CHAPTER 36
THE LAW OF CYBERSPACE

FOCUS TOPICS

FOCUS OBJECTIVES

To understand and appreciate:

- what laws apply to the internet;
- how e-commerce is regulated;
- the privacy risks associated with the internet;
- how governments and parents attempt to regulate content on the internet;
- the challenges for the legal system in regulating the internet; and
- the legal ramifications of social media

36.1 WHAT IS THE LAW OF CYBERSPACE?

The internet is a worldwide network of computers that has revolutionised our society. The internet can be used to communicate with others (by email, instant messaging, and by real-time voice conversations), find information about almost anything, buy and sell products, watch videos, play games, and seemingly hundreds of other activities. All of these activities take place in 'cyberspace', which is a term for the **virtual world** that can be used to visualise this worldwide network of computers that make up the internet.

However, not only are more and more people using the internet, they are increasingly contributing to the internet by creating their own 'space' in cyberspace, where they control the content. Once web page creation required a sophisticated knowledge of HTML computer code, but now user friendly tools make it possible for anyone to create a web page, be it on Facebook or Tumblr, or have a blog (or a weblog). A blog is probably the easiest and most common web page to create. These blogs take the form of an online journal or diary and can cover any topic – from the mundane life of a bored high school student to complex political analysis and debate.

Practical application P

Go to Blogger (www.blogger.com) - and set up a blog, either as a class or as individuals. As you move throughout this chapter, blog about what you learn and your answers to the activities, so that your non-Legal Studies classmates can understand about the law of cyberspace. [K] [I] [E]

Given that it is a worldwide network, the **internet is international,** which as you have seen in previous chapters, makes it very hard to regulate. However, it would be a mistake to think that laws do not apply to the internet. Indeed, the internet is still **regulated by a range of national and international laws**. These laws can be referred to as the law of cyberspace.

The law that applies to the internet is not only a mix of national and international law, it is also a mix of new law that was deliberately made to apply only to the internet, and existing (or 'old') law that applies to this new medium. The following matrix gives some examples of how these laws apply to the internet:

	Existing (or 'old') law	New law
National	*Defamation Act 2005* (Qld) – you still can't defame someone just because you do so on the internet	*Electronic Transactions Act 1999* (Cth) – a new law to govern contracts formed on the internet. *Spam Act 2003* (Cth) – a new law to deal with unwanted emails and instant messages.
International	*Hague Convention on Choice of Court Agreements* (Hague Convention) – the old law about which court hears an international dispute still applies	*UNCITRAL Model Law on Electronic Signatures 2001* – a new international model law for regulating electronic signatures, rather than the traditional paper signatures.

Even though the existing (or 'old') law continues to apply, **new law is continually being made to regulate the internet**. This new law, which will be the focus of this chapter, constantly struggles to keep up with the rapid pace of change on the internet.

36.2 ELECTRONIC COMMERCE (E-COMMERCE)

Electronic commerce, known as e-commerce, is **doing business electronically, usually using the internet**. The use of the internet makes e-commerce global, and always available. A website can continue taking orders 24 hours a day, making different business hours and time zones irrelevant. As Australians have one of the highest rates of internet use in the world, more and more of our transactions are occurring electronically. According to the Australian Bureau of Statistics, the number of people who shopped online grew from just 7% in 2000 to 31% in 2005, and to 68% in 2011.

There has been an increase in e-commerce because:

- it reduces the cost of doing business;
- of the high level of acceptance of internet use; and
- it provides greater access to interstate and global markets.

An example of the success of e-commerce is the American company Amazon.com which sells books and music on-line. It does not have any established shops so it does not have the expense of renting commercial premises in the world's cities, but is able to take orders and distribute its products worldwide.

There are disadvantages and concerns however with e-commerce. These include:

- e-commerce is a new, ever-changing and difficult medium to regulate;
- concerns as to the security of online transactions; and
- concerns as to the lack of privacy and confidentiality with online communications.

The legal system has endeavoured to regulate e-commerce and to address these concerns and difficulties.

ELECTRONIC TRANSACTIONS ACT 1999 (CTH)

As previously explained the internet has revolutionised the way individuals, organisations and businesses interact with each other. The use of the internet was so extensive that within a short space of time thousands of contracts were being made online. Legislation was needed to set out whether the courts would see these contracts as valid, how they would be interpreted, and the law that would applied.

The lead was taken by the Commonwealth Parliament which, on the recommendations of an appointed Electronic Commerce Expert Group, passed the *Electronic Transactions Act 1999* (Cth) (the Act). This Act was introduced to set up a legal framework for the operation of e-commerce in Australia that was **consistent with international standards**. For this reason it was based on the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce.

VOL 1
CH 11

The Act states that, for the purposes of Commonwealth law, **electronic transactions are valid and lawful** ways to conduct business. This means that electronic commerce is treated legally in the same way as paper based commerce. In that way, **e-commerce retains the principles and rules of contract law**. It simply allows for the requirements of a valid contract – offer, acceptance and consideration - to be done through electronic means.

The Act also gives business and the community the option of using electronic communications when dealing with Government agencies. The Act, however, does allow for regulations to limit or exclude provisions of the Act. To date, these have been mainly in regard to migration and citizenship documents.

As the provisions of the Commonwealth Act do not apply to matters governed by State law, the Queensland Government introduced the *Electronic Transactions Act 2001* (Qld) to complement the Commonwealth legislation. It also states that, as a general rule, Queensland law will not hold a transaction invalid because electronic communications were used. Although not identical, the Queensland Act has provisions that mirror the Commonwealth Act. Other states and territories have introduced similar Acts as well.

All of these Acts provide that:

- giving information electronically satisfies legal requirements that information be given in writing;
- signatures can be given electronically, that is, by some means that identifies the person and his or her approval (note that there are also international initiatives that recognise electronic signatures, including the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Signatures and the United Nations Convention on the Use of Electronic Communications in International Contracts);
- documents can be produced and sent electronically, but they must remain complete and unaltered, and be verified; and
- a person is only bound by an electronic communication if that person sent it, or it was sent with his or her authority.

Finally, as to **when and where is an online contract made**, the general law governing the contract will be that of the place where the contact was formed. And as e-commerce occurs globally, this can become complicated. Of course, a contract can always avoid this by stating in it which law is to apply.

Hypothetical H

Ed, who lives in Brisbane, has just bought a computer. He asks your advice on whether any of the following matters can be done electronically. [K] [E]

- The Taxation Department has requested documentation for travel expenses claimed last year.
- Ed wants to buy a bike he sees in an online advertisement for the sale of a bike from a person who lives in Sydney.
- Ed wants to order a book from the Queensland Government printer.

HOW SECURE ARE ON-LINE TRANSACTIONS?

One major concern about e-commerce is the security of online transactions. As you saw in Chapter 35, there is considerable potential for misuse and fraud. It is vital to have such transactions secure as Australians increasingly use the new e-technologies. The Australian Bureau of Statistics reported that in 2010-11, of the 13.3 million people who reported accessing the internet at home, 64% of people did so to pay bills online or do online banking.

Technology is being developed to address these security concerns. Encryption techniques have been developed to ensure that consumer information remains confidential and secure. This is done by scrambling the information transmitted in a form that only a person authorised to decrypt that information knows how to access the information. This prevents third parties from obtaining such details. An *Electronic Funds Transfer Code of Conduct* is being regularly revised to assist with the security of financial online transactions and to deal with liability for misuse of payments.

RESEARCH

Visit the Australian Government's Stay Smart Online site -

www.staysmartonline.gov.au/home_internet_users

and prepare a poster on how you can protect your information online. Alternatively, prepare a blog entry on protecting your information online. [K] [I] [E]

WHAT DO YOU THINK?

Do you think it is sufficiently safe and secure to buy and sell things, and to bank online? Would you do it? Why or why not? [K] [E]

SPAM

Spam is the term used to describe **electronic 'junk mail'** by which identical messages are sent to recipients by email or instant messaging. The content of these unwanted messages varies: some promote products or services, some contain pornographic images or links, and some try to trick users into providing personal or financial information, such as bank account numbers, passwords, credit card details (this latter type is known as **phishing**). Spam is now the overwhelming majority of internet traffic and phishing attacks are becoming more sophisticated.

RESEARCH

- Find out why the term 'spam' was used to describe electronic 'junk mail'. [I]
- How do spammers collect the email addresses to which the spam message is sent?[I]
- Find out why the term 'phishing' was coined. [I] What are the ways by which a phishing email can be detected? [I]

Apart from spam being simply irritating, it is a problem because it clogs up the internet, disrupts email delivery, reduces productivity, and as well frequently exposes users to offensive or fraudulent material.

To try to reduce the amount of spam many countries around the world, including Australia, have passed legislation that specifically targets spam. *The Spam Act 2003* (Cth) prohibits the sending of spam, defined in the Act as 'unsolicited commercial electronic messages', with an 'Australian link'. A message has an 'Australian link' if it originates or was commissioned in Australia, or originates overseas but was sent to an address accessed in Australia.

The Spam Act covers email, instant messaging, SMS (text messages) and MMS (image-based mobile phone messaging) messages of a commercial nature. It does not cover faxes, internet pop-ups or voice telemarketing. There is a Do Not Call Register which applies to telemarketing.

Any message that does not meet the following three conditions is considered to be spam:

Consent – the message must be sent with your consent.

Identify – the message must contain accurate information about the person or organisation that authorised the sending of the message.

Unsubscribe – the message must contain a functional 'unsubscribed' facility to allow you to opt out of receiving messages from that source.

Messages do not have to be sent out in bulk to be considered spam. Under Australian law, a single electronic message can also be considered spam.

Certain types of electronic messages are partially exempt from the *Spam Act*. However, these messages must still include accurate information to identify the person or organisation that authorised them. **Exempt messages** can be from:

- government bodies;
- registered political parties;
- religious organisations;
- charities; and
- educational institutions (sent to current and past students and their households).

The *Spam Act* is enforced by the Australian Communications and Media Authority (ACMA).

Case Study

Australian Communications and Media Authority v Clarity1 Pty Ltd [2006] FCA 410

Facts: The ACMA alleged that from 10 April 2004 Clarity1, an Australian company, periodically sent commercial emails to email addresses it had harvested from the internet using address-harvesting software or had purchased from organisations or persons selling electronic lists of email addresses harvested from the internet. (Address-harvesting software scours the internet searching for addresses available from public data.) In all, the ACMA alleged that Clarity1 sent 270305474 commercial emails (of which 74996560 were successfully sent) to 7956457 unique email addresses. The emails sent by Clarity1 contained an unsubscribe facility and the evidence was that some 166000 requests to be removed from the lists were made, all of which were acted upon. However, over the same time period only 79 complaints concerning spam from Clarity1 were made to the ACMA.

The ACMA alleged that Clarity1 had sent 'unsolicited commercial electronic messages', with an 'Australian link'.

Legal Issues: Had the recipients consented to the sending of the emails?

Decision: Clarity1 made three arguments as to consent, all of which were **rejected by the Federal Court.**

Clarity1 argued that as the emails contained an unsubscribe facility, Clarity1 was entitled to reasonably infer that any recipient who did not use this facility had consented to the sending of the emails. The Court rejected this argument, holding that there were 'powerful features of the evidence which are inconsistent with the drawing of any such inference and militate against it.'

Clarity1 argued that consent could be inferred from the business relationship between Clarity1 and the individual or organisation. The Court rejected this argument, holding that there could be no business relationship when the communication is one-sided. The relationship must have a connection arising from mutuality. Accordingly, the Court held that only the 182 purchasers who replied and wished to trade with Clarity1 had given their consent.

Clarity1 argued that the recipients had consented by publishing their electronic addresses on the internet. The Court also rejected this argument, holding that simply making an email address available somewhere on the internet could not be considered consent to receive spam.

RESEARCH

Go to the ACMA's website on spam -

www.acma.gov.au/WEB/STANDARD/pc=PC_310294

and make a poster on how you can help prevent spam by reporting it to the ACMA. Alternatively, write a blog entry on how you can report spam. [K] [I] [E]

36.3 ONLINE PRIVACY

Whether you are using the internet to read and send email; engage in e-commerce, social network on sites like Facebook, Tumblr and Twitter; or simply to 'surf the net' (by visiting various websites), **information about you and your online activities are likely to be collected by others.**

The *Privacy Act 1988* (Cth) is an extensive piece of federal legislation that covers privacy law. However, given the international nature of the internet this legislation will often not apply to your online activities. Therefore, the best way to protect your privacy online is to understand some of the risks and some of the technology used to track your online activities, so that you are able control what information you reveal about yourself when using the internet.

Practical application

Visit the website of the Office of the Privacy Commissioner -

www.privacy.gov.au/privacy_rights/index.html

- to understand how the Privacy Act protects your personal information generally.

You may then like to complete the Privacy Quiz for Individuals

www.privacy.gov.au/publications/ten_steps/quiz4ind.pdf

- to see whether you are a 'privacy guru' or not. [l]

PRIVACY FOR EMAILS

Although most people feel that emails are very private, the Office of the Privacy Commissioner has advised that we should remember:

Most email is insecure. Email can be compared to a postcard in that anyone who receives it can read it. Email may also be read if it is stored on servers during transmission.

Emails are hard to destroy. Many people think that if they delete their e-mail it is gone forever. This is not so as most electronic documents are backed up and recoverable.

Logging. Most software used to operate networks, including web servers, mail servers and gateways, log transactions and communications. These logs will normally include the email addresses of the senders and recipients of an email and the time of transmission, so who you are emailing and when can be obtained. System administrators are also capable of reading the contents of emails sent and received by the school or corporate network.

Emails can also be easily forwarded – so don't put anything in an email that you would not want others to see. There have been numerous cautionary tales where someone has put something embarrassing in an email that has been forwarded on and then gone viral, with hundreds and even thousands seeing the embarrassing message.

Case Study

In 2006 Lucy Ga, an Oxford University engineering graduate and an intern at Citigroup bank in London, emailed instructions to about 40 friends who were due to attend her 21st birthday party at the Ritz Hotel. One guest sent the message to a colleague. It then was forwarded around Citigroup, before circling the globe, making newspapers in Britain and the Middle East. Her email was fairly innocuous, she just seemed a little uptight about her party.

Under the heading, INSTRUCTIONS FOR ENTRY, she advised guests how to talk to Ritz staff on arrival: "When asked, 'How can I help you Sir/ Madame?', you reply, "I am here for Lucy's Birthday Party at the Rivoli Bar." If anyone had trouble getting in, "please call my mobile...and my PA Ms Gill [another intern] will kindly deal with your queries between 8:30pm to 10pm." Guests were to arrive at nine, but at staggered 15-minute intervals; the email listed who should arrive when.

1. How did Lucy Gao's email cause her embarrassment? [K]
2. What do these stories say about the nature of modern society? [E]
3. Should individuals be allowed to forward to emails to others? [E]

PRIVACY WHEN SURFING THE NET

Many people believe that, when they surf the internet, they are doing so anonymously, but every time you do, the hosts of those sites accessed are also able to track you and to know your interests and things you like. If you enter personal information they keep that stored after you leave.

This is made possible by the use of 'cookies'. Cookies are small text files that are kept on your computer's hard disk. When you visit a site that uses cookies, any information you give will be stored so that when you leave the site, a cookie is created on your hard disk. The cookie is updated each time you visit the site so that the previously stored data is there and ready for use. Cookies can help you in navigating sites because when you revisit a site they have the information of you already there. For example, if you have ordered a CD from an online site you won't have to re-enter your address details if you order from that site again.

Practical application

Many users are unaware that many of the sites they visit use cookies. Visit the following sites and look for the site's privacy policy or statement (often these policies are accessible by a small link on the bottom of the site's home page). Once you have found each privacy policy or statement, find out whether the site is placing a cookie on your computer's hard disk.

Facebook - www.facebook.com

Gmail - www.gmail.com

The Courier Mail - www.news.com.au/couriermail/

Use the Help settings in your web browser (eg. Internet Explorer, Firefox, Safari, Chrome) to find out how to change the cookie settings for your hard drive. [K] [I]

36.4 CONTENT REGULATION

While the internet has enabled people around the world to communicate, it has also enabled easy access to pornography, violence, techniques of terrorism, and race hate websites. Such material would normally be prohibited if made available in other forms, such as, in newspapers or films. If it is placed online, should, the censorship laws apply? If so, to whom - the person who put the offensive material on the internet, those who accessed it, or the Internet Service Provider (ISP) who facilitates the service?

▶ *WHAT DO YOU THINK?*

Over the past several years, this debate was argued in the Australian media because of a proposal by the Government to require all Australian internet service providers to provide a 'clean' feed to households and schools, free of pornography and other 'inappropriate' material. Ultimately the Government abandoned this proposal, however, there is clearly some offensive and unsafe material on the internet. The key issue is who should be responsible for ensuring the internet is safe for everyone, especially children.

1. Do you agree, or not agree, that governments have a responsibility to prevent people accessing certain information online? Or do you think it should be parents who make those decisions for their family members? [E]
2. Are there other forms of content on the internet that you think should also be banned by the government? If so, what are they? If you feel the government should not control what is placed on the internet, explain your reasons for this. [E]
3. In countries such as China the government regulates the internet very closely. Sites that are critical of the government or the country, or put forward contrary views, are routinely closed. It is argued that once you give power to regulate internet content to any government, it could be used at a future time to limit political debate and viewpoints. Do you think this is a valid or an invalid argument, given that at this stage it is only pornographic sites that are to be targeted? [E]

Issues also arise as to whether content on the internet is **misleading or deceptive**, if so, who is legally responsible? The person or the company who puts the material on the search engine, or the search engine itself. The following case on this issue commenced in 2007 in the Federal Court and was finally ressolved by the High Court of Australia in 2013.

C *Case Study*

Google Inc v Australian Competition and Consumer Commission (ACCC)
[2013] HCA 1 (6 February 2013)

Facts: Google Inc allows for sponsored advertising links to be put on the right-hand side of its pages. If a user 'googles', that is, searches for a particular term, additional advertising links may also come up at the side. The ACCC alleged that Google Inc. engaged in misleading or deceptive conduct as some of the advertisements (or sponsored links) had competitors' names which appeared very similar to the searched term. One example given to the court was that a query in google for 'Harvey World Travel' also gave a sponsored link to the company's competitor, STA Travel but with a URL under the heading 'Harvey Travel'.

Legal issue: Had Google engaged in misleading and deceptive conduct under *Australian Consumer Law 2010* (Cth) by allowing misrepresentations to be made by advertisers in the sponsored links (the Adwords)?

Decision: The High Court of Australia, in 2013, unanimously rejected the ACCC's argument that Google was responsible for whatever advertisers put on sites in response to search queries. Google merely communicated the advertising links without endorsing or adopting their contents.

36.5 SOCIAL MEDIA

Regardless of the appropriate role for government in preventing access to certain information online, the rapid growth of social media would make any attempt to do so increasingly difficult. At the end of 2012, there were 850 million monthly active users of Facebook, 175 million tweets were sent each day, and over 72 hours of video are uploaded to YouTube every minute. As such, it becomes very difficult for any government to monitor and regulate all that content. There are, however, several complex legal issues that have been created by the explosion of social media use over the past few years.

PRIVACY AND SOCIAL MEDIA

Social networking on sites like Facebook, Twitter and Instagram make it very easy to connect with 'friends' by sending messages, sharing photos, music and videos, and interacting with your 'friends' and others through a wide range of applications.

The Office of the Australian Information Commissioner (formerly the Office of Privacy Commissioner), has isued some advice about the potential privacy risks associated with social networking. The advice appears in FAQs available at

www.privacy.gov.au/faqs/ypr/index.html#social_networking

The FAQs offer four main steps people can take to minimise the potential privacy risks associated with social networking sites:

- Know your rights: read the site's privacy policy.
- Be careful what information you share on the site.
- Use the privacy tools on the site – control access to your search listing and profile.
- Make sure your anti-virus software is up-to-date.

With regard to any privacy-related complaints about a social networking site, the FAQs recommend:

- Contacting the site.
- Complaining to the site's 'trust-mark' issuer.
- Calling our Office's privacy enquiries line for advice on 1300 363 992.

WHAT DO YOU THINK?

1. What are the privacy risks assocated with social media? [K] [I] [E]
2. Do you think it is safe to use social networking sites? [E]
3. If you use a social networking site, have you taken the four steps suggested by the Privacy Commissioner? Why or why not? [K] [I] [E]
4. Do you think the recommendations are useful, or not? [E]
5. Is there anything else you think you could do to protect your privacy when using social networking sites? [K] [I] [E]
6. According to a CareerBuilder survey, as many as 56% of employers are checking out prospective employees on social media before they make a final decision. What practical steps can you take to ensure there is not damaging or embarrassing material about you on social media that may impact upon your ability to get a job? [K] [E]
7. Would you give your Facebook password to a prospective employer if you were asked for it in a job interview? Why or why not? [E]

CONTEMPT OF COURT AND SOCIAL MEDIA

In addition to talking about their personal lives on social media, people also comment about politics, sport, culture, and whatever is in the news, including high profile court cases. That means it is no longer just the mainstream media that is publishing information about matters that are before the courts. Instead, it means that everyone who uses social media needs to be careful about the laws of contempt of court, which aim to prevent interference with the administration of justice.

The most relevant form of contempt of court in this context is *sub judice* contempt. Sub judice refers to the period when a case is under a judge. *Sub judice* contempt prohibits the publication of information that will have a tendency to prejudice a case that is currently being hear or is pending hearing in a court.

In order for a person to be guilty of *sub judice* contempt, it must be proved that:

- there was a **publication**;
- the publication was publicised when the **proceedings were pending**;
- the publication had the requisite tendency to **interfere with the administration of justice**.

There have been several high profile criminal cases where people have gone to Facebook and Twitter to comment on the guilt of the accused.

WHAT DO YOU THINK?

When a person was arrested in 2011 for the murder of Daniel Morcombe, many people took to new media, such as Facebook, Twitter and blogs, to talk about the case. Many of the comments assumed the accused was guilty and were quite vitriolic in terms of how they described the accused. Some of the comments also identified and/or set out the history and background of the accused, some of it inaccurately.

This meant there was a very real risk that some of the comments directed at the accused were so damning and critical that it may make it difficult for that person to receive a fair trial. Once Brett Cowan was committed for trial for her son's murder, Daniel Morcombe's mother, Denise, begged supporters to be careful with their comments on social media.

1. In what way could comments posted to social media make it difficult for a person to receive a fair trial? [E]
2. In high profile cases where there has been a great of prejudicial pre-trial publicity on social media, what, if anything, should the court do? [E]

VOL 1 CH 9.3

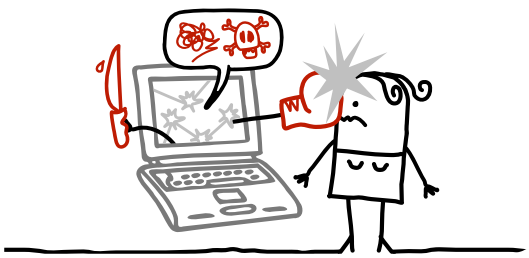
RESEARCH

Most people probably don't realise that the comments they make on social media may make it difficult for a person to receive a fair trial. To help educate the general public on this area of the law, and their responsibilities, create a poster that explains sub judice contempt and contains some practical advice for people when commenting on matters before the court on social media.[I] [E]

DEFAMATION AND SOCIAL MEDIA

VOL 1 CH 18

The laws of defamation also apply to the internet and social media. Defamation was discussed in Volume One at 18. What is posted on Facebook or tweeted **does amount to publication in the eyes of the law**.



Hypothetical

Which of the following scenarios may be considered defamation, and who would be liable?: [K] [E]

- Alice tweets that her friend "Brittany is a slut who can't be trusted".
- Charles retweets Alice's tweet about Brittany.
- Brittany responds by posting to Instagram an embarrassing photo of Alice, with her clothes all wet after she had been pushed in the pool on the last day of school.

LIABILITY OF WEBSITES AND PLATFORMS

An additional legal issue is to what extent should the website or platform also be liable for content, defamatory or otherwise, that is posted to their site.

WHAT DO YOU THINK?

Read the following piece from *The Conversation* 17 February 2012 and think about the following issues:

- Do you think websites or platforms like Facebook and Twitter should also be held legally responsible for things that their users post? [E]
- Do you agree with the author that Australian defamation law needs to be reformed in the way he suggets? [E]

Will Marieke Hardy's Twitter case change Australian law for ever?

By Peter Black

Twitter is being sued for defamation by a Melbourne man who was wrongly identified as the author of a "hate blog" directed at writer and TV personality, Marieke Hardy.

Hardy posted a tweet last year to "name and shame" Joshua Meggitt, the Melbourne man she incorrectly identified as the blog's author, leading Meggitt to sue Twitter for defamation.

While Meggitt and Hardy have already apparently reached a (confidential) legal settlement, the broader issue of Twitter's moral culpability and legal responsibility for allegedly defamatory tweets has now been brought sharply into focus.

This is the first time under Australian law Twitter has been sued for defamation, and it raises three interesting legal questions with respect to the liability of online intermediaries or platforms, such as Twitter, Facebook and YouTube.

1) It represents an application of the High Court's reasoning in the case of Australian businessman *Joseph Gutnick v the Dow Jones* publishing firm. (http://en.wikipedia.org/wiki/Dow_Jones_%26_Co._Inc._v_Gutnick). In that case, the High Court held that a cause of action for defamation arises in all places of publication. (That is, just because the Dow Jones is based in the US, it doesn't mean Gutnick couldn't bring the case to an Australian court.)

So even though Twitter is based in Silicon Valley, it can potentially be held liable for publication in Australia. This decision, while accepted law in Australia, has been very contentious overseas, particularly in the United States.

2) The case highlights the issue of whether disclaimers in the terms and conditions of various websites, such as the one on Twitter, provide legal immunity.

While such disclaimers will likely provide some protection, they will not provide absolute legal protection in all situations. Meggitt also has a strong argument in saying the terms and conditions will not protect Twitter against claims made by non-Twitter users.

3) It is one of the first cases in which the platform – in this case Twitter – rather than the person that actually made the defamatory comment has been sued.

This is novel because, in the United States, s 230 of the *Communications Decency Act* provides immunity from liability for providers and users of an "interactive computer service" who publish information provided by others.

In Australia we do not have an equivalent immunity for platforms such as Twitter, Facebook or even Google. In Australia, platforms will have to rely on either the defence of innocent dissemination or schedule 5, clause 91 of the *Broadcasting Services Act 1992* to avoid liability.

While both these provisions will clearly apply to internet service providers, they are unlikely to extend to provide immunity to platforms such as Twitter or Facebook. That means that, under Australian law, it is possible that platforms such as Twitter and Facebook could be held liable for posts made by their users.

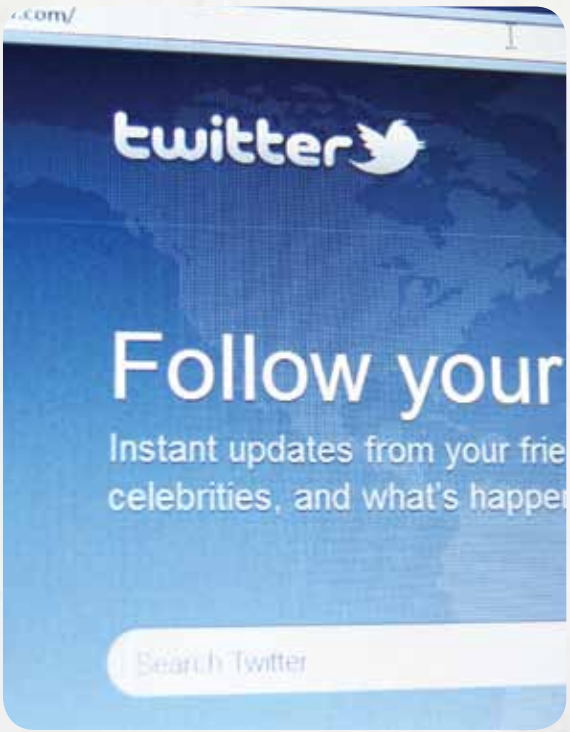
If that is indeed the result in this case, Australian defamation law will need urgent reform.

It is simply not practically possible for these platforms to filter all the content posted to these sites. If the law did require platforms to do so, they would either be forced to pass the considerable costs of doing so on to their members, withdraw from Australia altogether or change the very nature of their platform.

Moreover, if Australian law did place this burden on platforms, such a regulatory framework would be a powerful disincentive to innovative new services being developed and based in Australia.

The simple solution could be that, where defamation takes place on the internet, the individual who posted those defamatory remarks should be held responsible. Alternatively, if the legislature wishes to impose an additional level of liability upon online intermediaries and platforms, it should do so only where such an intermediary and platform fails to take account of a defamatory comment once they have been given notice.

A notice and takedown regime has similar antecedents in existing legal frameworks. With respect to copyright, the US *Online Copyright Infringement Liability Limitation Act* and s 116AG of the *Australian Copyright Act 1968* limits, in certain circumstances, the remedies available against carriage service providers to taking down infringing material, terminating a specific account and/or disabling access to an online location outside Australia.



In essence, the law is still struggling to keep up with rapid advances in technology over the past few decades, and this case has the potential to expose some weaknesses in Australia's existing defamation law with respect to online intermediaries and platforms.

It will definitely be a case to follow (both on and off Twitter).

REVIEW

1. What is the law of cyberspace?
2. What is the term given for doing business electronically?
3. What function is served by the *Electronic Transactions Act 1999* (Cth)?
4. Which legislation supplements this Act in Queensland?
5. What is the legal status of electronic transactions in Australia?
6. If a person does not give permission to an electronic communication being sent, can they be bound by it?
7. Where is an online contract made?
8. What technology has been developed to make e-transactions more secure?
9. Is the sending of spam lawful?
10. What are three conditions that need to be met for an email to be considered spam?
11. What messages are exempt from the *Spam Act 2003* (Cth)?
12. List four reasons emails raise privacy concerns?
13. What is a cookie?
14. What steps can you take to help ensure that your use of social networking sites is safe?
15. What is sub judice contempt?