

Keeping Students and their Personal Information Safe from Predators, Parents, Teachers and Themselves

MICHAEL WINRAM

Michael Winram
Emil Ford & Co – Lawyers
580 George Street
SYDNEY 2000
(02) 9267 9800
lawyers@emilford.com.au
www.emilford.com.au

TABLE OF CONTENTS

| | |
|--|-----|
| ABOUT THE AUTHOR | iii |
| I. Protecting Students from Unauthorised Photographers..... | 1 |
| 1. The Problem..... | 1 |
| 2. The Non-existent Right to Privacy | 1 |
| 3. No Right Not To Be Photographed..... | 5 |
| 4. Introducing a Right to Privacy..... | 6 |
| 5. Privacy Act Protection? | 7 |
| 6. Amending the Privacy Act..... | 10 |
| 7. National Classification Scheme and Online Regulation..... | 11 |
| 8. Reforming the National Classification Scheme and Online Regulation..... | 14 |
| 9. Protection Currently Available in New South Wales | 15 |
| 10. Proposed Reform – Criminal Law | 17 |
| (a) Create a new criminal offence to deal with unauthorised use of photographs of children. | 17 |
| (b) Create a criminal offence to deal with voyeurism where an expectation of privacy exists. | 17 |
| (c) Enforcing the Criminal Law. | 20 |
| 11. The Creating of a Body to Oversee Children’s Rights | 20 |
| 12. Conclusion: What Can Be Done About Unauthorised Photographs?..... | 21 |
| II Withholding a Student’s Personal Information From Parents and Students..... | 22 |
| 1. The Problem: A Parent’s Authority or Student’s Instruction | 22 |
| 2. Privacy Act Basics | 23 |
| (a) Privacy Policy | 23 |
| (b) Collecting Information..... | 23 |
| (c) Using and Disclosing Personal Information Collected..... | 24 |
| (d) Access and Correction | 25 |
| 3. Can a Student Consent or Withhold Consent?..... | 25 |
| 4. Complying with a School Privacy Policy and Collection Notice | 26 |
| 5. A School’s Contractual Relationship with Parents..... | 27 |
| 6. Other Reasons to Deny Access | 28 |
| 7. Conclusion: The Privacy Commissioner’s advice. | 30 |
| III Withholding a Student’s Personal Information from Teachers | 31 |
| 1. KJ -v- Wentworth Area Health Service | 31 |
| (a) The Facts | 31 |
| (b) The Law | 32 |
| (c) Collection and Disclosure of Information..... | 33 |
| 2. Application to Private Schools and Organisations Under the Privacy Act... | 34 |
| 3. How should Private Schools Use and Disclose Information? | 36 |
| 4. A Procedure for Deciding to Whom to Distribute Information..... | 38 |
| 5. Conclusion | 40 |

ABOUT THE AUTHOR

Michael Winram is a lawyer at Emil Ford & Co - Lawyers in Sydney.

Michael practises mainly in commercial law with a particular focus on not-for-profit organisations including schools, charities and other religious organisations. Michael has advised numerous educational institutions on privacy issues.

Michael is a member of the Australian and New Zealand Education Law Association (ANZELA) and will be speaking at ANZELA's Annual Conference in Hobart in October, 2006.

I. Protecting Students from Unauthorised Photographers

1. The Problem

In February 2002 it was reported that a gay voyeuristic website contained pictures of Melbourne schoolboys.¹ The schoolboys were in public places engaged in a variety of sporting activities such as rowing and playing football. In April 2002 Yahoo! shut down a sports fetish website that contained unauthorised photographs of a 16-year-old male surf lifesaver.² In January 2004 police raided the house of a man who had been taking inappropriate photographs of children on Sydney's northern beaches.³ Inspector Robert Duncan stated:

*"We would ask people to be aware that it is becoming a more and more common occurrence...we get a lot of people doing that inappropriately."*⁴

As a result of the publication of unauthorised photographs appearing on voyeuristic websites, the Attorney-General, Philip Ruddock, is considering new laws to prohibit voyeuristic photography of children.⁵ This paper will consider the current laws that relate to unauthorised photography, the proposed law reform and the approaches of other common law countries.

2. The Non-existent Right to Privacy

In Australia there is no common law right to privacy. The High Court first articulated this position in *Victoria Park Racing -v- Taylor*⁶ where the owner of a racecourse sued the owner of an adjoining block of land for erecting a tower from which the owner of the adjoining block could view the entire racecourse and

¹ "USA:VIC gay website containing Melbourne schoolboys withdrawn", *Australian Associated Press*, 22 February, 2002; "Schoolboys counseled on net pics," *MX Newspaper*, 21 February 2002; Vic-Police powerless to act on gay website containing schoolboys", *Australian Associated Press* 22 February, 2002. Also reported in Standing Committee of Attorneys-General, *Unauthorised Photographs on the Internet and Ancillary Privacy Issues: Discussion Paper*, August 2005

² "Teen put on gay site may lead to camera ban" *Herald Sun*, 3 April, 2002.

³ "Beach snappers stalking young kids" *The Sun-Herald* 11 January, 2004

⁴ "Beach snappers stalking young kids" *The Sun-Herald* 11 January, 2004

⁵ "These photos may be illegal" *The Sydney Morning Herald*, 16 November, 2005

⁶ *Victoria Park Racing and Recreation Grounds Company Limited -v- Taylor* [1937] HCA 45; (1937) 58 CLR 479 (26 August 1937).

broadcast the results of each race over the radio. The broadcasts were so articulate that many people, who would ordinarily have attended the racecourse and paid the entry fee, preferred to stay at home and listen on the radio. The owner of the racecourse claimed that its privacy had been infringed by the defendant erecting the tower, viewing the racecourse and broadcasting the results of each race. On the issue of privacy, the High Court unanimously adopted the English position that there is no authority that shows that any general right of privacy exists and the owner of the racecourse could not use privacy laws to prevent the owner of the adjoining block from erecting the tower, viewing the racecourse and broadcasting the results of each race. Presumably, the Court's position would have been the same had the owner of the adjoining block taken photographs from the tower.

The High Court was invited to depart from *Victoria Park Racing -v- Taylor* in *ABC -v- Lenah*⁷ and declare that:

- (a) Australian law now recognises a tort of invasion of privacy; and
- (b) a tort of invasion of privacy is available to corporations as well as individuals.

The majority of judges left open the possibility of recognising an Australian tort of privacy but did not go so far as to establish such a tort. Gummow and Hayne JJ (with whom Gaudron J agreed) declared that *Victoria Park Racing -v- Taylor* did not stand in the path of the development of such a cause of action. Callinan J (dissenting) stated:

“It seems to me that, having regard to current conditions in this country, and developments of the law in other common law jurisdictions, the time is ripe for consideration whether a tort of invasion of privacy should be

⁷ *Australian Broadcasting Corp -v- Lenah Games Meats Pty Ltd* (2001) 185 ALR 1

recognised in this country, or whether the legislatures should be left to determine whether provision for a remedy for it should be made.”⁸

Even Gleeson CJ noted the observation of the former Chief Justice of the United States Supreme Court that:

“Technology now permits millions of important and confidential conversations to occur through a vast system of electronic networks. These advances, however, raise significant privacy concerns. We are placed in the uncomfortable position of not knowing who might have access to our personal and business e-mails, our medical and financial records, or our cordless and cellular telephone conversations.”⁹

However, it is unlikely that a tort of invasion of privacy will develop in the common law of Australia. Even if it does, it is some time off and it would not be prudent for schools, parents, students or anyone else to rely on its development. The reasons why it is unlikely that a tort of invasion of privacy will develop are as follows:

- (a) In his judgement in *ABC -v- Lenah*, Gleeson CJ concluded that the lack of precision in the concept of privacy is a reason for caution in declaring a new tort of invasion of privacy. He also noted that it would be especially difficult in the Australian Legal System because it has no counterpart to the First Amendment to the United States Constitution or the Human Rights Act 1998 of the United Kingdom. David Lindsay has commented that:

“while judicial recognition of an Australian tort of privacy would improve the position of individuals under the general law, an adequate regime must await the extra-judicial development of a bill of rights. As this seems unlikely, it would seem that protection of

⁸ *Australian Broadcasting Corp -v- Lenah Games Meats Pty Ltd* (2001) 185 ALR 1 per Callinan J at 335

⁹ *Bartnicki -v- Vopper* 69 USLW 4323 at 4331 (2001) Per Rehnquist CJ

*rights and freedoms under Australian Law is destined to be
influenced indirectly by developments elsewhere.”¹⁰*

- (b) As quoted above, Callinan J thought it was ripe to consider whether a tort of invasion of privacy should develop or whether the legislators should be left to determine a suitable remedy. However, although Kirby J in *ABC -v- Lenah* refrained from commenting on whether a tort of invasion of privacy should develop, in previous judgments he has stated: “*the result of legislative inaction is that no tort of privacy invasion exists.*”¹¹ This would indicate that at least Kirby’s J preference might be for legislators to determine a suitable remedy.
- (c) Gummow and Hayne JJ acknowledged in their judgment in *ABC -v- Lenah* that the preferable legal method is to look to the development and adaptation of recognised forms of action to overcome new privacy situations and circumstances. As an example, they list the following areas of law that could develop: injurious falsehood, defamation, confidential information and trade secrets, passing-off, the tort of conspiracy, the developing tort of harassment and the action on the case for nuisance.¹² In their case note, Greg Taylor and David Wright concluded that *Lenah* would have succeeded had it argued for the development of the law of confidential information rather than for the introduction of a new tort of privacy. They state:

“All this is particularly disappointing considering that the leading English Case, Argyll, had been referred to with approval by Mason J in an earlier High Court decision, that similar principles have been applied at State Supreme Court level, and that the UK

¹⁰ David Lindsay, *Protection of privacy under the general law following ABC -v- Lenah Game Meats Pty Ltd: Where to now?* [2002] PLPR 45

¹¹ *Australian Consolidated Press Ltd -v- Ettingshausen* unreported, Court of Appeal of New South Wales, 13 October 1993 per Kirby P at 15.

¹² *Australian Broadcasting Corp -v- Lenah Games Meats Pty Ltd* (2001) 185 ALR 1 per Gummow and Hayne JJ at 123

precedents indicate a sensible and logical way in which the law of Australia could be developed in a defensible and incremental fashion so as to provide protection in cases of egregious invasions of privacy. There would have been no need for the creation of a new tort, merely for an old principle to be slightly refashioned and UK precedents followed.”¹³

- (d) There are at least two superior court cases since *ABC -v- Lenah* which show a reluctance to recognise a tort of privacy. The Victorian Supreme Court in *Giller -v- Procopets*¹⁴ and the Federal Court in *Kalaba -v- Commonwealth of Australia*¹⁵ concluded that an Australian tort of privacy had not developed.

3. No Right Not To Be Photographed

Given the state of the common law, that there is no common law right to privacy, Dowd J was able to say resolutely in the criminal matter *R v Sotheren*:

“A person, in our society, does not have a right not to be photographed...clearly, the action of taking the photograph was not in contravention of an Australian law...”¹⁶

It was surprising, therefore, to hear Police Sex Crime Squad Manager Detective Chief Inspector Bob Sullivan declare publicly that it was illegal for people to take unauthorised video footage or still photographs of children. The statement was made after police raided the house of a man they suspected was taking inappropriate photographs of children on Sydney’s northern beaches. He said:

“It is an offence to be there [the beach] without a proper excuse, videotaping or filming children.”¹⁷

¹³ Greg Taylor and David Wright, *Australian Broadcasting Corporation -v- Lenah Game Meats, Privacy, Injunctions And Possums: An Analysis of the High Court’s Decision*, [2002] MULR 36

¹⁴ *Giller -v- Procopets* [2004] VSC 113

¹⁵ *Kalaba -v- Commonwealth of Australia* [2004] FCA 763

¹⁶ *R -v- Sotheren* [2001] NSWSC 204 per Dowd J

In fact, that would only be true if the photographer had already been convicted of a child related offence and the Local Court had made a child protection prohibition order under the *Child Protection (Offenders Prohibition Orders) Act 2004* prohibiting the photographer from taking photographs of children.

4. Introducing a Right to Privacy

Although the current High Court is unlikely to introduce a tort of privacy, the government could introduce one. The *International Covenant of Civil and Political Rights (1966)* states that:

1. “No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home, or correspondence, nor to unlawful attacks on honour and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks.”¹⁸

Although Australia is a party to the International Covenant on Civil and Political Rights, the federal government has not used it as an opportunity to introduce a tort of invasion of privacy.

Canada is also a party to the International Covenant on Civil and Political Rights. As a result Quebec introduced the Quebec Charter of Human Rights and Freedom. It states that a person has the right to respect for his or her private life. However, the same Charter also provides that the public have a right to be informed and the right to freedom of expression. In the Charter, the right to freedom of expression prevails over the right to privacy. So, the right to privacy is not absolute. For example, the Charter will not necessarily protect photographs of public figures being taken. However, in applying the Charter, the Supreme Court of Canada decided that photographs of students, even if fully clothed, could infringe that

¹⁷ Sean Berry, *Beach snappers stalking young kids*, The Sun-Herald, 11 January, 2004.

¹⁸ As quoted in Standing Committee of Attorneys-General, *Unauthorised Photographs on the Internet and Ancillary Privacy Issues: Discussion Paper*, August 2005

student's right to respect for his or her private life. In *Aubry -v- Editions Vice-Versa*¹⁹ the Supreme Court ruled that the publication of a photograph of a 17-year-old girl, sitting on a step outside a building in Montreal, taken without her consent, infringed that girl's right to respect for her private life. The 17-year-old girl had claimed that she had been subject to ridicule following the publication.

In the Standing Committee of Attorneys-General discussion paper on *Unauthorised Photographs on the Internet and Ancillary Privacy Issues*,²⁰ the Attorneys-General note the Quebec Charter but do not recommend that similar provisions be introduced in Australia. Further, the Australian Law Reform Commission ("ALRC") has recommended that a general statutory right to privacy should not be recommended in Australia. In effect, the ALRC does not recommend that a counterpart to the Quebec Charter, the First Amendment of the United States or the Human Rights Act 1998 of the United Kingdom be implemented in Australia. Rather the ALRC proposed that detailed and specific legislation be enacted that would define the values to be protected, the circumstances of the protection and the defences that would be available.

5. Privacy Act Protection?

The *Privacy Act 1988* (Cth) does not introduce a right to privacy in Australia. Rather, it regulates the collection, storage, use and disclosure of personal information. Its scope is narrow. It does not apply to individuals who, acting in a private capacity, take photographs of another person without their consent. The Privacy Act applies to:

- (c) Commonwealth and Australian Capital Territory government agencies;
- (d) Credit providers and reporting agencies; and

¹⁹ *Aubry -v- Editions Vice-Versa* [1998] SCR 591

²⁰ Standing Committee of Attorneys-General, *Unauthorised Photographs on the Internet and Ancillary Privacy Issues: Discussion Paper*, August 2005

- (e) Organisations that are not small businesses. Small businesses are businesses that have an annual turnover of \$3,000,000.00 or less unless the small business provides a health service or holds any health information (except information contained in an employee record).²¹

Accordingly, there are many organisations to which the Privacy Act does not apply. The Privacy Act applies to most private schools because most private schools provide a health service (if they have a sick bay or registered nurse on campus) or hold health information about students.

The information that the Privacy Act regulates is:

- (a) **Personal information**, which is information or an opinion, 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.²²
- (b) **Health information**, which is information or an opinion about;
 - (i) the health or disability of an individual,
 - (ii) an individual's express wishes about the future provision of health services; or
 - (iii) a health service to be provided to an individual;that is also **personal information**.²³
- (c) **Sensitive information**, which is **health information** or information about an individual's;
 - (i) Racial or ethnic origin;

²¹ s6D, *Privacy Act 1988* (Cth)

²² s6, *Privacy Act 1988* (Cth)

²³ s6, *Privacy Act 1988* (Cth)

- (ii) Political opinions;
- (iii) Membership of a political association;
- (iv) Religious beliefs or affiliations;
- (v) Philosophical beliefs;
- (vi) Membership of a professional or trade association;
- (vii) Membership of a trade union;
- (viii) Sexual preferences or practices; or
- (ix) Criminal record;

that is also **personal information**.²⁴

Further, the Privacy Act only applies to personal information that is contained in a ‘record.’²⁵ A record includes a photograph or other pictorial representation of a person.²⁶ A photograph will contain personal information if it is possible to identify the individual in the photograph. A photograph may contain health information. For example, if a photograph contains a student in a wheel chair, that photograph will contain health information about that student’s disability. A photograph may also contain other sensitive information. For example, a photograph of a student praying may reveal information about the student’s religious beliefs or affiliations.

Although the Privacy Act does not protect students from being photographed by individuals, it does protect students from being photographed by schools and other organisations to which the Privacy Act applies. If the Privacy Act applies, it compels schools or other organisation to comply with the National Privacy

²⁴ s6, *Privacy Act 1988* (Cth)

²⁵ s16B, *Privacy Act 1988* (Cth)

²⁶ s6, *Privacy Act 1988* (Cth)

Principles.²⁷ The National Privacy Principles regulate the collection, storage, use and disclosure of personal information. As a photograph of a student is considered by the Privacy Act to be a record that contains personal information, the school or organisation would have to provide a notice to the individual of its taking of the photograph. In some circumstances, the school or organisation would have to obtain the consent of the individual being photographed (for example, if the photograph were to contain sensitive information). The photograph could then only be used for the purpose for which it was taken or a related secondary purpose which is within the individual's reasonable expectations.

If the school or organisation does not notify the individual that it is taking a photograph, and if the school or other organisation uses the photograph other than for the purpose for which it was taken or a related secondary purpose, the individual could refer the matter to the Privacy Commissioner for investigation. Therefore, if a student or a school discovers unauthorised photographs on another organisation's website, and there is reason to believe that the Privacy Act applies to the internet host, the student or school could refer the matter to the Privacy Commissioner for investigation.

6. Amending the Privacy Act

The Privacy Commissioner has reviewed the adequacy of the Privacy Act and its application in light of new technologies, such as the internet.²⁸ The Privacy Commissioner noted that individuals acting in their personal capacity now have the ability to invade the privacy of other individuals. The Commissioner thought that the government should consider changing the Privacy Act so that it could cover activities of private individuals. The Commissioner noted:

²⁷ s16A, *Privacy Act 1988* (Cth)

²⁸ Office of the Privacy Commissioner, *Submission to the Standing Committee of Attorneys-General*, November, 2005

“It is worth reflecting that there did not appear to be a great deal of support from submissions to the Review, or in consultations undertaken by this Office during the Review, for changing the Privacy Act so that it could cover the activities of private individuals in their personal capacity. For example, in its submission to the Review, the Australian Consumers’ Association expressed the view that controlling individual behaviour is best left to social norms backed by general or specific laws.”²⁹

7. National Classification Scheme and Online Regulation

Although the common law and the Privacy Act will not always protect students from unauthorised photographers, other federal legislation may assist.

- (a) **National Classification - *Classification (Publications, Films and Computer Games) Act 1995 (Cth)***. This Act established the national classification scheme. The national classification scheme is a cooperative arrangement between the Commonwealth, States and Territories and is administered by government ministers from each jurisdiction. The scheme establishes the Classification Board which classifies films, computer games and other publications. The Classification Board also provides classifications to the Australian Communications and Media Authority (ACMA) on internet content.

The Classification Board is made up of members who are supposed to broadly represent the Australian community. The board has a moral authority; section 11 of the Act requires the Classification Board to take into consideration various matters including the standards of morality, decency and propriety generally accepted by reasonable adults.³⁰ Further, the Classification Board must make its decisions in accordance with the National Classification Code which is approved by the Commonwealth,

²⁹ Office of the Privacy Commissioner, *Submission to the Standing Committee of Attorneys-General*, November, 2005

³⁰ s11, *Classification (Publications, Films and Computer Games) ACT 1995 (Cth)*

State and Territory Ministers responsible for the scheme. For example, the National Classification Code classifies films as G, PG, M, MA15+, R18+, X18+ and RC. RC, which stands for ‘Refused Classification,’ applies to the classification of films, publications and computer games. If a publication, film or computer game is given an RC classification, that publication, film or computer game is banned. The definition of RC includes material that:

“describe or depict in a way that is likely to cause offence to a reasonable adult, a person who is, or appears to be, a child under 18 (whether the person is engaged in sexual activity or not)”³¹

Therefore, if material involving students under 18 is depicted in a way that would be offensive to a reasonable adult, that material may be given an RC classification by the Classification Board. For example, a book containing students in their underwear or in swimming costumes may, in particular circumstances and contexts, cause offence to a reasonable adult and be given an RC classification which would prevent its publication.

Further, the Classification Board has, in the past, classified an image of a five year old child fully clothed on a web page as RC because the URL of that webpage was offensive.³² The Attorneys-General, in their discussion paper³³, note that although an innocent photograph of a child on a web site with a link titled ‘sex with boys pics’ would be classified RC, the Classification Board would not be able to take into account the content of a linked web page if the link were merely titled ‘more pics’ (even if the linked web site contained child pornography).

³¹ *National Classification Code*, available at
<<http://www.oflc.gov.au/resource.html?resource=60&filename=60.pdf>>

³² Standing Committee of Attorneys-General, *Unauthorised Photographs on the Internet and Ancillary Privacy Issues: Discussion Paper*, August 2005

³³ Standing Committee of Attorneys-General, *Unauthorised Photographs on the Internet and Ancillary Privacy Issues: Discussion Paper*, August 2005

- (b) **Internet Regulation – *Broadcasting Services Act 1992 (Cth)*.** Schedule 5 of this Act established a regulatory scheme to deal with internet content. The scheme is administered by the ACMA. The Act prohibits the following internet content:
- (i) content which is or would be classified RC or X18+ by the Classification Board; and
 - (ii) content which is or would be classified R18+, hosted in Australia and not subject to a restricted access system which complies with the criteria determined by the ACMA.

Interestingly, the Act does not make it an offence to host prohibited content. An offence is only committed if the host fails to comply with a take-down notice. The scheme establishes the following system:

- (i) Members of the public can make complaints about internet content to the ACMA if it would be prohibited content under the Act.
- (ii) The ACMA refers the internet content to the Classification Board for a classification decision.
- (iii) If, before the Classification Board makes a decision, the ACMA suspects that the internet content will be prohibited content, it can issue an interim take-down notice which requires the internet host to remove the content until it has been classified by the Classification Board.
- (iv) If the Classification Board classifies the internet content as prohibited content, the ACMA will issue a take-down notice to the internet host.
- (v) The internet host must comply with any take-down notice issued by the ACMA as soon as possible and at least before 6pm the next

business day. The internet host is guilty of an offence if it does not comply with a take-down notice. The penalty is 50 penalty units which is \$5,500.00.

- (vi) The ACMA may then apply to the Federal Court for an order that the person cease supplying internet carriage services or cease hosting internet content.
- (vii) If the internet content is not hosted in Australia, the ACMA will notify the suppliers of approved internet filters. If the internet content is sufficiently serious (for example, child pornography), the ACMA may refer the internet content to law enforcement agencies in the internet host's jurisdiction.

8. Reforming the National Classification Scheme and Online Regulation

One of the major problems with the National Classification Scheme is that the Classification Board does not consider the privacy of the people in the photographs, the purpose of the photographs or how the photographs were obtained. Rather the Classification Board objectively considers the image and determines whether it would be likely to offend a reasonable adult. Further, the Classification Board is not able to take into consideration the content of a linked web page. The Attorneys-General, in their discussion paper³⁴, have suggested that the Classification Board be given power to look at the broader context of images on web pages. That is, the Attorneys-General suggest that the Classification Board be able to consider linked sites.

It is possible that, had the Melbourne schoolboy rowers complained to the ACMA about their photographs on the internet, the Classification Board would have classified the photographs as offensive to the reasonable adult. The ACMA would then have been able to issue a take-down notice. However, the Attorneys-

³⁴ Standing Committee of Attorneys-General, *Unauthorised Photographs on the Internet and Ancillary Privacy Issues: Discussion Paper*, August 2005

General have noted that this mechanism was not used by the Melbourne schoolboy rowers. As a result, the Attorneys-General have suggested an education campaign to make the community and police aware of the existing mechanisms for making complaints about internet content. The Office of the Privacy Commissioner has endorsed an education campaign.

9. Protection Currently Available in New South Wales

The following Acts in New South Wales may be of assistance in preventing unauthorised photographs being taken and used in a manner that might cause students distress:

- (a) ***Summary Offences Act 1988 (NSW) – Indecent Filming or Photographing.*** Section 21G of this Act prohibits a person from filming or taking photographs of another person to provide sexual arousal or sexual gratification if the person being photographed:
 - (i) is undressed or engaged in a **private act** in which a reasonable person would expect privacy; and
 - (ii) does not consent to being filmed or photographed.

A person is only engaged in a **private act** if the person is using the toilet, showering or bathing, carrying on a sexual act of a kind not ordinarily done in public or any other like activity. While this legislation might prevent a school sporting coach or other person from taking photographs of students in a locker room, it does not prevent people taking photographs of students at sporting events or in other public places. For example, this Act would not prevent photographs being taken of students at a rowing event because rowing in a public place is unlikely to be considered a private act.

This Act also prohibits a person from conducting themselves in an offensive manner in or near a public place or a school.³⁵ Although it has never been tested, the act of taking photographs of students is unlikely to be considered offensive unless those photographs are of the kind covered by Section 21G of the Act. For example, taking photographs of students at a school swimming carnival will not be considered offensive. It is the use to which photographs are put that usually causes distress.

- (b) **Crimes Act 1900 (NSW) – Stalking.** Section 562AB of the Act prohibits a person from stalking or intimidating another person *with the intention of causing the other person to fear physical or mental harm*. This section is of limited use because of the need to establish the intention of the stalker to cause the student to fear physical or mental harm. In many cases, a person who is taking photographs of students does not intend to cause the student to fear physical or mental harm.

Pornography. Section 91H of the Act makes it an offence to produce, disseminate or possess child pornography. Child pornography is material that depicts or describes, in a manner that would cause offence to reasonable persons, a person under the age of 16:

- (i) engaged in sexual activity,
- (ii) in a sexual context, or
- (iii) as the victim of torture, cruelty or physical abuse (whether or not in a sexual context).

This section will not protect students from having their photograph taken in contexts that are not sexual. For example, photographs of students taken at the beach or at a school swimming carnival will usually not be

³⁵ s4, *Summary Offences Act 1988* (NSW)

considered to be pornography. Further, many students are older than 16 years of age.

10. Proposed Reform – Criminal Law

(a) Create a new criminal offence to deal with unauthorised use of photographs of children.

The Attorneys-General, in their Discussion Paper, propose two alternatives to amend the criminal law:

- (i) That it be an offence to capture images of children that a reasonable adult is likely to consider:
 - (A) exploitative; or
 - (B) offensive; or
 - (C) for the purpose of sexual gratification.
- (ii) That it be an offence to post unauthorised photographs of children that are intended or excite or gratify sexual interest.

The advantage of the first alternative is that it is broad enough to capture people who take photographs, not just those who publish or use them. In the second alternative the element of sexual gratification would have to be present before there was an offence.

(b) Create a criminal offence to deal with voyeurism where an expectation of privacy exists.

The proposal of the Attorneys-General in their Discussion Paper is to pass laws similar to the proposed law in New Zealand, and the laws in the United Kingdom, and Canada. The New Zealand Law Commission

released a paper entitled *Intimate Covert Filming*.³⁶ The Commission recommended that the New Zealand criminal law be amended to make it an offence to make, publish or possess a voyeuristic recording. The penalty for making or publishing a voyeuristic recording is three years' imprisonment. The penalty for possessing a voyeuristic recording is only one year's imprisonment. The Commission recommended that the definition of a voyeuristic recording be:

- (i) A visual recording of another person without the knowledge or consent of that person when the person is in circumstances that would reasonably be expected to provide privacy, and is
 - (A) Nude or has his or her sexual organs, pubic area, buttocks, or her breasts exposed or partially exposed; or is
 - (B) Engaged in explicit sexual activity; or is
 - (C) Engaged in an intimate bodily activity such as using the toilet.
- (ii) A visual recording of another person without the knowledge or consent of that person under that person's clothing for the purpose of viewing their sexual organs, pubic area, buttocks, breasts or underwear in circumstances where it is unreasonable to do so.

The proposed New Zealand voyeuristic offence would not have protected the Melbourne schoolboy rowers whose picture appeared on a gay voyeuristic website. The voyeuristic offence involves a higher level of intimacy than taking photographs of schoolboys in swimwear in a public place. In fact, the New Zealand Commission decided not to widen the scope of the offence to include filming of people in public in non-intimate circumstances even if the purpose of filming was for sexual gratification.

³⁶ New Zealand Law Commission, *Intimate Covert Filming* Study Paper (2004)

Canada has also introduced legislation to amend the sexual offences part of its Criminal Code. The legislation targets voyeurism as both a sexual offence and a privacy offence. The legislation makes it an offence to surreptitiously observe or make a visual recording of a person in circumstances that give rise to a reasonable expectation of privacy where it is done for a sexual purpose. It is likely that this legislation would capture the person who took the photographs of the Melbourne schoolboy rowers if the photographs were taken for a sexual purpose. However, the schoolboys would have to prove that the photographer had invaded a reasonable expectation of privacy.

In the United Kingdom, the Sexual Offences Act 2003 makes it an offence to:

- (i) observe a person doing a private act for the purpose of obtaining sexual gratification;
- (ii) operate equipment with the intention of enabling a third party, for the purpose of sexual gratification, to observe a person doing a private act;
- (iii) record a person doing a private act if the recording is to enable a third person to obtain sexual gratification

and the person observed does not consent to being observed.

Section 67 of the Sexual Offences Act 2003 states that a person is doing a private act if the person is in a place which, in the circumstances, would reasonably be expected to provide privacy, and:

- (i) the person's genitals, buttocks or breasts are exposed or covered only with underwear,
- (ii) the person is using a lavatory, or

- (iii) the person is doing a sexual act that is not of a kind ordinarily done in public.

However, this act would not protect the Melbourne schoolboy rowers because it is unlikely that rowing in a public place would be considered a place which a person would reasonably be expected to provide privacy.

(c) Enforcing the Criminal Law.

If the two new criminal offences referred to above were to be introduced, there would have to be an appropriate way to have inappropriate content removed from internet web sites. The Attorneys-General, in their discussion paper, recommend that it be made clear that take-down notices be issued under the Broadcasting Services Act 1992 where the content or internet host provider has contravened the new criminal offences.

11. The Creating of a Body to Oversee Children's Rights

The Attorneys-General have also suggested that the government consider creating a body to oversee children's rights. This suggestion arose out of an analysis of Dutch Copyright Laws.

The Netherlands experienced some problems with the trade of videos depicting naked children.³⁷ As the videos did not contain child pornography, the Dutch Criminal Code did not provide a remedy for the children and their carers. As a result, the government introduced amendments to the Dutch Copyright Act to provide both civil and criminal responses to the issue. The intention of the legislation was to eradicate videos made without the parent's or child's consent. More specifically, legislation was supposed to prevent videos and photographs being taken of children on beaches, whether or not the children were naked.

³⁷ United Nations, *Initial reports of States parties due in 1997: Netherlands* (1997); also reported in Standing Committee of Attorneys-General, *Unauthorised Photographs in the Internet and Ancillary Privacy Issues*, Discussion Paper, August, 2005.

The civil provisions are contained in section 21 of the Dutch Copyright Act. Section 21 makes it an offence to publish a portrait of a person, made without commission, if it would be contrary to the reasonable interest of the person shown in the portrait. In the example of the Melbourne schoolboy rowers, it is likely that it would be contrary to the reasonable interest of the schoolboys to have their portrait published on a gay voyeuristic website. Under the Dutch Copyright Act, the parents or child could apply to the civil courts for an injunction preventing the publication of the portraits. The parents and the child could also ask for an injunction requiring the publisher to destroy all copies of the portrait.

The criminal provisions are contained in section 35 of the Dutch Copyright Act. Section 35 makes it an offence to publicly exhibit or otherwise publish a portrait without being entitled to do so. The person bringing the action has to prove that there is a reasonable interest in preventing the publication. The Attorneys-General, in their discussion paper, note that a problem with this is that evidence proving that there is a reasonable interest in preventing the publication of a portrait would usually come from the people contained in the portrait. This is problematic if the people in the portrait cannot be identified.

The Attorneys-General note that it would be inappropriate to amend Australian Copyright Laws because Australian Copyright laws protect the intellectual property in a creative endeavour and can only provide remedies for acts that are connected to infringements of intellectual property rights. As an alternative, the Attorneys-General suggest that, for example, a Commissioner for Children be given the role of protecting children's reasonable interest with regard to unauthorised photographs.

12. Conclusion: What Can Be Done About Unauthorised Photographs?

There is currently no law prohibiting an individual from taking a photograph of another person unless the person being photographed is using the toilet, showering or bathing, carrying on a sexual act of a kind not ordinarily done in public or any other like activity and the person taking the photograph is doing so

for sexual arousal and gratification. If a school suspects that inappropriate photographs are being taken of its students, there is nothing preventing the school from approaching the photographer and asking the photographer to stop taking photographs. If the photographer continues to take photographs, the only recourse for the school is to call the police who could charge the photographer for nuisance. Schools could also adopt the position of Surf Life Saving Tasmania and require photographers at school events to register with the school – this would include parents who wish to take photographs of their own children.³⁸

If a school suspects that photographs are being taken by an organisation to which the Privacy Act applies, the school could report the organisation to the Privacy Commissioner for investigation. Schools should ensure that when they take photographs of students, they comply with the National Privacy Principles. If a school, or student, discovers unauthorised photographs on a website, the school, or student, could ask the ACMA to arrange for the site to be classified by the Classification Board, and request that an interim take-down notice be issued before a determination is made.

II Withholding a Student’s Personal Information From Parents and Students

1. The Problem: A Parent’s Authority or Student’s Instruction

The Privacy Act does not distinguish between adults and children. As a result, children have some rights when it comes to the collection, storage, use and disclosure of their personal information. Schools often collect personal information about students from a student’s parents. Schools also collect personal information about students from students themselves. What should schools do if a parent demands that a school provide him or her with access to personal information about their child but the student objects? If a student requests access to personal information that the school holds about him or her, how should the school respond?

³⁸ “Lifesavers Sharpen Focus on Photographers as Beach” *Surf Lifesaving Australia News*, 2 February, 2006.

2. Privacy Act Basics

As already noted, the Privacy Act regulates the collection, storage, use and disclosure of personal information. If the Privacy Act applies, Section 16A requires schools to comply with the National Privacy Principles (NPPs). There are 10 NPPs that are contained in Schedule 3 to the Privacy Act.

(a) Privacy Policy

NPP 5 states that a school must set out in a document clearly expressed policies on its management of personal information. This document is usually referred to as a school's privacy policy. The privacy policy must be made available to anyone who asks for it. Further, a school must, on request by a person, take reasonable steps to let that person know what sort of personal information it holds, for what purposes, and how it collects, holds, uses and discloses that information.

(b) Collecting Information

In addition to the requirement to have a privacy policy, NPP 1.3 states that at or before the time the school collects information about an individual, it must take reasonable steps to ensure that the individual is aware of:

- (i) the identity of the school and how to contact it;
 - (ii) the fact that he or she is able to gain access to the information;
 - (iii) the purpose for which the information is collected;
 - (iv) the organisations (or types of organisations) to which the school usually discloses information of that kind;
 - (v) any law that requires that particular information to be collected;
- and

- (vi) the main consequences for the individual if all or part of the information is not provided.

To comply with NPP 1.3, many schools have a collection notice which contains all the information required by NPP 1.3 and is usually given to parents and students on enrolment.

(c) Using and Disclosing Personal Information Collected.

The NPPs regulate how a school, to which the Privacy Act applies, should use and disclose the personal information it collects. Generally, schools should only use and disclose personal information for the primary purpose of collection.³⁹ A school's primary purpose in collecting personal information is usually to provide schooling. It is possible to argue that disclosing personal information about a student to a student's parent is part of providing schooling to that student. However, this is not always going to be the case and should be weighed against a student's right under the Privacy Act to control his or her personal information.

There are only limited circumstances in which a school can use and disclose personal information other than for the primary purpose of collection. Some of those circumstances listed are if:

- (i) the use and disclosure is for a secondary purpose related to the primary purpose and the individual (usually the student) would reasonably expect the school to use or disclose the information for the secondary purpose; for example, the Privacy Commissioner believes that most students would reasonably expect that school reports would be provided to parents;⁴⁰
- (ii) the individual has consented to the use or disclosure;

³⁹ NPP 2, Schedule 3, *Privacy Act 1988* (Cth)

⁴⁰ Office of the Federal Privacy Commissioner, "FAQs: Can Parents whose children attend a private school/college still get access to their children's school reports?" <<http://www.privacy.gov.au/faqs>>

(iii) the school reasonably believes the use and disclosure will lessen or prevent a serious and imminent threat to an individual's life, health or safety; and

(iv) the use or disclosure is required or authorised under law.

(d) Access and Correction

NPP 6 regulates who should be given access to the information that a school holds about an individual. It states that a school must provide the individual (which will usually be the student) with access to the information it holds about that individual on request, except in certain circumstances. This raises an issue as to whether a parent can request access to information held about that parent's child. The answer will depend on the student's maturity, the school's privacy policy and the contractual relationship between the school and the parent. The Privacy Act, and in particular the NPPs, do not take into consideration the unique relationship between schools, parents and students.

3. Can a Student Consent or Withhold Consent?

The Privacy Commissioner has stated that a young person can give consent or withhold consent if he or she has sufficient understanding and maturity to understand what is being proposed.⁴¹ A student who is 18-years-old will generally be considered to have sufficient understanding and maturity to understand what is being proposed. This principle is consistent with the current common law in Australia where parental power to consent diminishes gradually as the child's capacities and maturity grow.⁴² The rate of development will depend on the individual child.

⁴¹ Office of the Federal Privacy Commissioner, "*Guidelines to the National Privacy Principles*" September, 2001

⁴² *Secretary, Department of Health and Community Services -v-JMB and SMB* (1992) 175 CLR 218.

The Privacy Commissioner has indicated that in matters where a student, with the requisite understanding and maturity, withholds consent or asks the school to deal with his or her personal information in a certain way, the school should look to its privacy policy.⁴³

4. Complying with a School Privacy Policy and Collection Notice

A school's privacy policy should address issues of consent and rights of access to the personal information of students. A school should make clear in its privacy policy that parents may consent on behalf of students. The privacy policy should also cover how a school will respond to a student's request for access to his or her personal information. For example, the school's privacy policy could contain clauses like the following:

- (a) *The school respects every parent's right to make decisions concerning their child's education.*
- (b) *Normally, the school will refer any permission notices and other notices in relation to the personal information of a student to the student's parents. The school will treat consent given by parents as consent given on behalf of the students, and notice to parents will act as notice given to students.*
- (c) *The school may, at its discretion, on the request of a student, grant that student access to information held by the school about them, or allow a student to give or withhold consent to the use of their personal information, independently of their parents. This would normally be done only when the maturity of the student or the student's personal circumstances so warranted.*

These clauses cover some of the issues that the Privacy Act fails to recognise in the unique relationship between a school, parents and students. First, clause (a)

⁴³ Office of the Federal Privacy Commissioner, "Guidelines to the National Privacy Principles" September, 2001

above recognises the importance of the relationship between parents and child and the parents' right to make decisions concerning their child's education. Second, clause (b) above states that the school will primarily deal with parents in relation to the collection, use and disclosure of personal information about a student. This clause is also important because usually when a school accepts the enrolment of a student, the school enters into a contract with one or both of a student's parents or carers. The contract will usually require a school to keep a parent informed about the schooling of the student. Therefore, it is important for the school's privacy policy to acknowledge that, although students have some rights in relation to their personal information, parents also have a contractual right to be informed about the progress of their child's education.

Third, clause (c) above is drafted widely enough to give the school the discretion to decide whether or not to act on a student's instruction not to give parents access to that student's personal information. This discretion is important because there may be circumstances when a school will want to withhold personal information from a parent. For example, a school may not wish to send a school report home to a parent it suspects is abusive. Further, there may be circumstances where obtaining consent of parents is impractical or inconvenient. For example, a teacher may wish to take a photograph of a student to place on a classroom wall. It would be inconvenient to obtain the consent of a parent to the collection of a student's personal information in this way if the teacher was able to obtain consent from the student directly.

5. A School's Contractual Relationship with Parents

As already noted, the contractual relationship between a parent and a school is important when it comes to handling personal information of a student. Where a student's parents are separated, often only one parent will have taken responsibility for enrolling the student in the school and so only one parent will have signed the contract with the school (for example, the enrolment application and acceptance). A school is under no obligation to disclose personal information

to a parent who is not a party to the contract between the school and the student's other parent. However, the Privacy Commissioner has indicated that it will usually be in the student's reasonable expectation, and therefore permissible under the NPPs, for a school to disclose education related material to a non-residence parent even if that parent is not a party to the contract with the school.⁴⁴

6. Other Reasons to Deny Access

NPP 6 lists other reasons schools may deny access to students or parents to personal information it holds. Access can be refused if:

- (a) The information is not health information, and access would pose a serious and imminent threat to the life or health of any individual. For example, if a teacher has recorded that a boy informed the teacher that he is gay⁴⁵ and the school suspects that providing access to that information to that student's father would pose a serious and imminent threat to the life or health of the student, the school could refuse access to that information.
- (b) The information is health information, and access would pose a serious threat to the life or health of any individual.
- (c) Access would have an unreasonable impact upon the privacy of other individuals. For example, if an incident at school which involves a number of students is recorded in an Incident Report that contains the personal information of a number of students, a school could only give access to those parts of the report which relate to that parent's child. That is, a school cannot disclose personal information about a student to another student or to another student's parent.

⁴⁴ Office of the Federal Privacy Commissioner, "*Can non-custodial parents whose children attend a private school/college still get access to their children's school reports?*" <<http://www.privacy.gov.au/faqs>>

⁴⁵ Information about the sexual orientation of a student is classified as "sensitive information" in section 6 of the *Privacy Act 1988* (Cth)

- (d) The request for access is frivolous or vexatious.
- (e) The information relates to existing or anticipated legal proceedings between the school and the student or the student's parents, and the information would not be accessible by the process of discovery in the proceedings.
- (f) Providing access would reveal the intentions of the school in relation to negotiations with the student or the student's parents in such a way as to prejudice those negotiations.
- (g) Providing access would be unlawful.
- (h) Denying access is required or authorised by law. For example, the Family Court may order that access to a student's personal information be denied to a particular parent.
- (i) Providing access would be likely to prejudice an investigation of possible unlawful activity. For example, the school, or police, may be investigating an allegation of abuse by a teacher. A school could deny access to a parent to personal information about the student if providing access would prejudice the investigation. In some circumstances the investigator will need to interview a parent or the student. The outcome of that interview may be altered if the person is given access to personal information collected during the investigation.
- (j) Providing access would be likely to prejudice the work of a law enforcement body.
- (k) Providing access would be likely to cause damage to the security of Australia.
- (l) Providing access would reveal evaluative information generated within the school in connection with a commercially sensitive decision-making

process. In this case, the school may give an explanation of the commercially sensitive decision rather than give direct access to the information. This is particularly important if schools are compiling data and classifying students in certain categories for the purpose of making decisions about a student's education or place within the school.

It is important to note that if schools are going to deny access to parents or students, the NPPs require the school to provide reasons for the denial of access. Further, there is nothing preventing a school from charging a fee for access to personal information provided that those fees are not excessive.

7. Conclusion: The Privacy Commissioner's advice.

As a result of the failure of the Privacy Act to address the special relationship between schools, parents and students, the Privacy Commissioner has issued a number of statements on how the personal information of students should be handled by schools. It is important to note that many of the issues raised have not been tested in the courts. Although the Privacy Commissioner's opinions provide guidance, they are not necessarily authoritative.

The Privacy Commissioner has stated that only in exceptional circumstances will students be able to stop schools from providing reports to parents, including non-residence parents.⁴⁶ If a student requests that a report not be sent to his or her parent, the school would have to consider many things including:

- The school's privacy policy;
- The contractual relationship between the school and the student's parent;
- Whether the child has sufficient understanding and maturity; and

⁴⁶ Office of the Federal Privacy Commissioner, "*FAQs: Can Parents whose children attend a private school/college still get access to their children's school reports?*"; Office of the Federal Privacy Commissioner, "*Can non-custodial parents whose children attend a private school/college still get access to their children's school reports?*" <<http://www.privacy.gov.au/faqs>>

- The likely outcome of providing the report to the student's parent. For example, a school should consider whether providing a report to a student's parent would cause the student considerable anxiety. Further, a report should not be sent if there is a demonstrable risk to the child.

The Privacy Commissioner has also indicated that generally, non-education related material can be released to parents when it is in the reasonable expectation of the student.⁴⁷ However, schools must be mindful of the maturity and understanding of the student and weigh that up with the need for parents to be informed. In particular, if disclosure of a student's non-education related material will lessen or prevent a serious or imminent threat to a student's life, health or safety, information about that student could be disclosed to a parent.

III Withholding a Student's Personal Information from Teachers

1. KJ -v- Wentworth Area Health Service

In *KJ -v- Wentworth Area Health Service*⁴⁸, the Tribunal was asked to consider whether an organisation could pass personal information about an individual within that organisation.

(a) The Facts

KJ was a patient at Nepean Cancer Care Centre (NCCC) between 2000 and 2001. NCCC is a unit of Nepean Hospital which is part of the Wentworth Area Health Service. KJ was referred to NCCC by her General Practitioner. NCCC provided multi-disciplinary care. KJ was treated by a psychologist, psychiatrist, doctors, nurses, a dietician and a physiotherapist. NCCC kept a general medical file about KJ which contained information personal to KJ and, in particular, matters relevant to

⁴⁷ Office of the Federal Privacy Commissioner, "FAQs: Can private schools disclose non-education related personal information about students to their parents?" <<http://www.privacy.gov.au/faqs>>

⁴⁸ *KJ -v- Wentworth Area Health Service* [2004] NSWADT 84

her treatment. The psychologist and psychiatrist placed notes about their consultation with KJ on her general medical file.

(b) The Law

As the Wentworth Area Health Service is a public sector agency, the *Privacy Act 1988* (Cth) did not apply to it. The *Privacy and Personal Information Protection Act 1988* (NSW) regulates the collection, use and disclosure of personal information of public sector agencies in New South Wales. This Act applies to public schools in New South Wales. The New South Wales Act does not mirror the Privacy Act, but there are many similarities. Rather than the NPPs applying to the Wentworth Area Health Service, the Information Privacy Principles (IPPs) are applicable.

IPP 3 (which is also section 10 of the New South Wales Act) states:

“If a public sector agency collects personal information from an individual, the agency must take such steps as are reasonable in the circumstances to ensure that, before the information is collected or as soon as practicable after collection, the individual to whom the information relates is made aware of the following:

(a) the fact that the information is being collected,

(b) the purposes for which the information is being collected,

(c) the intended recipients of the information,

(d) whether the supply of the information by the individual is required by law or is voluntary, and any consequences for the individual if the information (or any part of it) is not provided,

(e) the existence of any right of access to, and correction of, the information,

(f) the name and address of the agency that is collecting the information and the agency that is to hold the information.”

IPP 12 (which is also Section 19 of the New South Wales Act) states:

“A public sector agency must not disclose personal information relating to an individual’s ethnic or racial origin, political opinion, religious or philosophical beliefs, trade union membership, health or sexual activities unless the disclosure is necessary to prevent a serious or imminent threat to the life or health of the individual concerned or another person”

(c) Collection and Disclosure of Information

KJ claimed that IPP 3(c) required the psychiatrist and psychologist to let her know who, within and outside Western Area Health Service, would receive and have access to the information they collected during sessions with her. She asserted that had she known her mental health records would have been available to doctors, nurses, a dietician and a physiotherapist, she would not have provided that information to her psychologist and psychiatrist.

KJ also claimed that Western Area Health Services was in breach of IPP 12 for disclosing her clinical records by having them available in her general medical file for her doctors, nurses, dietician and physiotherapist to see. She asserted that her mental health records should have been placed in a separate file that only the psychiatrist and psychologist could access. She also claimed that two doctors outside NCCC had been given access to her clinical records.

Western Area Health Services asserted that IPP 3 is concerned with the dissemination of information beyond the relevant agency to others. The Privacy Commissioner submitted that IPP 3 should not be read down in that way and submitted that the principle of openness requires that IPP 3 should apply to the dissemination of information within the relevant agency. The Tribunal agreed with the Privacy Commissioner and stated:

“In the absence of an express limitation, the provision of information to employees of the relevant Agency should not be considered as falling outside the scope of IPP 3. Such an artificial distinction is not consistent with the Privacy Act’s purpose of establishing principles for dealing with personal information in an open and accountable manner.”⁴⁹

In relation to IPP 12, the Tribunal stated:

“While generally speaking the expression “disclosure” refers to making personal information available to people outside an agency, in the case of large public sector agencies consisting of specialised units, the exchange of personal information between units may constitute disclosure.”⁵⁰

The Tribunal also stated that the type of information in issue is relevant in determining whether an organisation can disseminate personal information to employees. In this case, because the information was sensitive health information related to the mental health issues of KJ, the Tribunal decided that the psychiatrist’s and psychologist’s notes should have been kept in a separate file where other employees of Western Area Health Service would not have access.

2. Application to Private Schools and Organisations Under the Privacy Act

⁴⁹ *KJ -v- Wentworth Area Health Service* [2004] NSWADT 84 per Montgomery S at 33

⁵⁰ *KJ -v- Wentworth Area Health Service* [2004] NSWADT 84 per Montgomery S at 50

There are similarities between the New South Wales Act and the Federal Privacy Act. Both Acts aim to encourage organisations to deal with personal information in an open and accountable manner. The following table places IPP 3 and NPP 1.3 side by side. The table shows the similarities between IPP 3 and NPP 1.3.

| Information Privacy Principles, <i>Privacy and Personal Information Protection Act 1998</i> | National Privacy Principles, <i>Privacy Act 1988</i> |
|---|--|
| IPP 3: If a public sector agency collects personal information from an individual, the agency must take such steps as are reasonable in the circumstances to ensure that, before the information is collected or as soon as practicable after collection, the individual to whom the information relates is made aware of the following: | NPP 1.3: At or before the time (or, if that is not practicable, as soon as practicable after) an organisation collects personal information about an individual from the individual, the organisation must take reasonable steps to ensure that the individual is aware of: |
| (a) the fact that the information is being collected, | |
| (b) the purposes for which the information is being collected, | NPP 1.3(c): The purposes for which the information is collected. |
| (c) the intended recipients of the information, | NPP 1.3(d): The organisations (or types of organisations) to which the organisation usually discloses information of that kind. |
| (d) whether the supply of the | NPP 1.3(e): Any law that requires the |

| | |
|--|--|
| <p>information by the individual is required by law or is voluntary, and any consequences for the individual if the information (or any part of it) is not provided,</p> | <p>particular information to be collected. NPP 1.3(f): The main consequences (if any) for the individual if all or part of the information is not provided.</p> |
| <p>(e) the existence of any right of access to, and correction of, the information,</p> | <p>NPP 1.3(b): The fact that he or she is able to gain access to the information.</p> |
| <p>(f) the name and address of the agency that is collecting the information and the agency that is to hold the information</p> | <p>NPP 1.3(a): The identity of the organisation and how to contact it.</p> |

One of the main differences between the two provisions is between the IPP 3(c) and NPP 1.3(d). IPP 3(c) requires the organisation to make the individual aware of the intended “recipients” of the information whereas NPP 1.3(d) requires a school, to which the NPPs apply, to make the individual aware of the organisations, or types of organisations, to which the school usually discloses information of that kind. As a result, it is possible that private schools are not under an obligation to list all the people within the school’s community to whom the school will disclose the information. However, schools should not assume that they may simply distribute personal information collected about students to all employees or to others in a school’s community.

3. How should Private Schools Use and Disclose Information?

NPP 2 regulates the use and disclosure of personal information that a private school collects. NPP 2.1(a) states:

*“An organisation must not use or disclose personal information about an individual for a purpose (the **secondary purpose**) other than the primary purpose of collection unless:*

(a) both of the following apply:

(i) the secondary purpose is related to the primary purpose of collection and, if the personal information is sensitive information, directly related to the primary purpose of collection;

(ii) the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose.”

The guiding principle for a school is that it should only use or disclose personal information that it collects about a student for the purpose for which it was collected, or for a secondary purpose within the student’s reasonable expectation. The primary purpose of a school collecting personal information is usually to provide schooling. Schools could therefore assume that personal information collected for the purpose of providing schooling can be used and distributed by the school to teachers and other employees in a way that enables the school to provide schooling.

However, not all information a school collects relates to providing schooling. The following are examples of non-education related information that schools may collect:

- (a) Many schools employ a counsellor who counsel students on issues that students encounter in life outside of school. For example, issues relating to parents’ divorcing each other, the sexual preference of a student or past abuse.

- (b) Many schools have a registered nurse on campus or a sick bay. In the course of providing medical care to students, a school's nurse may collect certain health information, about a student.
- (c) Unfortunately, many schools have had to interview students in relation to allegations of abuse, whether or not the abuse was directed towards the student from whom the information was collected. When investigating allegations of abuse, schools naturally collect personal, and sometime sensitive and health information about a student.

4. A Procedure for Deciding to Whom to Distribute Information.

First, when deciding how personal information should be used or disclosed, a school should classify the information as either personal information, health information or sensitive information. The Tribunal in *KJ -v- Wentworth Area Health Service* stated the type of information is relevant when determining how to use and disclose the information. This will also be true for schools to which the Privacy Act 1988 (Cth) applies.

Second, a school should then refer to its privacy policy and collection notice to determine how it informed the student it would use and disclose the information it collected. Hopefully, the school's privacy policy and collection notice mirror the NPPs, and in particular NPP 2. The following are examples of determining to whom a school could disclose personal information.

- (a) If the information is merely personal information (that is, the information is not health information or sensitive information), the school may use and disclose the information for the purpose for which it was collected or for a secondary purpose related to the primary purpose where the student would reasonably expect the organisation to use and disclose that information for the secondary purpose. For example, details of the grades of a student may be provided to a form master who has responsibility for overseeing the education of a student. Further, a

student will reasonably expect a school to disclose his or her grades to his or her parent. This disclosure would be a secondary purpose related to the primary purpose.

- (b) If the information is sensitive information, then it may be used and disclosed for the purpose for which it was collected or a **directly** related secondary purpose. Schools should not assume that they can pass sensitive information to all teachers employed by the school. For example, if a school counsellor records that a boy informed the counsellor that he was gay, then disclosing that information to the student's maths teacher will most likely not be considered a directly related secondary purpose and therefore the disclosure would not be permitted unless the student had expressly consented to the use or disclosure.
- (c) If the information is health information, then it may be used and disclosed for the purpose for which it was collected or a **directly** related secondary purpose. Again, schools should not assume that they can pass health information to all teachers employed by the school. However, in some circumstances they must disclose the information. For example, a parent may inform a school on an enrolment form that his or her child has Attention Deficit Disorder. This is likely to affect the way a teacher teaches the student and may even affect the schooling of other students. A school may tell that student's teachers that he or she has Attention Deficit Disorder because the disclosure will be for the primary purpose of collection, being providing schooling to the student.
- (d) NPP 2.1(e) will also allow schools to disclose personal information if they believe that the use or disclosure is necessary to lessen or prevent a serious and imminent threat to an individual's life, health or safety. This will be relevant for schools that have students with health problems such as anaphylaxis. A school should disclose to a student's teacher the fact

that the student has anaphylaxis so that the teacher is prepared to respond to any reactions the student might have in class.

5. Conclusion

Schools should not assume that they can disclose all information that a school collects to all employees of the school. Schools should learn from *KJ -v- Wentworth Area Health Service* that it is not a good idea to have one general file for a student that contains all information collected about that student and have that file available to all employees at the school. Schools should classify the information that they collect about students and file the information appropriately so that the information is not disclosed inappropriately.