most recent handsets offer a variety of opportunities to receive, capture and transfer data such as video and audio. Effectively the mobile phone appears to offer everything a computer can offer except on a smaller scale. With such potential, the incidents involving the transfer of sensitive data and digital intrusion through mobile phones have been documented within the media. Such incidents are clearly impacting upon the way individuals interact within and beyond the educational context. In order to examine the current and emergent risks mobile technologies may present towards privacy, the following paper employs the use of a taxonomy designed specifically for this purpose. Finally, the implications for educational establishments, mobile phone manufacturers and policy development in light of such risk analysis will be considered and discussed.

Context
During the past twenty-five years, the increase in the use of the mobile phone, sometimes referred to as the cellular phone, has escalated with a reported 1.8 billion mobile subscribers worldwide in 2004; a figure which has more than doubled in just four years (World Telecommunication/ICT Development Report, 2006). Additionally, a recent survey stated that over three quarters of 7-16 year olds (77%) in the United Kingdom now own a mobile phone (HBOS 2006). Communication devices such as these have become integrated into everyday lives in almost all areas of the globe and may be viewed as one of the most significant developments in the fields of information and communications technology. (Plant 2000)

Mobility of communication extends beyond the relatively familiar telephone functionality with, for example, opportunities to capture and transfer images, sound and video, access the World Wide Web and interact with others through text and e-mail. In addition to communication through speech, the convergence of technologies such as the digital camera, MP3 players and office-related software has effectively generated a powerful handheld computer (Prensky 2005). Consequently, the mobile phone owner is increasingly able to maintain contact with other individuals in a seamless and truly mobile manner through a multiplicity of modes.

In recent years there has been a developing interest amongst some researchers and educators in the potential of devices, such as the mobile phone, to support formal educational pursuits. As highlighted by Anderson and Blackwood (2004), the current use of mobile phones ‘is often personal, informal and ad hoc’. A study undertaken by Savill-Smith (2002) highlighted the fact that young adults aged 16-24 used their phone to maintain social contact and access entertainment facilities such as games. Children aged 7-16 years also view mobile phones as a key method of communication with friends and family members (HBOS 2006).

From these studies, it may be argued that the mobile phone is not currently perceived by owners, teachers or the general community as being relevant or appropriate to the process of schooled learning and therefore has no purpose within the educational setting. However individuals such as Prensky (2005), Anderson and Blackwood (2004) and Sotillo (2003) provide arguments which question whether this can, or should, continue to be the case. Prensky highlights the potential of the mobile phone as a powerful handheld computer whilst Anderson and Blackwood and Sotillo identify a range of benefits including 'strong pedagogical reasons to incorporate mobile learning and the use of mobile devices into educational practices.' (Anderson and Blackwood, 2004:7) The power, accessibility and flexibility of the mobile phone in supporting learning with multimedia technologies, web access and multiple modes of communication will perhaps serve to blur the boundaries of educational activity which are largely created by geography and time. Furthermore, with increasing numbers of children and young adults gaining personal access to mobile phones, the likelihood that these devices will enter the school environment will also continue to increase. Arguments for the integration of mobile phone technology into aspects of the taught curriculum within and beyond the school environment will, perhaps, gather momentum.

Privacy

Without minimising the benefits that the mobile phone can bring to the educational setting, there is a real need to address privacy concerns for individuals within that environment. New technological devices bring with them new dangers, and there is a difficulty in determining what the risks to privacy are. As pointed out by Palen and Dourish (2003), little has been accomplished in terms of analyzing the relationship between technology and privacy. It may be argued that the rapid development of technology does not always allow for detailed analysis of the potential consequences related to mobile communications. Often, the process of development and use is dynamic and society, including the educational setting, is ill-prepared to respond at the same speed in order to generate an environment where privacy is not compromised.

Risk assessment

Risk assessments concern themselves with specific hazards and how to address them. One difficulty in straight-forward risk assessment is that the many devices do not fit neatly into specific risk categories due to the multiplicity of hazards. Problems also arise when different experts attribute different meanings to risks. In these situations, a taxonomy can act as a looser framework within which risks may be evaluated.

There are two taxonomies of note that would appear to fit this context. The first is the *Taxonomy of Risk* from the Cyberspace Research Unit at Lancaster which addresses the problems faced by the young people when engaging with the Internet (O'Connell and Bryce, 2006). The second is a taxonomy proposed by Solove (2006) and identifies the different privacy harms and problems that have already achieved a significant amount of social recognition. However, these taxonomies do not fully address the impact that mobile technologies have upon individuals. Therefore, a new taxonomy is required based

upon emergent concepts from qualitative data collected from vulnerable groups (Atkinson et al, 2006). This is illustrated by the matrix in Table 1.

	Propensity for Harm	***Divulging Personal Information***	***Unauthorised Intrusion***
e-Sociability	Device functionality Manifestation of risk		
Data Boundaries			
Access Control			
Technological Impact			

Table 1: Taxonomy of Threat

The categories along the top of the matrix address three areas where risks to an individual manifest themselves. These three areas are extracted from an understanding that privacy is protection from harm, control over personal information and freedom from unauthorised intrusion. These consider the potential impact where damage to personal privacy could take place; where threats to giving out personal information might lie; and where there is the potential for unwanted and uninvited intervention.

Within each of the three categories, risks from technology are examined within four separate areas:

1. e-Sociability
   The act of being sociable and placing it within the electronically connected context.
2. data boundaries
   Where individuals place boundaries around their personal data and who places those boundaries.
3. access control
   Who is allowed to cross the boundaries for personal data and how the decisions are made to allow or deny access.
4. technological impact
   Anything that alters an individual's behaviour because of technology.

Table 2 summarises some of the existing functionalities and operations associated with mobile phone technology and presents examples of risk for each of the aforementioned categories.

	Propensity for Harm	***Divulging Personal Information***	***Unauthorised Intrusion***
e-Sociability	Device functions: Text, Camera, Phone calls, Email, Blogging, Bluetooth. Manifestations: Bullying, abuse		
Data Boundaries	Device Functions: User-controlled: Text, Camera, Phone calls, email, blogging, Bluetooth.		

	Manifestations: Third-Party: Location based services, surveillance
Access Control	Change SIM card Contact Service provider Location based tracking services Unfair charging strategies
Technological Impact	School policies on mobile phones Examination procedures 'cheating'

Table 2: Summary of Functionality and Associated Threats

e- Sociability

Mobile phones provide different methods for interaction: text messaging; image messaging; phone calls and email. Cameras embedded within the devices provide high resolution to take clear digital photographs and there is the ability to record short video clips. It is increasingly difficult to purchase a mobile phone without a camera and new phones are available with two cameras, one for taking digital photographs and another smaller one for use for use in video calls. Because they are embedded within the mobile phones, the pictures are then easily transmitted.

Bluetooth along with Wireless (Wi-Fi) connectivity provide different methods of transfer of images at little or no cost to the owner of phone, making them an attractive choice for sharing pictures with friends. To use Bluetooth, two devices must be paired together. New phones also provide the ability to watch videos and some like the Nokia N73 allow videos to be downloaded. O2 encourages people to upload content in return for payment (O2, 2006) and video social networking websites such as YouTube are launching the facility to use mobile phones to view the videos posted on the website (BBC, 2006).

Web access is made easier from the mobile phone with the use of General Packet Service (GPS). This allows charging by amount of data consumed rather than per connection, thus making Internet connectivity cheaper. Email can be collected whilst mobile using this type of connection or the bluetooth or Wi-Fi mentioned earlier. New Nokia phones contain LifeBlog software offering the ability to create an online diary, a blog, whilst on the move. Connecting the phone to the home computer reduces the costs for the user of uploading to an existing blog.

Each of the six methods identified above for e-sociability, namely: text; phone calls; camera; bluetooth; email; and blogging described earlier have the ability to be abused by individuals to bring about harm to another individual, they also blur the boundaries between the other two elements in the taxonomy, divulging personal information and unauthorised intrusion. Primarily the risks manifest themselves in terms of mugging; bullying; and predatory behaviour.

Bullying of both pupils and teachers has been raised as a problem. Text stalking cases have reached one million per year and there have been 5,640 prosecutions under UK

harassment legislation introduced in 1997 (Goodchild and Heathcote, 2005). NCH quoted figures of 14% of young people being affected (Catan, 2006). Field (2006) describes text bullying as being the result of a combination of factors to provide anonymity to the bullies; an increase in majority of young people owning a mobile phone; telecommunications service providers being slow to react; and weak laws. Given that text messaging has been identified as the preferred medium for mobile communication between teenage peer groups (Devitt and Roker, 2006) this trend looks likely to continue. The convergence of text messages, emails, video and camera phones along with social networking websites into one useful, small, device provide useful tools for bullies. However, bullying and video clips of violence, otherwise known as "happy slapping" are not the only concerns. Devitt and Roker (2006) found that a third of young people they interviewed had experienced an unpleasant incident with their mobile phone which included theft and mugging along with the bullying and "happy slapping".

Bluetooth has two particular issues that are worthy of note. The first is that once two phones are paired, the receiver has no control over what they receive. This can lead to proliferation of unwanted and perhaps distressing images. The second issue is that there are also security vulnerabilities which could allow malicious code to be run on the mobile phone (Zetter, 2004).

Blogging has become a popular past-time and is considered to be a growing phenomenon. (BBC, 2006a) It has also been identified by the Child Exploitation and Online Protection Centre (CEOP 2006) as an area of concern. McMillan and Morrison (2006) observe how young people build their community around the interactive technologies. The mobile phone now provides the facility for that interaction to take place, irrespective of where the user is situated.

Data Boundaries

Controlling where personal information is divulged becomes more complex with the influence of mobile communications. There are two main influences, user-controlled sharing of information and third party. As mentioned in the earlier section on e-sociability, sharing of personal information can be facilitated easily but it can also be controlled with the functions on the mobile phone. However, it is the third party actions, intruding upon the data boundaries of other people that are the primary concerns.

Transforming the mobile phone into a surveillance tool has become easier. Software can be downloaded to transform a mobile phone into a surveillance camera (Smart Card Group, 2006) and voice analysis software can be used to monitor phone calls and advise on predominant emotions (Power, 2006).

Access Control

Controlling who has access to an individual through mobile communication relies upon the techniques designed into the device and the policies adopted by the telecommunications providers. Should an individual be experiencing problems and wish to change their mobile phone number, they have two options, one is to change the SIM card within the device for a relatively small sum of money; the other option is to

approach the service provider and ask for a number change. Currently there is no facility on the device to block specific individuals from contacting the user.

From the perspective of location tracking upon the mobile phone itself, the user of the phone is expected to have agreed to the location tracking. However, the initial confirmation text message can be erased before the phone is handed to the user; reminder text messages can be sent during time periods of between 14 to 31 days. However, Rootsecure (2006) describe how to overcome these protection methods.

Technological Impact

There are clear implications that educational establishments need to respond in a manner which will protect the interests of the individuals within their premises. Some schools are already developing policies which set out their expectations with regard to mobile phone use. In general, such policies identify theft, bullying, unauthorised use of image capture and potential disruption to discipline as the areas for concern. Whilst it is recognised that these issues constitute clear risks to the safety and security of individuals within the school it is equally clear that the less obvious risks associated with access, tracking and data boundaries are not included.

In some instances, teachers have reported that incidents arising from inappropriate use of the camera facility on a mobile phone prompted the school to collect all mobile phones from children as they entered the school and return them at the end of each day. Such actions create management and organisational challenges for small schools and would be prohibitive in large schools.

For the majority of schools, the development of a policy which states that mobile phones are not to be used during the school day provides the only means of protection from the potential of inappropriate use. Teachers report that this has not prevented incidents where mobile phones have been used to facilitate bullying with unsolicited images being captured and distributed.

As pointed out by the British Educational Communications and Technology Agency (BECTA) 'The dangers associated with a standard PC regarding unsuitable material apply to mobile phones and other devices too, yet because mobile phones are personal and private devices, it is not always possible for parents or schools to monitor their use.' (2004)

References

Anderson P and Blackwood A (2004) Mobile and PDA technologies and their future use in education, JISC Technology and Standards Watch, (online) retrieved December 2006 Available from www.jisc.ac.uk/uploaded_documents/jisctsw_05_04.doc

Atkinson S, Jagodzinski P, Johnson C, Phippen AD, (2006), Personal Privacy: Exploitation or Control through Technology, Proceedings of the Sixth International Network Conference (INC2006), Plymouth, UK, 11-14 July, pp269-276

BBC, (2006), YouTube moves to the small screen, BBC, 28 November 2006 http://news.bbc.co.uk/1/hi/technology/6190984.stm

BBC, (2006a), blogging set to peak next year , BBC, 14 December 2006 http://news.bbc.co.uk/1/hi/technology/6178611.stm

BECTA (2004) Data Protection and Security, Coventry, BECTA

Catan, T, (2006), Bullies move into cyberspace, The Times Online, retrieved November 2006 http://www.timesonline.co.uk/article/0,,13509-2457146,00.html

CEOP, (2006), Blogs, Think You Know, retrieved November 2006 http://www.thinkuknow.co.uk/control/blogs.aspx

Devitt,K and Roker, D, (2006), The Role of Mobile Phones in Family Communication, TSA, Brighton

Goodchild, S and Heathcote, E, (2005), I was getting 40 texts a day. Then they became really sinister, The Independent on Sunday, September 18, 2005

Halifax and Bank of Scotland (2006) Children In London Are 2006's Pocket Money Winners (online) retrieved December 2006 http://www.hbosplc.com/media/pressreleases/articles/halifax/2006-04-15-01.asp?fs=/media/press_releases.asp

McMillan, S.J. and Morrison, M, (2006), Coming of age with the Internet, In New Media & Society, Vol 8 (1), PP 73-95, Sage, London

O2, (2006), LookAtMe, O2, http://www.o2.co.uk/fungames/lookatme

O'Connell, R., Bryce, J., (2006), Young People, Well Being and Risk Online, Council Of Europe, http://www.coe.int/t/e/human_rights/media/1_Intergovernmental_Co-operation/MC-S-IS/H-inf(2006)005_en.pdf

Palen, L., and Dourish, P., (2003) Unpacking "Privacy" for a Networked World. Conference on Human Factors in Computing Systems '03 Ft Lauderdale, Florida

Plant, S., 2000. On the mobile: the effects of mobile telephones on social and individual life (online) retrieved December 2006). http://www.motorola.com/mot/doc/0/234_MotDoc.pdf

Power, M, (2006), How to catch a cheating partner, The Independent, 17th February, 2006

Prensky M (2005) What Can You Learn from a Cell Phone? Almost Anything! *Innovate* 1 (5).retrieved December 2006 http://www.elearningsource.info/elearning/What%2520Can%2520You%2520Learn%2520from%2520a%2520Cell%2520Phone.pdf

Rootsecure, (2006), Locate almost anyone in the UK without their permission, rootsecure.net, retrieved February 2006 http://www.rootsecure.net/?p=reports/locate_anyone_in_uk

Savill-Smith C (2002) The M-Learning Project and its Investigation into Young Adults' use of Mobile Phones, Paper presented at the Annual Conference of the British Educational Research Association, University of Exeter, 12-14 September 2002 (online) (accessed 14 December 2005, cited 14 December 2006) Available from http://www.leeds.ac.uk/educol/documents/00002199.htm

Smart Card Group, (2006), ICAMCU , , http://www.icamcu.com/

Solove, D, (2006), A Taxonomy of Privacy, University of Pennsylvania Law Review, Vol 154, No 3, p477

Sotillo, S., (2003) Pedagogical Advantages of Ubiquitous Computing in a Wireless Environment. The Technology Source, May/June 2003 available from http://technologysource.org/article/pedagogical_advantages_of_ubiquitous_computing_in_a_wireless_environment/

World Telecommunication/ICT Development Report (2006) Measuring ICT for social and economic development (eighth edition), International Communications Union

Zetter, K, (2004), Security Cavities Ail Bluetooth, Wired News, 8th August 2004http://wired.com/news/privacy/0,1848,64463,00.html?tw=wn_story_page_prev2