WEBCAMS IN SCHOOLS: A PRIVACY MENACE OR A USEFUL MONITORING TOOL?

DR JOAN SQUELCH† & DR ANDREW SQUELCH
CURTIN UNIVERSITY OF TECHNOLOGY, WESTERN AUSTRALIA

Worldwide, schools are increasingly turning to technology to monitor the school environment with a view to providing a safer environment and improving school discipline. The use of surveillance technology in society is not new and the public will often find themselves on camera in public places and at public events in the interest of public safety and security. However, the use of surveillance devices such as webcams in classrooms to monitor student behaviour and observe teacher performance raises concerns about privacy and data protection. This article considers the role of surveillance technology, in particular webcams, in school safety and discipline, and the balance between making schools safe and respecting peoples' right to privacy. Issues relating to privacy and data protection with reference to relevant aspects of Commonwealth law and, in particular, law pertaining to schools in Western Australia are discussed. The article concludes with some guidelines for developing school polices on the acceptable use of surveillance devices in schools.

I INTRODUCTION

The establishment of a safe and secure school environment is essential for effective teaching and learning as well as for an orderly and disciplined school. A safe school may be defined as one that is free of danger and possible harm; a place in which staff and students can work, teach and learn without fear of intimidation, harassment, humiliation and violence. Therefore, a safe school is one that is physically and psychologically safe. Indicators of safe schools include the presence of certain physical aspects such as secure fencing and gates; buildings that are in a good state of repair; and well maintained school grounds. However, more importantly, safe schools are characterised by positive discipline, a school culture and ethos that is conducive to teaching and learning, professional teacher conduct, positive parent and community involvement, good governance and management practices and an absence, or low level, of crime and anti-social behaviour.

Australian schools are generally safe schools. However, they are not immune from crime and violence, and anti-social behaviour. Bullying, harassment, assaults, vandalism, graffiti, theft and arson are just some of the safety and disciplinary problems that schools have to deal with on a regular basis. Creating safe schools and maintaining a disciplined orderly school environment are generally a high priority for school administrators and teachers. School administrators and teachers have a duty to ensure schools are safe and to maintain discipline. To this end schools are expected to have school safety and discipline policies in place that provide for a range of school safety and discipline strategies. One strategy that is available to schools, and which some schools use, is surveillance technology. The use of the traditional closed circuit video and, now more recently, webcams, are another option that schools can turn to for solutions to provide safer school environments and improve school discipline. However, the use of technology, and

†*Address for correspondence*: Dr Joan Squelch, School of Business Law, Curtin University of Technology, GPO Box U1987, Perth WA 6845, Australia. Email: joan.squelch@cbs.curtin.edu.au

the possible increasing use of internet-linked technology, to monitor schools and classrooms, raises concerns about privacy and the protection of data. The main purpose of this article is to provide guidelines for the development of appropriate school policies for the use of surveillance technology. To this end, the article first considers the role of surveillance technology, in particular webcams, in school safety and discipline, and the balance between making schools safe and respecting peoples' right to privacy. This is followed by a discussion on issues relating to privacy and data protection with reference to relevant aspects of Commonwealth law and, in particular, law pertaining to schools in Western Australia.[1] The article concludes with some guidelines for developing school polices on the acceptable use of surveillance devices in schools.

II Surveillance Technology in Schools

The use of surveillance technology in society is not new and the public will often find themselves on camera in public places and at public events, all in the interest of public safety and security. Closed circuit television (CCTV), both passive and active systems, is commonplace in areas such as shopping centres, offices, banks, airports and government buildings. The aim is to deter unlawful and inappropriate activity and to aid in the identification of perpetrators of crime. With the growing threat of international terrorism, countries around the world are increasing the use of surveillance technology.

Surveillance technology is also found in schools. The primary aims of surveillance technology in schools are to enhance the safety of students and staff, protect school property against destructive acts and aid in the identification of perpetrators of crimes and anti-social behaviour.[2] In Western Australia, CCTV is one of several strategies used by the Department of Education and Training to boost security in public schools. According to departmental guidelines, schools in WA may use CCTV but approval must be obtained from the Security division of the Department of Education and Training and it must comply with applicable State and Commonwealth laws. The guidelines further require that schools must ensure that the 'system does not reasonably infringe on the privacy of individuals' and the use of a CCTV system 'should only be considered if no other appropriate options have proven or are likely to prove successful'.[3] According to the head of school security, the use of CCTV has contributed to the reduction in insurance claims for destructive incidents. Up to 2001 the cost of insurance claims had risen to $19.3 million, while in 2004 the cost of claims was reduced to $5.98 million.[4] Similar situations are reported in other States. In a 2005 media release, the Education Minister for South Australia, Jane Lomax-Smith, reported that the Department of Education and Children's Services was investing $4 million in school security, which included installing surveillance cameras. The Minister stated that 'over the last decade up to $10 million of taxpayers' funds has been needed each year to fix smashed windows, fire-damaged classrooms and other wanton damage to schools'.[5] The benefits of CCTV in protecting school property were also highlighted in a previous ANZELA Conference paper on school safety. Peter Christie provided an example of the use of closed circuit cameras in a Sydney school that had been used successfully to monitor staff movement, control vandalism and detect people responsible for thefts.[6] The use of surveillance cameras is, therefore, seen as an effective means of monitoring areas of the schools and reducing vandalism and other destructive conduct.

Another more controversial use of surveillance technology is for observing and assessing teacher performance. On Channel Nine's *A Current Affair* programme, it was reported that a private secondary school was using real-time surveillance technology to observe and record teachers in the classroom with the primary purpose of improving teaching and developing a better learning environment. This was done with the consent of the staff and was promoted as a positive

means of improving school performance. A teachers' union representative interviewed rejected the practice on the basis that it is a breach of privacy. However, is this in fact a breach of privacy? The school principal argued that there was no breach of privacy. There are inevitably conflicting views and opinions on the question of privacy rights.[7]

Advancements in digital technology have produced webcams, which provide another technological means of monitoring student behaviour and keeping schools under close watch. Unlike traditional closed circuit camera technology, webcams are cameras connected to a network and/or the Internet via a computer.[8] The webcam captures images that are automatically uploaded, using appropriate computer software, to a webserver and these images can subsequently be viewed by anyone with the relevant Internet address and a password, where applicable. All that is required for a webcam set-up is a webcam, computer with Internet access and a website to display the images. Webcams can be purchased for as little as $60. One of the most common uses of webcams is to view places of interest, interesting events, scenery and wildlife. In this regard, webcams can be a very useful educational tool for bringing the world into the classroom. Consider for example, touring the Busselton Underwater Observatory, viewing the space shuttle launch or watching a bird on its nest—all from the classroom.

However, in addition to using webcams as a beneficial teaching and learning resource, some schools are turning to the electronic eyes as a means of monitoring the school and student behaviour, and monitoring teacher performance with a view to improving the quality of teaching and classroom management. Like CCTV, webcams can be used to monitor areas of the school such as hallways, parking areas, classrooms, sport centres, offices, and student locker areas. Using existing Internet technology and infrastructure, webcams can provide a cheaper, faster and easier means of conducting surveillance. However, unlike CCTV, webcams connected to the Internet offer a more advanced and flexible monitoring capability. They can be used to directly connect the home and school so that parents can observe the classroom and their children's activities and behaviour in real-time from the home or office, or from any location in the world. Parents have an instant window to the classroom for which they need a computer connected to the Internet, a web browser and the Internet address of the school's webcam webpage. This application is already being used extensively in childcare centres.[9] The problem is that if parents can view the data on the Internet, there are countless other people who could gain access using unscrupulous means, especially if the site is not thoroughly secure. [10] The connection of webcams to wireless networks adds extra dimensions to the risk of privacy because of the increased possibility of data interception by people using readily available electronic hacking devices.

Currently there is little information and no research on the use of webcams in classrooms and their effectiveness in improving safety, discipline and teacher performance. However, according to Toppo 'school districts in cities nation wide [USA] and in England are experimenting with classroom webcams for security reasons'.[11] For example, the Biloxi school district in Mississippi, USA, has installed webcams in all its classrooms with a view to improving discipline and monitoring teacher performance.[12] Using webcams to monitor classrooms and control student behaviour may be a positive goal, but using webcams to assess teacher performance raises concerns. Braggs notes that webcams could 'have a negative effect on teacher morale if they have to worry about constant observation'.[13] Moreover, the presence of webcams in the classroom could create a culture of distrust, and teachers may have legitimate concerns about data being used by administrators in a punitive way. Toppo reports that 'privacy advocates, teacher groups and others worry about putting classes under an all-day microscope' and that 'some say cameras can be misused and interfere with teaching'. For instance, parents could start challenging what

teachers say and do in the classroom, and school administrators could be tempted to view records whenever a parent complains about a teacher or what is being taught. There is further concern that 'districts using them could become complacent about security'.[14]

A *Privacy Issues*

Whilst webcams, and other surveillance technology, may have a useful role to play in school safety and discipline, the use of cameras has raised concerns and questions about the privacy rights of students and staff. Braggs warns that 'webcams are an intrusion into the learning environment masquerading as a safety precaution'.[15] In a position paper on video surveillance in schools, the British Columbia Civil Liberties Association (BCCLA) for instance argues that 'general monitoring of student behaviour is an unacceptable intrusion into [students] private lives'. It is accepted that surveillance technology has a place in monitoring certain areas of the school for exceptional security reasons. However, cameras will also 'view and record student behaviour that is, while not perfect, also not violent and destructive'. The BCCLA points out that cameras 'record students engaged in normal and acceptable behaviour, that is now suddenly under the constant gaze of an electronic eye affording them no privacy'. [16] But what constitutes the right to privacy and what are the privacy implications of surveillance technology in schools?

The right to privacy is a basic human right valued in many societies. A right to privacy has been recognised and entrenched in many international and national human rights instruments and constitutions.[17] In Australia, however, there is no constitutional right to privacy and currently the common law does not appear to recognise a general right to privacy.[18] However, although the courts have not settled this position, more recent case law suggests that Australians may have a common law right to privacy.[19] The extent of privacy protection is largely limited to actions for breach of confidentiality and defamation. There are, however, scattered pieces of legislation that deal with the protection of personal information. The *Privacy Act 1988* (Cth) and various state counterparts provide some protection with regard to the use, collection and disclosure of personal information (discussed below).

The right to privacy is a complex concept and no attempt is made in this article to provide a comprehensive analysis of the concept.[20] It is noted in the *Laws of Australia* that 'the term privacy is difficult to define given its social and cultural relativity and breadth of activity it encompasses'.[21] The *Privacy Act 1988* (Cth) itself does not even define privacy! The Australian Law Reform Commission described privacy broadly as 'material which so closely pertains to a person to his innermost thoughts, actions and relationships'. A narrower definition of privacy is the right of individuals and groups to 'determine for themselves to what extent information about them is communicated to others'.[22] In very general terms, the right to privacy is associated with personal autonomy, protecting individuals against interference in their personal lives and activities, and the protection of personal communication and information.

The use of surveillance technology has the potential to infringe privacy rights insofar as it intrudes on people's private lives and activities, and captures and records personal information about people, with or without their knowledge or consent. However, the use of surveillance technology is commonplace in public places and is permitted by law. The question is then what are the limits to which surveillance technology can be used. In a report on privacy, the Australian Law Reform Commission (ALRC) proposed that it is not feasible to regulate the use of surveillance or recording by optical devices in public places such as streets and parks and other entirely public places. The report stated that people in a public place 'must anticipate that they may be seen, and perhaps recorded, and must modify their behaviour accordingly'. On the other hand,

it was argued that 'where a person may reasonably expect that his activities will be private, that expectation should be respected'.[23] To this end a distinction is drawn between private and public places. The more public a place is, the lower the expectation of privacy. However, determining whether a space is private or public and whether a person has a reasonable expectation of privacy in particular circumstances is difficult. The distinction between the private and public sphere has also become increasingly blurred with the proliferation of technology and an increase in public surveillance in the interests of public safety and security.[24] Moreover, the right to privacy is not absolute and is subject to other rights and interests of individuals, groups and society as a whole. As Ackermann J held in a South African case on privacy issues, the right to privacy has to be demarcated with reference to others and the interests of the community. He stated that 'privacy is acknowledged in the truly personal realm, but as a person moves into communal relations and activities such as business and social interaction, the scope of personal space shrinks'.[25] This view was also aptly expressed in a Canadian case in which La Forest J stated that 'the degree of privacy the citizen can reasonable expect may vary significantly depending on the activity that brings him or her into contact with the state. In a modern society, it is generally accepted that many activities in which individuals can engage must nevertheless to a greater or lesser extent be regulated by the state to ensure that the individual's pursuit of his or her self-interest is compatible with the community's interest'.[26]

In terms of surveillance devices in schools, this raises the question of whether schools, and in particular classrooms, are public or private places, and whether students and teachers have a 'reasonable expectation of privacy' when they are on school property. Although schools have restricted access, and therefore are not entirely public places like a public park, they are largely public places. When students and staff enter the school gates they move into a communal area where their individual, personal rights and interests may be demarcated and interpreted within the context of the wider school community. Thus, for instance, when it comes to a question of school safety and discipline, the personal rights of the individual are weighed and balanced against the rights of the broader school community to a safe and orderly environment. Students and staff can expect their activities at school to be more highly regulated and monitored than when they are in the inner sanctum of their home. However, whilst teachers and students may have a lesser expectation of privacy at school, they do not expect to completely sacrifice their privacy at school. Students and staff do not expect all their activities and communications to be public knowledge and under constant surveillance. Moreover, they maintain a right to the protection of personal information and the right to confidentiality of information.

B *Data Protection*

An important aspect of the right to privacy is the *protection of personal data* (personal information). This has become increasingly important with the growth in information technology. Information or data protection is concerned with the collection and handling of personal data. Various data protection directives and laws aimed at the protection of personal data exist in one form or another in most countries.[27]

In Australia, laws protecting the collection and use of personal data are haphazard, with little uniformity across States. The *Privacy Act 1988* (Cth) is the primary piece of legislation relating to information privacy at a Federal level. However, the *Privacy Act* is limited in scope and applies to Commonwealth and Australian Capital Territory agencies, credit providers, credit reporting agencies and organisations that use tax file numbers (Pt II of the Act). Section 14 of the *Privacy Act* contains eleven Information Privacy Principles, which apply to Commonwealth and

ACT government agencies. The Information Privacy Principles govern the purpose for collecting personal information, the gathering of personal information, the quality of information collected and recorded, the storage and security of personal information, record keeping, access to personal records, use of personal information, and disclosure of personal information.

The *Privacy Amendment Act 2000* (Cth) provides National Privacy Principles that govern the privacy of personal information held by private organisations (*Privacy Act 1988*, Schedule 3). Therefore, the application of the privacy principles extends to private schools, other than a school with an annual turnover of $3 million or less and which does not hold health information and provide a health service.

The ten National Privacy Principles set out how private sector organisations, including private schools, should collect, use, record, maintain and disclose 'personal information'. Personal information is defined as 'information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion'. A 'record' is defined as 'as a document, database (however kept) or a photograph or other pictorial representation of a person'. The collection of personal data by means of surveillance cameras and webcams would fall within the meaning of personal information.

The National Privacy Principles, therefore, regulate the *collection of personal information* and the *use and disclosure of personal information*. With regards to the collection of personal information the first National Privacy Principle prohibits collection of information by organisations unless the information is necessary for one of the organisation's functions or activities. Further, an organisation may only collect personal information by lawful and fair means and when collecting personal information the organisation must make certain disclosures to the individual. In particular the person must be made aware of the identity of the organisation, the purpose for which the information is to be collected and how the person may access the information. Other principles also require an organisation to take reasonable steps to make sure the personal information is accurate, complete and up-to-date and to ensure it is not misused. The collection of 'sensitive information' is generally prohibited unless the individual gives consent.[28] The National Privacy Principles provide further restrictions on the use and disclosure of information. In general, an organisation is prohibited from using or disclosing personal information about an individual for a purpose other than 'the primary purpose of collection' unless an exception applies, for example, if use or disclosure is required or authorised by law.

The Federal *Privacy Act* does not regulate State or Territory agencies, except for the ACT. The States and Territories have their own various privacy laws that regulate the collection, use and disclosure of information. Western Australia does not have specific privacy legislation. However, the *Surveillance Devices Act 1998* (WA) ('*Surveillance Devices Act*') is a primary piece of legislations relevant to the use of surveillance technology in schools in Western Australia.[29] In general the legislation prohibits the installation, use and maintenance of optical surveillance devices to monitor or record private activities. This is, however, subject to certain exceptions.

Section 3 of the *Surveillance Devices Act* defines 'optical surveillance device' as:

> any instrument, apparatus, equipment, or other device capable of being used to record visually or observe a private activity, but does not include spectacles, contact lenses or a similar device used by a person with impaired sight to overcome that impairment.

Section 6 of the *Surveillance Devices Act* makes it an offence to install, use, or maintain an optical surveillance device to record or observe a private activity. 'Private activity' is defined to

mean an activity carried on in circumstances that may 'reasonably be taken to indicate that any of the parties to the activity desires it to be observed only by themselves, but does not include an activity carried on in any circumstances in which the parties to the activity ought reasonably to expect that the activity may be observed'. Similarly, 'private conversation' means 'any conversation carried on in circumstances that may reasonably be taken to indicate that any of the parties to the conversation desires it to be listened to only by themselves, but does not include a conversation carried on in any circumstances in which the parties to the conversation ought reasonably to expect that the conversation may be overheard'. The *Surveillance Devices Act* does not cover an activity outside this definition.

The few exceptions to the general prohibition on the use of optical surveillance devices include:

- Where the parties to the private activity expressly or impliedly consents (s 6(3)(a));
- Where the principal party to the activity expressly or impliedly consents and the installation, use or maintenance is reasonable necessary for the protection of the lawful interest of that party (s6(3)(iii)); and
- Use in accordance with Pt 5 of the *Surveillance Devices Act*, which provides for the use of devices in the public interest.

The use of surveillance devices in the public interest includes the use of devices by persons who have children under their supervision and care to record and observe the private activity of a child or protected person[30] if there are reasonable grounds for believing that the use of the devices will contribute to the protection of the best interest of the child or protected person *and* it is in the public interest (s 27(3)).

Surveillances cameras and webcams fall within the definition of optical surveillance devices given above and any information recorded is personal information that would be subject to data protection principles. The *Surveillance Devices Act* binds public schools in Western Australia that intend using surveillance devices. The prohibition applies to circumstances in which people reasonably expect their activities to be observed only by themselves. It does not include an activity carried on in any circumstances in which the parties to the activity 'ought reasonably to expect that the activity may be observed'. What can teachers and students reasonably expect in schools? What activities in schools would fall within the definition of 'private activity' that would not be subject to observation and recording? In discussing privacy above, it was noted that teachers and students can expect to have a lower expectation of privacy in a school and few areas of the school would be considered private.

The installation and use of cameras and webcams in schools may also fall within one or more of the exceptions to the general prohibition contained in section 6 of the *Surveillance Devices Act*. One exception to the general prohibition is that surveillance devices may be used where a 'principal party to the activity consents' and the use is for the 'protection of lawful interests'. Schools may argue that the use of surveillance devices is reasonably necessary to improve teaching, maintain good discipline and protect teachers and students, and school property against crimes and anti-social behaviour. The question is who must give consent and can students give consent? Teachers can consent to having their classrooms monitored but what about the students? Parents may need to give consent on behalf of their children. However, the law may recognise that in certain circumstances students could give consent themselves.[31] The second exception to the general prohibition is the use of devices 'in the public interest' and in particular for 'the protection of the best interests of the child'. Schools may present compelling arguments that the

use of surveillance devices in schools is both in the public interest in terms of providing safe and secure schools, and in the best interests of the students by providing a safe learning environment and improving the quality of teaching.

III Issues in Developing an Acceptable Use Policy

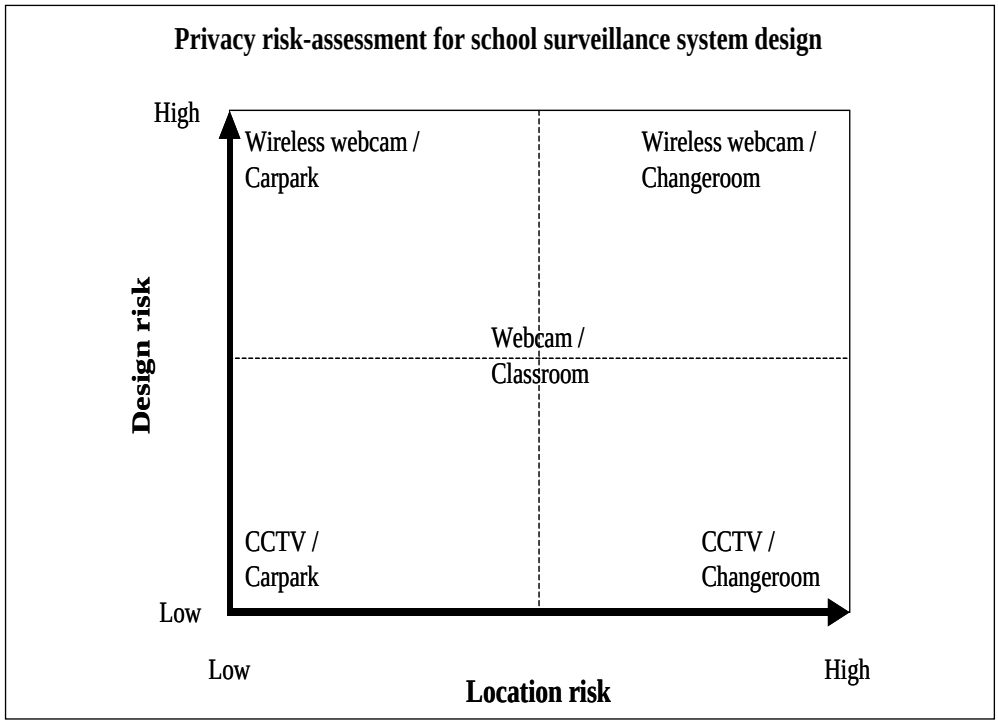
Many schools are currently using surveillance technology in the interest of school safety and discipline, and it is likely that this will increase over time. With the growth in digital technology and wireless technology webcams and the like present an easy, efficient and low cost means of monitoring schools and classrooms. If schools intend using such technology it is essential for schools to have a policy on the acceptable use of surveillance technology. This section of the article provides some guidelines on the acceptable use of surveillance technology gleaned from legislative frameworks and school practice on the use, design and management of surveillance systems.

A *Why the School Needs a Surveillance System*

Before installing surveillance devices it is essential for a school board (or governing body) to first ensure they have the necessary authority to install surveillance devices. In order to justify the use of surveillance devices, a school board needs to decide what the purpose is for having surveillance devices. The use of surveillance should serve specific and clearly articulated goals such as enhancing students' safety and deterring destructive acts against school property. The school might decide to install devices in response to a particular security problem in the school that requires the use of surveillance devices. There should, therefore, be reasonable and justifiable reasons for installing surveillance devices in schools. It should provide a solution to a problem and not simply be a quick fix solution or a knee-jerk reaction to some particular incident. Therefore, before opting for optical devices, school administrators need to consider other less intrusive means. It is also recommended that school boards consult the parent and student community when installing surveillance technology to ensure that the school community is informed about the purpose of the surveillance and to allay any fears or concerns about privacy issues and negative perceptions about 'big brother' watching.

B *System Design*

It is important for school boards to consider the type of system that is best suited to achieving the stated goals, to identify the appropriate locations for installing devices and to determine the operational times of the system. The design and operation of the system should present as little intrusion as possible and be sufficient to meet the stated goals. To this end it is recommend that the school board conduct a Privacy Impact Assessment to determine the degree of intrusiveness and the risk of breaching privacy rights. The more intrusive the surveillance devices are the greater the risk of breaching privacy rights. Monitoring physical areas of the school during times when there is little human activity, for example, after school hours, presents a very low risk while monitoring human activity in classrooms presents a higher risk. Therefore, the reasonable use of overt surveillance devices to monitor certain physical areas of the school such as car parks and laboratories is not uncommon and is low risk. However, the use of surveillance devices in more private areas of the school where there is a reasonable expectation of privacy such as classrooms, the staffroom, offices, meeting rooms and school locker areas presents a higher risk and is more intrusive. This is illustrated in the following risk-assessment diagram.



At the very high-risk end of the scale is the use of surveillance devices in areas such as toilets and changing rooms. Generally the use of surveillance devices in such areas would be prohibited. However, would a school be able to install a device in a cloakroom or at the entrance of toilet blocks in an attempt to reduce serious acts of drug use and bullying in the interest of student's safety?

C *Consent and Notification*

Covert surveillance, that is surveillance without notification or consent, is generally not acceptable. School boards should obtain the consent of the relevant parties prior to installing and using surveillance devices. In gaining consent, it is necessary to explain why the surveillance device is being used, what the school will do with the data and what security measures are in place to protect data. Generally, it is expected that parents would need to give consent to their children being monitored and recorded. Consent may be express or implied. Express consent is given explicitly, either orally or in writing. Implied consent arises where consent may be inferred from the circumstances. However, in order to ensure legal certainty and clarity, consent should preferably be express and in writing. Although consent could possibly be inferred from parents signing a school safety and discipline policy, in the absence of any clear provisions on the use of surveillance systems in the policy, parents may not be consenting to their children being viewed and recorded by webcams or other cameras. It is advisable for schools to address issues of consent and access to personal information in a school surveillance policy.

Although the *Surveillance Devices Act* (WA) is silent on the issue of notification, it is recognised that it is good practice to display reasonable and adequate warning signs to notify people that surveillance devices are in operation. There may be situations where it may be acceptable to use covert surveillance and not have warning signs, for example, in areas of a school that have been the target of repeated criminal and destructive acts.

D *Data Management*

Another important aspect of surveillance technology and protection of personal information is the management of the recorded and stored data. Privacy legislation regulates the way in which personal data is collected and used. It has already been noted that data recorded via surveillance cameras and webcams constitutes personal data. A school policy would need to provide clear guidelines for collecting, using, storing and accessing data. Consideration needs to be given to how the data will be stored, who will be responsible for managing the data and who will have access to the data. Recorded data must be kept in a safe and secure place and that access should be limited to a few authorised personnel. Data should be kept for a defined period and thereafter destroyed in an appropriate manner. Schools need to ensure that electronic records are permanently removed as mere deletion from a file does not necessarily remove all traces of the record.

The data that is recorded and stored may only be collected and used for the purpose stated in the policy. Furthermore, the individuals on whom the data is collected and stored should be entitled to access the data, which may be limited by the law. The policy should also set out the procedures for individuals to whom the data relates to gain access to the data, and should comply with relevant legislation. For instance, the *Freedom of Information Act 1992* (WA)[32] gives people the right to access documents held by a government agency, which includes schools under the education department, subject to a number of exemptions. Documents include written material, photographs, tape recordings, films, videotapes and information stored in a computerised form. Some documents may be exempt, for example, documents relating to the protection of public interest or privileged documents.

IV Conclusion

Schools worldwide are faced with the challenge of maintaining safe and orderly school environments. Technology presents schools with some solutions to monitor and control the school environment with a view to reducing criminal and destructive acts on and against school property. Webcams are a relatively cheap and effective way of keeping a school under constant watch. However, while webcams may appear to be a very useful monitoring tool they also raise concerns about the impact they may have on people's privacy. Webcams will gather data that is personal and sensitive, and not necessarily easy to secure. Schools also have to be cautious about the unintended consequences of using such technology to keep schools safe. If schools intend using technology such as webcams to enhance school safety and discipline, they should have a very clear and comprehensive policy that governs its use and implementation, and above all the protection of personal data. School boards must also be aware of their liabilities and responsibilities if there is a breach of privacy.

Endnotes

1. It is beyond the scope of this article to provide a comprehensive and systematic discussion on privacy law in Australia and surveillance technology law in all the States and Territories.

2. In the USA, for example, there was a notable increase in the use of surveillance technology following the Columbine High School shooting in April 1999 in which 12 students and a teacher were killed. It is also reported that the St Petersburg School District has spent US $3 million installing surveillance cameras in schools. Other incidents of horrific school shootings and incidents of serious crime have given further impetus to the use of surveillance technology. Thomas Tobin, 'Schools find benefits, limits to surveillance' *St Petersburg Times online* (Tampa Bay) 16 April 2005 <www.sptimes.com/2005/04/16/news_pf/Tampabay/Schools_find_benefits.shmtl> at 29 July 2005.
3. Department of Education and Training, Western Australia, *Faculties and Services: Security and School Watch* (2005) <www3.eddept.wa.edu.au/facilitiesandservices/default.cfm> at 8 August 2005.
4. Information provided by Mr John Marrapodi, Head of Security, Department of Education and Training, Western Australia 8 August 2005.
5. Government of South Australia, Media Release, 'School Security' 11 July 2005 <www.ministers.sa.gov.au> at 19 August 2005.
6. Peter Christie, 'Safety in the city: some insights from a school in the Sydney CBD' In: *Innovation & internationalism: pushing the boundaries of law.* Proceedings of the ANZELA 13th Annual Conference, Wellington, New Zealand 22-24 September 2004.
7. Channel Nine, *A Current Affair* 17 August 2005.
8. Webcams need to be connected to a suitably equipped computer that is itself connected to the Internet or network. Netcams are special forms of webcams that connect directly to the Internet or network without the need for a separate computer. In this article webcam is used to refer to both types.
9. There are various 'nanny-cams' available on the market. GuardianCam is one system that enables parents to monitor their children in childcare <www:guardiancam.com>. See also Michelle Woo, 'Webcams at day care ease parents' concerns' *USA Today* 18 October 2004 <http://www.usatoday.com> at 2 August 2005.
10. It is reported that at Livingston Middle School in Tennessee, a camera was placed in the girls' and boys' locker-room because school administrators were concerned that students were sneaking out of gym. The cameras were pointed at doors leading outside, but the wide-angle lens took images of children changing their clothes. The pictures were accessed over the Internet because access codes had not been changed. A lawsuit against the Overton County School Board is pending. See also Phyllis Emert, 'Cameras in the classrooms: snooping or security?' *The Legal Eagle* (2004) <http://www.njsbf.com/njsbf/student/eagle/winter04-2.cfm> at 28 July 2005. In this case, parents have filed a lawsuit in the US District Court in Nashville and the parents are asking for $4.2 million in damages <http://www.tennessean.com/education/archives/03/07/35281568.shtml> at 3 August 2005.
11. Greg Toppo, 'Classroom webcams offer cheap, easy surveillance' *USA Today* 11 August 2003.
12. The author contacted the Superintendent of the Biloxi School District in order to obtained current information on the use and success of the webcams in Biloxi schools but has received no reply.
13. Dominique Braggs, 'Webcams in the classroom: How far is too far?' (2004) 33(2) *Journal of Law and Education* 275.
14. Toppo, above n 11, 1.
15. Braggs, above n 13, 275.
16. British Columbia Civil Liberties Association, 'Video surveillance in public schools: a position of the British Columbia Civil Liberties Association' <www.bccla.org/positions/privacy/03schoolvideo.html> at 2 June 2005.
17. See Article 8 of the *European Convention on Human Rights*; section 14 of the *South African Bill of Rights*; and the Fourteenth Amendment of the *USA Constitution*, which has been interpreted to include a general right to privacy.
18. The Australian High Court decision in *Victoria Park Racing Recreation Grounds Co Ltd v Taylor* (1937) 58 CLR 479 is generally cited for this position.
19. In *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2002) 208 CLR 1999, which addressed the issue of whether the secret and unlawful filming of operations at a possum processing factory was grounds for granting an injunction to prevent the ABC from broadcasting the film, the

court considered the general right to privacy at common law. Although there was much discussion on the issue of privacy, the High Court left open the question of whether there is a general right to privacy. The court left open the possibility of a new tort of invasion of privacy. However, if such a tort were recognised it would be limited to natural persons and not corporations. See Jonathan Horton, 'Common law right to privacy moves closer in Australia' [2001] *Privacy Law and Policy Law Reporter* 62 <http://www.austlii.edu.au/au/journals/PLPR/2001/62.html> at 24 April 2006. It is also interesting to note that in the case of *Grosse v Purvis* [2003] QDC 151, a Queensland District Court judge recognised a tort of invasion of privacy. In this case, in which the defendant stalked and harassed the plaintiff, the plaintiff was awarded damages for breach of privacy rights. This judgment, however, is not binding on other courts or jurisdictions.

20. For a discussion on the concept of privacy see David Lindsay, 'An exploration of the conceptual basis of privacy and the implications for the future of Australian privacy law' (2005) 4 *Melbourne University Law Review*.
21. Law Book Company, *The Laws of Australia* Vol 21.4 (at) 21.4 Privacy [92].
22. Ibid, [92].
23. Australian Law Reform Commission, *Privacy* Report No 22, Vol 2 (1983) [1186].
24. The Australian Law Reform Commission recommended that 'public place' be defined as it is defined for police offences. Ibid, [1187]. It is interesting to note that the Criminal Code of Western Australia does not define 'public'.
25. Ackermann J in *Bernstein v Bester NO* 1996 (2) SA 751 (CC) 67.
26. La Forest J, *Thompson Newspapers Ltd v Canada* (1990) 47 CRR 1 cited in Johan De Waal, Iain Currie & Gerhard Erasmus (eds), *The Bill of Rights Handbook* (2001).
27. See the *European Union Data Protection Directive* UN Doc *95/46EC* (1995); *Personal Information Protection and Electronic Documents Act* 2000 (Canada); *Data Protection Act 1978* (France); *Personal Data (Privacy) Ordinance 1995* (Hong Kong) and the *Data Protection Act 1998* (UK).
28. *Privacy Act 1998* (Cth) Schedule 3. National Privacy Principle 10: Sensitive information includes personal information about racial origin, political and religious affiliations and sexual orientation.
29. Similar legislation may be found in other States, for example, the *Surveillance Devices Act 1999* (Vic); the *Listening and Surveillance Devices Act 1972* (SA) and the *Surveillance Devices Act 2000* (NT).
30. A 'protected person' is a person who has a mental impairment and cannot give consent to the use of an optical surveillance device, *Surveillance Devices Act 1998* (WA) s 27(4).
31. Although the Federal *Privacy Act 1988* (Cth) does not specify an age which individuals can make their own privacy decisions, guidelines to the National Privacy Principles provided by the Federal Privacy Commissioner, states that as a general rule 'a young person is able to give consent when he or she has sufficient understanding and maturity to understand what is being proposed'. <www.privacy.gov.au/publications/nppgl_01.html> at 16 August 2005.
32. The Federal *Freedom of Information Act 1982* (Cth) provides persons with a right to access documents held by a Commonwealth agency.