Lawyers and educators working together to protect schools, teachers and students from You Tube and other websites that malign them.

Michael Winram

Emil Ford & Co – Lawyers

10 September 2008

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

ABOUT THE AUTHOR

Michael Winram is an associate at Emil Ford & Co - Lawyers in Sydney. He practises mainly in commercial law and education law with a particular focus on educational institutions and other not-for-profit organisations including charities and other religious organisations. Michael has advised many educational institutions throughout Australia in relation to privacy issues, planning and development issues, the expulsion of students, family court disputes, governance issues, debt recovery and other contractual issues including enrolment procedures and enrolment contracts. He has also represented schools and students in the Supreme Court of New South Wales, the Land & Environment Court of New South Wales, the Australian Industrial Relations Commission and the Local Courts of New South Wales.

Michael is a member of ANZELA and is a member of the *NSW Chapter Committee*. He is also a member of the Law Society of New South Wales and is a Fellow of the Tax Institute of Australia.

Michael has presented at conferences in Tasmania, Melbourne and Sydney and published numerous papers on topics such as privacy, bullying and other issues relevant for schools.

Michael Winram

Emil Ford & Co – Lawyers

Level 5, 580 George Street,

SYDNEY NSW 2000

Tel: 02 9267 9800

Fax: 02 9283 2553

Michael.Winram@emilford.com.au

www.emilford.com.au

Lawyers and educators working together to protect schools, teachers and students from You Tube and other websites that malign them.

Michael Winram

Emil Ford & Co - Lawyers

The problem

A school principal discovers a website that maligned the school, its students and the principal. After becoming aware of the website, the school's board did almost nothing to try to protect the reputation of the school, its students and principal.

Another school principal discovers a video on You Tube of a segment of the final leaving assembly for the year 12 students. Linked to that video were other videos of students at a party after the school formal. The behaviour of students on the videos indicated that they were drunk. Some students on the video could be heard saying "I'm too drunk to stand up" and "Take your pants off."

At yet another school, parents and students had been communicating with a teacher on Facebook. Parents received reports from the teacher concerning their child through Facebook. Students also communicated with the teacher on Facebook. You could imagine the parents' surprise when it was discovered that the Facebook page had been created by other students at the school who had adopted the identity of the teacher.

Apparently, that particular teacher saw the humour in the situation. However, it does raise issues as to what can be done about websites that malign teachers and other students. Many teachers would be aware of websites such as http://au.ratemyteachers.com/ where students can rate teachers on easiness, helpfulness, clarity and coolness. No doubt, some teachers would be offended at the thought that they are referred to on websites.

Can anything be done?

It's my name and image – I reserve the right to control it!

It is easy to see how people may perceive that, if they discover their name, or a photograph, or some other information that identifies them on a blogsite or a social networking page, that they have the right to require that it be removed. This is not necessarily true. In Australia, there seem to be very limited rights to control personal information – whether that information is on an internet site or otherwise.

Accordingly, if personal information is discovered on the internet, it is important to analyse the content to see if the content itself is legally objectionable.

What about privacy?

In Australia, there is no High Court authority to suggest that there is a common law right to privacy. The High Court's position was first articulated in 1937 in *Victoria Park Racing -v- Taylor*[1] where the High Court unanimously adopted the English position that there is no authority that shows that any general right of privacy exists. After considerable advances in technology, the High Court was asked to re-visit the issue in *ABC -v- Lenah*[2] 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 in that case did not go so far as to establish a tort of privacy. Chief Justice Gleeson stated in that case that the *"lack of precision of the concept of privacy is a reason for caution in declaring a new tort of the kind for which the respondent contends. Another reason is the tension that exists between the interest in privacy and interest in free speech."*[3] Three other judges in that case said that a better course would be to look to the development and adaptation of recognised forms of action to overcome new privacy situations. Callinan J (who dissented) went further to say:

> *"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 recognised in this country, or whether the legislatures should be left to determine whether provision for a remedy for it should be made."*[4]

Many academics with whom I have spoken about *ABC -v- Lenah* have indicated that their reading of the case was that the High Court was subtly suggesting that they were ready to establish a tort of invasion of privacy, and were inviting an appropriate case to consider the issue. That was certainly the opinion of two judges in inferior courts in Australia.

In *Grosse -v- Purvis*[5] Justice Skoien in the District Court of Queensland said that in his view the individual judgements in *ABC -v- Lenah* contain propositions that can be identified with clarity to found the existence of a common law cause of action for invasion of privacy. In *Grosse -v- Purvis* the Mayor of Maroochy Shire Council claimed she was being stalked by a former romantic partner (this case did not involve the publication of any material). She claimed that she suffered post-traumatic stress disorder as a result of verbal and physical abuse by her former partner. She sued and was awarded

---

[1] *Victoria Park Racing and Recreation Grounds Company Limited -v- Taylor* [1937] HCA 45; (1937) 58 CLR 479 (26 August 1937).
[2] *Australian Broadcasting Corp -v- Lenah Games Meats Pty Ltd* (2001) 185 ALR 1
[3] *Australian Broadcasting Corp -v- Lenah Games Meats Pty Ltd* (2001) 185 ALR 1 per Gleeson CJ
[4] *Australian Broadcasting Corp -v- Lenah Games Meats Pty Ltd* (2001) 185 ALR 1 per Callinan J at 335.
[5] *Grosse -v- Purvis* [2003] QDC 151 at 415ff

damages under various causes of action including the tort of invasion of privacy. Justice Skoien said:

> *It is a bold step to take, as it seems, the first step in this country to hold that there can be a civil action for damages based on the actionable right of any individual person to privacy. But I see it as a logical and desirable step. In my view there is such an actionable right.*

Of course, after declaring that a right to privacy exists, the Judge had to then lay out the essential elements of the tort which he said would be:

> *(a) a willed act by the defendant,*
>
> *(b) which intrudes upon the privacy or seclusion of the plaintiff,*
>
> *(c) in a manner which would be considered highly offensive to a reasonable person of ordinary sensibilities,*
>
> *(d) and which causes the plaintiff detriment in the form of mental psychological or emotional harm or distress or which prevents or hinders the plaintiff from doing an act which she is lawfully entitled to do.*[6]

Similarly, in the County Court of Victoria, Judge Hampel said in *Doe -v- ABC & Ors*[7] that the case before him was an appropriate case to:

> "*respond, although cautiously, to the invitation held out by the High Court in Lenah Game Meats and to hold that the invasion, or breach of privacy alleged here is an actionable wrong which gives rise to a right to recover damages accordingly to the ordinary principals governing damages in tort."*[8]

The facts in *Doe -v- ABC & Ors* revealed that Ms Doe's name, together with other identifying information, was broadcast over the radio. After the broadcast, Ms Doe said:

> *"I felt I had no control at all over anything that was happening in my life at the moment when probably an hour ago I had a piece of my life given back to me when [my husband] was found guilty and I felt I was, I don't know, stripped naked in public again. I felt humiliated. I felt like everyone in the street and everyone around me know that it was on the radio."*

Ms Doe's husband had been convicted of raping her, and various other offences, a short time before the broadcast. Because of the seriousness of the crime, Ms Doe's name was prohibited from being published under the *Judicial Proceedings Reports Act.* Ms Doe succeeded on the basis that publishing her name was against section 4(1A) of that Act.

---

[6] *Groose -v- Pervis* [2003] QDC 151 (16 June 2003) at 444
[7] *Doe -v- ABC & Ors* [2007] VCC 281
[8] *Doe -v- ABC & Ors* [2007] VCC 281 at 157

She went further to request that the court also find the defendant liable for damages under the tort of invasion of privacy. Judge Hampel said:

> *The wrong that was done here was the publication of the personal information, in circumstances where there was no public interest in publishing it, and where there was a prohibition on its publication. In publishing the information, the defendants failed to exercise the care which could be reasonably required of them to protect the plaintiff's privacy and comply with the prohibition on publication imposed by s4(1A). This, coupled with the absence of public interest, the clearly private nature of the information, and the prohibition on publication, all point to the publication being unjustified. In my view, a formulation of unjustified, rather than wilful, in these circumstances provides a fair balance between freedom of speech and the protection of privacy…the information is personal or confidential information which the plaintiff had a reasonable expectation would remain private, and clearly private. Its disclosure was plainly something which an individual was entitled to decide for herself.*[9]

Because neither of these two cases were appealed to a Supreme Court in the relevant state, they should be relied on cautiously. They do indicate that lower courts are willing to hear cases based on the tort of invasion of privacy. However, one should be careful in applying them too directly. The facts in both cases were extreme and the plaintiff was successful on other grounds. For example, in *Doe -v- ABC & Ors,* broadcasting the name of the Plaintiff was illegal under the *Judicial Proceedings Reports Act* and the broadcast of Ms Doe's name caused considerable psychological damage to a woman who had suffered the most extreme attacks from her ex-husband.

If we rely on the High Court's current position, that there is no common law right to privacy, at common law it is not necessarily an invasion of privacy if pictures, videos or other information about a student, teacher or school appear on the internet. There is very little a school can do to have the material removed on this basis alone.

What about a legislative right to privacy?

The Privacy Act does not introduce a right to privacy in Australia and is of limited use because it only applies to organisations that turn over $3million a year. It does not apply to individuals. Accordingly, if an individual places photographs, videos or other information about another person on an internet blogsite or on a social networking page the individual placing the photograph, video or other information is not necessarily in breach of the Privacy Act.

However, on 11 August 2008, the Australian Law Reform Commission (ALRC) released its privacy inquiry report. It recommended that the government amend the Privacy Act to introduce a statutory cause of action for serious invasions of privacy. Professor David Weisbrot said in a press release:

[9] *Doe -v- ABC & Ors* [2007] VCC 281 at 163

> *"Although the federal Privacy Act is only 20 years old, it was introduced before the advent of supercomputers, the internet, mobile phones, digital cameras, e-commerce, sophisticated surveillance devices and social networking websites – all of which challenge our capacity to safeguard our sensitive personal information."*[10]

The ALRC recommendation was that the cause of action cover circumstances in which:

(a) there has been an interference with the individual's home or family life;

(b) an individual has been subjected to unauthorised surveillance;

(c) an individual's correspondence or private communication has been interfered with; or

(d) sensitive facts about an individual's private life have been disclosed.

The ALRC report also says that the *"cause of action should apply only where the individual had a reasonable expectation of privacy; and the act or conduct complained of is highly offensive to a reasonable person."*[11]

The ALRC have given examples of when this cause of action might be available, including[12]:

- After the break-up of their relationship, Mr A sends copies of a DVD of himself and his former girlfriend (Ms B) engaged in sexual activity to B's parents, friends, neighbours and employer;

- Mr C sets up a tiny hidden camera in the women's toilet at his workplace, capturing images of his colleagues that he downloads to his own computer and transmits to a website hosted overseas, which features similar images; and

- Ms D works in a hospital and obtains access to the medical records of a famous sportsman, who is being treated for drug addiction. D makes a copy of the file and sells it to a newspaper, which publishes the information in a front page story.

Another interesting aspect of the report is its comments on children and other young people. The report found that children were more likely to pass on personal information via the internet, on social networking pages, blogsites and other websites. The report also found that many children did not understand that deleting a profile did not mean that the information was ultimately deleted. The Commission recommended that the introduction

---

[10] "Australia must rewrite privacy laws for the Information Age", media release 11 August 2008, www.alrc.gov.au.

[11] *"A Statutory cause of action for serious invasions of privacy: getting the balance right"* Media Briefing Note 10, ALRC Privacy Inquiry, 11 August 2008, www.alrc.gov.au

[12] These examples can be seen in *"A Statutory cause of action for serious invasions of privacy: getting the balance right"* Media Briefing Note 10, ALRC Privacy Inquiry, 11 August 2008, www.alrc.gov.au.

of a cause of action for serious invasion of privacy should also address issues relating to children. From this we might infer that, what may not be a serious invasion of privacy to an adult, may be a serious invasion of privacy for children. If such a distinction were made, it would be a significant shift from the current Privacy Act which does not distinguish between adults and children.

It will be interesting to see how the Australian government responds to the ALRC report. In addition to the ALRC report, Australia is a party to the *International Covenant of Civil and Political Rights (1966)* which states that:

> *(a) 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.*
>
> *(b) Everyone has the right to protection of the law against such interference or attacks.*

The government has not yet used its membership to this covenant to introduce a tort of privacy. This covenant is merely attached as a schedule to the Commonwealth *Human Rights and Equal Opportunity Commission Act 1986*. Given the ALRC report and the government's membership of this covenant, we may assume that the government will introduce a tort of privacy in the not too distant future.

Until then, the legal position remains that, in only exceptional cases, will lower courts allow a plaintiff to claim damages for invasion of privacy if he or she discovers personal information on the internet. A plaintiff is more likely to succeed if he or she can rely on other heads of damage or other legal principles.

Isn't there an act that regulates online content?

The Australian government has set up a system of online regulation in co-operation with State governments. The aim of online regulation, according to the Minister for Communications and the Arts at the time, was that "material accessed through online services should not be subject to a more onerous regulatory framework than 'off-line' material such as books, videos, films and computer games."[13]

The *Broadcasting Services Amendment (Online Services) Act 1999 ("the Online Services Act")* is largely complaints based. In most circumstances, Internet Content Hosts (ICH) and Internet Service Providers (ISP) are only required to remove content following formal notification from the Australian Communications and Media Authority (ACMA) if it is prohibited content or potentially prohibited content. The legislation also addresses the huge problem of ICH and ISP being liable in other areas for carrying and hosting content of which they are not aware. Section 91 of Schedule 5 of the *Online Services Act* states that a law of a State or Territory, or a rule of common law or equity, has no effect to the extent to which it:

[13] Corker, Nugent, Porter, "Regulation Internet Content: A Co-Regulatory Appriach" [2000] *UNSWLJ* 5.

(a) subjects an ICH or ISP to liability (either criminal or civil) in respect of hosting particular internet content in a case where the host was not aware of the nature of the internet content; or

(b) requires an ICH or ISP to monitor, make inquires about, or keep records of, internet content hosted by the host.

Therefore, if you discover information about yourself or your school on a blogsite or on You Tube, the first step is to write to the ICH or ISP informing them of the content and asking them to remove it. It is more than likely that an ICH or ISP will not remove the content unless you are able to show that the material is illegal or may expose the ICH or ISP to a claim for damages.

How do I know if the material is illegal?

The *Classification (Publications, Films and Computer Games) Act 1995 (Cth)* has established a national classification scheme. The national classification scheme is a co-operative 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 ACMA on internet content.

The Classification Board is made up of members who are supposed to broadly represent the Australian community. The Classification 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.[14] Further, the Classification Board must make its decisions in accordance with the National Classification Code which is approved by the Commonwealth, 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, as it relates to publications, includes material that:

(a) describe, depict, express or otherwise deal with matters of sex, drug misuse or addiction, crime, cruelty, violence or revolting or abhorrent phenomena in such a way that they offend against the standards of morality, decency and propriety generally accepted by reasonable adults to the extent that they should not be classified; or

(b) describe or 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); or

[14] s11, *Classification (Publications, Films and Computer Games) Act 1995* (Cth)

(c) promote, incite or instruct in matters of crime or violence.[15]

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.[16] In a discussion paper[17], the Attorneys-General 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). The ALRC have recommended that the Classification Board be able to consider linked sites when analysing internet content.

Schedule 5 of the *Online Services Act* established a regulatory scheme to deal with internet content. The scheme is administered by the ACMA. The Act prohibits the following internet content:

(a) content which is or would be classified RC or X18+ by the Classification Board; and

(b) 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.

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:

(a) Members of the pubic can make complaints about internet content to the ACMA if it would be prohibited content under the Act.

(b) The ACMA refers the internet content to the Classification Board for a classification decision.

(c) 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.

---

[15] *National Classification Code*
[16] Standing Committee of Attorneys-General, *Unauthorised Photographs on the Internet and Ancillary Privacy Issues: Discussion Paper,* August 2005
[17] Standing Committee of Attorneys-General, *Unauthorised Photographs on the Internet and Ancillary Privacy Issues: Discussion Paper,* August 2005

(d) If the Classification Board classifies the internet content as prohibited content, the ACMA will issue a take-down notice to the internet host.

(e) 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.

(f) 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.

(g) 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.

I have already noted that the procedure set out in *Online Services Act* is complaints based. This is one of the biggest problems with the procedure. ACMA will generally not investigate the content of an internet site unless a complaint is made. However, in July 2008, the ACMA approved an Internet Industry Code of Practice which requires commercial content services providers to have internet content assessed by a trained content assessor where:

(i) The content has not been classified by the Classification Board; and

(ii) The commercial content service provider, acting reasonably, considers the Stored Content to be substantially likely to be classified as Prohibited Content or Potential Prohibited Content.[18]

A Commercial Content Service provider is a content service provider that is operated for profit or as part of a profit-making enterprise and is provided to the public but only on payment of a fee (whether periodical or otherwise). This part of the Code does not bind designated content providers or hosting service providers who are not commercial.

Can someone commit a crime by posting material on the internet?

It is possible to commit a crime by posting material on the internet. Sections 473.1 to 475.2 of *The Criminal Code,* which is a schedule to the *Criminal Code Act 1995* (Cth) contains criminal offences in relation to online material.

Threat to kill: Section 474.15(1) of *the Code*, makes it an offence if:

[18] Internet Industry Code of Practice, 10 July 2008, www.iia.net.au

(a) the first person uses the internet to make a threat to another person (the second person) to kill the second person or a third person; and

(b) the first person intends the second person to fear that the threat will be carried out.

The penalty is imprisonment for 10 years. It is not necessary to prove that the person receiving the threat actually feared that the threat would be carried out.

Threat to cause serious harm: Section 474.15(2) of *the Code*, makes it an offence if:

(a) the first person uses the internet to make to another person (the second person) a threat to cause serious harm to the second person or a third person; and

(b) the first person intends the second person to fear that the threat will be carried out.

The penalty is imprisonment for 7 years. It is not necessary to prove that the person receiving the threat actually feared that the threat would be carried out.

Using the internet for a hoax threat: Section 474.16 of *the Code,* makes it an offence if:

(a) a person uses the internet to send a communication; and

(b) the person does so with the intention of inducing a false belief that an explosive, or a dangerous or harmful substance of thing, has been or will be left in any place.

The penalty is imprisonment for 10 years.

Using the internet to menace, harass or cause offence: Section 474.17 of *the Code*, makes it an offence if:

(a) a person uses the internet; and

(b) the person does so in a way (whether by the method of use or the content of a communication, or both) that reasonable persons would regard as being, in all the circumstances, menacing, harassing or offensive.

The penalty is imprisonment for 3 years. In *The Groves No. Four Minyama*[19] an owner of a strata unit made telephone calls to an adjoining owner at 4 a.m. and hung up as soon as the calls were answered. It was found in that case that the "dead phone calls" were menacing, harassing or offensive. However, one should be cautious before relying on this section. Proving that a person used the internet in a way that is menacing, harassing or offensive will not necessarily mean that the person has violated the section. One must

[19] *The Groves No. four Minyama* [2006] QBCCMCmr 317 (19 June 2006)

also prove that the person who used the internet in a menacing, harassing or offensive way was aware of a substantial risk that a reasonable person would regard the conduct as menacing, harassing or offensive and that it was unjustifiable to take that risk. That is, the fact that the internet content is objectively menacing, harassing or offensive is not sufficient. The intention, knowledge or recklessness of the person posting the internet content must also be considered. This was articulated more clearly by Philip McMurdo J in the Queensland Court of Appeal in *Crowther -v-Sala*[20]*:*

> *"If the law creating the offence does not specify a fault element for a physical element that consists of a circumstance or a result, then the corresponding fault element is recklessness. Under s5.4(4) a person is reckless with respect to a circumstance if she is aware of a substantial risk that the circumstance exists and having regard to what is known to her, it is unjustifiable to take that risk. Similarly, a person is reckless with respect to a result if she is aware of a substantial risk that the result will occur and having regard to what is known to her, it is unjustifiable to take the risk. By s5.4(4) if recklessness is a fault element, then proof of intention, knowledge or recklessness will satisfy the element. A person has an intention with respect to a circumstance if she believes it exists or will exist and with respect to a result if she means to bring it about or is aware that it will occur in the ordinary course of events."*

If the material is not illegal but is defamatory can I sue the ICH or the ISP?

Defamation is a tort that protects the reputation of individuals and corporations. Its principal remedy is damages. Justice Kirby helpfully set out in *Dow Jones & Company Inc -v- Gutnick* the deeply entrenched common law principles necessary to establish the tort of defamation:

1. *damage to reputation is essential for the existence of the tort of defamation;*

2. *mere composition and writing of words is not enough to constitute the tort; those words must be communicated to a third party who comprehends them;*

3. *each time there is such a communication, the plaintiff has a new cause of action, and*

4. *a publisher is liable for publication in a particular jurisdiction where that is the intended or natural and probably consequence of its acts.*[21]

Before commencing proceedings in defamation, the person who published the material must be identified. This can be a difficult task as there is usually a chain of publication. For example, if I write a book, I may write it, another will edit it, a printing press will

[20] *Crowther -v- Sala* [2007] QCA 133 (20 April 2007)
[21] *Dow Jones & Company Inc -v- Gutnick* [2002] HCA 56 per Kirby at 124

print it, another person may deliver it to bookstores and libraries, libraries may have it available to borrow and bookstores may sell it. Similarly, with the internet someone may write defamatory material, upload it in Sydney, but the content is ultimately stored and accessible from a computer in India. Traditionally, the law in Australia has protected subordinate distributors of defamatory material. Accordingly, printers, newsagents, libraries and bookstores were protected from defamation.

How then, does this relate to internet content?

Dow Jones & Company Inc -v- Gutnick

The Court was asked this question in *Dow Jones & Company Inc -v- Gutnick.*[22] Dow Jones & Company Inc is the publisher of the *Wall Street Journal* and *Barron's* magazine. Like many print publications it also operated a website that contained the same content as the printed publications. The website was www.wsj.com and, for a fee, a subscriber could access the online version of *Barron's* magazine. Subscriptions were not limited to geographic location, so long as the subscriber could pay by an approved credit card over the internet.

An article was published in *Barron's* magazine, and on the online version, on 28 October 2000 entitled "Unholy Gains" that portrayed Mr Gutnik as an abettor to a convicted criminal, Nachum Goldberg. He claimed that the publication defamed him because it implied that he "was masquerading as a reputable citizen when he was a tax evader who had laundered large amounts of money through Goldberg, and bought his silence."[23]

Mr Gutnick commenced proceedings in the Supreme Court of Victoria only in relation to the material that was available in the State of Victoria. After losing in the Victorian Supreme Court, Dow Jones appealed to the High Court claiming that the statement, of which Mr Gutnick complained, was published in New Jersey (because that is where the website's server was located) and that New Jersey was the appropriate jurisdiction to govern questions of substance in the proceedings. Interestingly, 18 other businesses and organisation supported Dow Jones in the High Court, including Yahoo!, Amazon.com, News Limited and the Australian Internet Industry Association.[24]

However, the majority in that case said:

> *In defamation, the same considerations that require rejection of location of the tort by reference only to the publisher's conduct, lead to the conclusion that, ordinarily, defamation is to be located at the place where the damage to reputation occurs. Ordinarily that will be where the material which is alleged to be defamatory is available in comprehensible form, assuming, of course, that the person defamed has in that place a reputation which is thereby damaged. It is only when the material is in comprehensible form that the damage to reputation is*

[22] *Dow Jones & Company Inc -v- Gutnick* [2002] HCA 56
[23] *Gutnick -v- Dow Jones & Company Inc* [2001] VSC 305 (28 August 2001)
[24] Anna Beyer, "Defamation on the Internet: Jospeh Gutnick -v- Dow Jones", *Murdoch University Electronic Journal of Law*, Volume 11 Number 3 (September 2004) www.austlii.edu.au

> *done and it is damage to reputation which is the principal focus of defamation, not any quality of the defendant's conduct.*

The majority went on to say:

> *It is where that person downloads the material that the damage to reputation may be done. Ordinarily then, that will be the place where the tort of defamation is committed.*

This judgment has received considerable criticism from various groups who are concerned that, because internet content is available world wide, vexatious litigants may be able to commence proceedings in numerous jurisdictions for the same material. Indeed, Justice Kirby admitted in his judgment that the dismissal of Dow Jones' appeal does not represent a wholly satisfactory outcome. He went on to say:

> *Where large changes to settled law are involved, in any area as sensitive as the law of defamation, it should cause no surprise when the courts decline the invitation to solve problems that others, in a much better position to devise solutions, have neglected to repair.*

Despite these criticisms, the legislators have not introduced legislation to address some of these concerns. Accordingly, the current law in Australia is that, in relation to defamation, an action may be bought against a person in the jurisdiction where the material may be downloaded and read.

Mark Forytarz and Paul Castrian –v- Google Australia Pty Ltd

The liability of search engines for defamation is currently under consideration in the Victorian Supreme Court in *Forytarz & Castrian -v- Google*. This case will, if it is not settled prior to judgment, test the boundaries of Australia's defamation laws and the *Online Services Act.* Mark Forytarz and Paul Castrian are real estate agents in Melbourne who found defamatory statements on a blogsite posted by Neil Jenman. The blogsite could be accessed by typing their names into Google's search engine and then clicking on the hyperlinks that are displayed on the cached pages on Google after the "Google Search" button is clicked.

Mr Forytarz and Mr Castrian wrote to Google asking that it remove access to the defamatory blogsites. They also wrote to Destra Corporation Limited, who they initially alleged hosted the blogsites on its servers, requesting that Destra remove the postings from its servers. Both Google and Destra refused and Mr Forytarz and Mr Castiran commenced proceedings in the Victorian Supreme Court claiming that Google and Destra were responsible for publishing the defamatory material and are liable for damage that they have suffered as a result. Mr Forytarz and Mr Castrian have subsequently removed Destra as a defendant as Destra was able to show that it was not the host at the relevant time. Interestingly, they did not include Mr Jenman as a defendant, even though it was his blogsite and he was the author of the material.

Because Mr Forytarz and Mr Castiran wrote to Google, Google can probably not rely on section 91 of schedule 5 to the *Online Services Act,* that it was not aware of the nature of the content on the blogsite. What will be interesting is whether the Court finds Google liable for damages in defamation for not taking steps to remove access to the material after being notified of its objectionable content. This case has the potential to break new ground in the liability of ISP and ICH and it will be interesting to read the judgment.

What if it is the School's own students are uploading the material?

From a legal perspective, most of the rights and obligations attaching to adults generally will be the same as those attaching to students. Accordingly, if a student defames a school, teacher or other student, the school can request that the student remove the content on the basis that the student may be liable in defamation. However, I believe that there are some proactive steps schools can take to protect their reputation and keep a check on information that is being posted on the internet. I should acknowledge that I am not a teacher and have not been involved in the day to day running of schools, apart from advising schools on legal issues and representing them in court. I have no doubt that many schools will have better solutions than the ones I will suggest!

Get to know what internet sites are being used by Students.

I started this paper by telling the story of students that had created a profile of a teacher on Facebook and had assumed his identity and communicated with parents. Students at the school used to tell him that he was a "cool" teacher because he had a Facebook page. The hoax was ultimately discovered after some months when the teacher inquired of another staff member as to what Facebook was. I know of one principal who decided that, rather than banning access to Facebook on school computers, he would join Facebook and students and teachers were only allowed to access Facebook on school computers if they included him as a friend. That way, he was able to monitor the content on the Facebook pages of teachers and students, and even monitor communication between teachers and Students.

Unless you know what sites are being used by students, it is impossible to keep track of how students are using the internet either at school or out of school.

Educate your students on the use of internet sites.

One of the alarming outcomes of the ALRC report were the reports of discussions with young people. ALRC President, Professor David Weisbrot said:

> *"While young people clearly understand technology, and in particular the internet, it was clear that they did not have a good understanding of what happens to their information once it is posted. For example, many thought that deleting the profile, or even a particular item, meant that the information is removed completely from the on-line environment – which often is not the case at all...For these reasons, the ALRC recommend that the Privacy Commissioner, industry associations and educational authorities provide children and young people with*

> *more information on privacy issues, so that they can better protect their own privacy and respect the privacy of others."*[25]

A starting point for educating students is the Australian Government's site: http://www.netalert.gov.au/. It contains information on how to educate students on safe and appropriate use of internet sites. It also contains links to education programs such as:

- CyberNetrix: www.cybernetrix.com.au
- Netty's World: www.nettysworld.com.au
- Cyber Quoll: www.cyberquoll.com.au
- WiseuptoIT: www.wiseuptoit.com.au
- Cyber Smart Kids: www.cybersmartkids.com.au

Ensure your policies address the appropriate use of the internet by Students and staff!

Schools must have internet and e-mail policies that state how students and staff may use computers owned by the school. The policies should also address consequences for maligning the school, staff or other students regardless of whether the school's computers are used. For example, is it the school's policy that a student will be expelled for misrepresenting the school or a teacher on the internet? Are there consequences for students uploading videos onto sites such as You Tube that malign the school?

Apparently, proceedings have commenced in the Australian Industrial Relations Commission (AIRC) for the unfair dismissal of Karl Tilcock. Karl worked at the Foster's brewery in Queensland. In his spare time he made You Tube videos that offended other employees and portrayed Foster's in a bad light. News.com.au has reported that Karl denies producing the videos on company time. Fosters claims that Karl was warned about making videos in violation of company policies.[26] Although the AIRC has not yet heard the matter it is important to note that it would have been difficult for Fosters to terminate Karl's employment, and subsequently defend the matter in the AIRC, if they did not have policies outlining the consequences of making disparaging remarks about the company and about employees on the internet.

Conclusion

The biggest issue for law makers is trying to get the balance right between the general human right of free speech with the need to protect individuals and organisations, such as schools and students, from internet content that maligns them. As I have indicated, at present there is no general right to privacy. If you discover a website that contains

---

[25] *"Children, Young people and privacy"* Media Briefing Note 10, ALRC Privacy Inquiry, 11 August 2008, www.alrc.gov.au

[26] *"Fosters sacks autistic worker over You Tube jokes",* by Tuck Thompson, 8 September 2008, www.news.com.au.

information about your school or students, you do not have an automatic right to request that it be removed. However, if you believe it is a serious breach of privacy, of if you believe the content is defamatory, the first step is to write to the ISP and the ICH to request it be removed. Remember, ISP and ICH will not be liable under any head of damage under any State or Territory legislation or under the common law, until they have been made aware of the content. If you suspect the internet content is prohibited content then you should make a complaint to ACMA.

Schools should also:

- Be aware of internet sites that are used by its staff and students;
- Have policies that outline how school computers may be used and the consequences of maligning the school, its staff or students, even if the content is posted on the internet from personal computers;
- Educate students on using the internet safely.

Most of the law in this area is yet to be developed. There may well be a new legal landscape in a very short time if the federal government introduces a tort of invasion of privacy and if the Victorian Supreme Court finds *Google* liable in defamation after it became aware of the defamatory material. The law will always be slower than the pace at which internet technology develops. Schools should ensure that they keep up to date with the development of internet technology and respond appropriately.