GUIDE TO SOCIAL MEDIA
RISKS AND OPPORTUNITIES FOR BUSINESS
## Contents

**Introduction**  
What do we mean by “social media”?  
What do you need to consider?  
Social media providers’ terms of use  
The standard terms  

**Creating and maintaining a social media presence**  
Planning and establishing a social media presence  
Establishing social media communication responsibility  
Social media governance strategy  
Promotional activity and advertising issues  
Continuous disclosure obligations and social media  
Discrimination  

Why you should monitor your own social media sites for objectionable content  
What should you do when you find objectionable content?  
Responding to negative comments  
Should you remove content?  

Recordkeeping  

Protecting your reputation from attacks by others on social media  
What types of attacks could be made?  
Trolling  
Sock puppets  
Astroturfing  

Intellectual property and confidentiality  
Copyright  
Trade marks  
Breach of confidential information  
Fake pages and fraudulent accounts  
Monitoring third-party social media sites for content  
What are your options for defending yourself?  
Who’s liable for content?  
Self-help mechanisms  
Taking down fake sites  
Defamation and corporations  
Misleading and deceptive conduct  
Injurious falsehood  
Discrimination  
Criminal sanctions for trolling  

**Practical steps and matters to consider**  
Litigate or engage?  
Developing a crisis management plan  
Assessing the risk in user-generated content on third-party sites  
How will you respond?  
Steps to take to get material removed from third-party sites  
Where is something “published”?  
Obtaining social media content for use in litigation  
Issuing subpoenas on social media operators  

**Employee use of social media**  
Employee social media policy  
Awareness training  
Branded feeds on Twitter and ownership of customer lists  
An employee’s LinkedIn profile  
Contractors  

Personal vs professional comment on social media  
Policies and training: Stutsel v Linfox  
Connection with business: Fitzgerald v Escape Hair Design  
Threatening behaviour and out of hours “posting”: O’Keefe v The Good Guys [2011] FWA 5311  

**Key contacts**
Introduction

Even if your business never has a social media presence, your employees, competitors and detractors all will (not to mention fraudsters), so you do need to understand how it works and have a social media policy of some sort.

In our Guide to Social Media: Risks and Opportunities for Business, we set out the practical issues your business will need to consider, whether you’re creating your own social media account, or dealing with others’ use of their own.
What do we mean by “social media”?

“Social media” covers a variety of web-based or mobile technologies that turn published communication into interactive dialogue.

Publishing content through social media is not the same as publishing content to other web-based platforms, although both involve the uploading of material to the internet. Traditional publication in an online format is static; publishing through social media commonly invites a response and can lead to conversation between the publisher and one or more readers – or just between readers.

There are a number of characteristics of publishing through social media that distinguish it from website-based publication, including:

• it allows the uploading and creation of user-generated content, often simply referred to as “UGC”;
• online communities can be established in which users participate in the publication;
• providing for multiple interaction with an online conversation (for example, facilitating the direct interaction with other users or contributors to the social media platform); and
• content can be shared very quickly and widely.

What do you need to consider?

A fundamental starting point for risk management with social media is the extensive limitation of liability that social media providers impose through the disclaimers contained in their terms of use. Those disclaimers of liability effectively eradicate legal avenues of redress against social media providers by third parties.

There are two main issues to consider:

• do you have a broad risk management strategy to cover a variety of uses of social media that affect the business, such as reputation management and employee use of social media?
• what are your goals and strategy to establish a social media presence, if any, for your business, and does your risk management strategy deal with the additional risks arising from your active participation?

Relevant social media use (and misuse) will generally fall into one of three categories:

• Creating and maintaining a social media presence: The company has to determine its own presence within social media: which sites it chooses to have an official presence on, who is responsible for keeping the content of that presence up to date (and, where applicable, ensuring that no changes to the content have been made by unauthorised third parties).

• Protecting your reputation from attacks by others on social media: This could occur through one or more of the social media sites or on sites that the business does not own or has no control over. It could originate from an employee or group of employees or from people previously unknown to the company.

• Employee use of social media: Use of social media sites by employees will encompass a number of issues such as using social media in work time, potential workplace harassment via social media, the potential for disclosing confidential information or denigration of the employer.

You’ll need to have policies that deal with all three of these categories.

Social media providers’ terms of use

Users enter into a contract with the social media provider as soon as they register to use the services of a social media platform. That means that even though no money passes hands, their use of the social networking site is governed by a contractual relationship between the registered user and the social media provider.

The terms of the contract are recorded in the social media providers’ terms of use, generally found on the relevant website. The contract is governed largely by standard terms of use that are published on the social media’s site “as is” – there is no opportunity to negotiate those terms.
For this reason it is important to become familiar with those terms.

All social media platforms have terms of use that are relatively similar and largely based on US law (as most of the social media providers are US owned). They generally cover:

- data security;
- the protection of minors;
- privacy;
- defamation;
- consumer protection; and
- intellectual property rights.

However, it is important to note that there is no contractual relationship between users of the same social media site. While this may seem obvious, it is an important point as it means that a business with a social media presence that has a dispute with another user of the social media platform, for example, over intellectual property infringement, would need to resort to the usual laws and remedies applicable between parties when a dispute arises.

The standard terms

Standard terms generally include the granting of a licence by the registered user to the social media provider giving it permission to host and publish the material uploaded content (otherwise known as user-generated content) on the social networking site.

However, ownership of the material is retained by the poster, not the social media provider. The corollary of this is that responsibility for the content of that material lies with the poster, not the host, which generally disclaims all liability for user-generated content.

The standard terms of use include a comprehensive indemnity granted by the registered user to the social media provider for third-party claims resulting from the registered user’s use of the social media site.

Most social media providers are based in the US, in particular in California, and for this reason their standard terms include choice of law and dispute clauses that are governed by Californian law.
Social media is interactive and operates in a content-driven, information-sharing, fast-paced environment. It is dangerous to assume that a business may establish a social media presence by publishing information in the same manner as posting information to the company’s website. Social media publication is by its nature interactive and can go viral in minutes, so social media sites must be carefully monitored.

The main issues you will need to consider are:

- who will be responsible for what you say?
- what you can say – and how you can say it; and
- how you will monitor or respond to any user-generated content on your sites.

If you are attacked online it will not be limited to your own social media sites, but we’ll deal more generally with crisis management in the next chapter – here we will focus on what you say and control on your own sites.

Planning and establishing a social media presence

The starting point is simple: get in first and register before someone else uses your brand and/or name. Pirate or fraudulent sites and cybersquatting are common and take time and resources to remedy.

Creating and maintaining a social media presence

This includes registering business names, brands and products or services. Most social media providers have separate terms of use that deal with branded pages and may even have specific applications for the creation of branded pages. They will also regulate the use of their logos (for example, using the Facebook logo to link to a branded Facebook page from a corporate website).

Generally, once a user name has been registered by its proper owner, a social media provider will not allow that same name to be reused by a different user or entity. There is no fee for registering a user name with social networking sites like Facebook, Twitter and LinkedIn.

Most social media providers have their own set of rules of publishing behaviour that a registered user adopts under the standard terms of use. These guidelines restrict the content of uploaded material and typically deal with offensive language, nudity, pornography, hate speech and intellectual property infringements.

Establishing social media communication responsibility

You need to identify and appoint members of the in-house legal team or corporate communications team who will be responsible for your business’ social media sites, publishing news items or updates, and responses to others’ comments.

Social media governance strategy

The purpose of a good governance strategy is to ensure the in-house legal team or corporate communications team:

- implements and then maintains its approach to social media;
- retains control over the business’ publication on social media; and
- monitors and responds appropriately to the interaction generated through social media (ie. user generated content).

A governance strategy should cover:

- what types of information can be released via social media, and what cannot (such as confidential information);
- who has responsibility for the types of communication;
- any internal sign off required before publication;
- how social media content traffic is to be monitored and by whom, including outside business hours;
- details of the administrators for each of the social media sites;
- out of hours access to social media accounts when required;
- general risk minimisation;
- intellectual property rights infringement and what to do when this happens;
• compliance with any advertising regulations;
• the use of branding and the control of marketing strategies through social media;
• compliance with disclosure rules (ASX listed companies);
• liability to third parties for the content of social media pages; and
• social media use by employees.

A social media policy that governs the official business use of communication through social media will be a useful risk management and training tool for every business with a presence on social media platforms. You’ll also need to develop one specifically for employees, which we deal with in chapter 4, “Employee use of social media”.

Promotional activity and advertising issues

As a starting point, any promotional or advertising activities on social media must comply with the law. Both courts and the advertising self-regulation system administered by the Advertising Standards Bureau treat advertising on social media like any other form of advertising.

You will need to identify and comply with:

• any industry-based regulations in the various jurisdictions your business operates in; and
• any applicable laws, such as the prohibition on misleading and deceptive representations under the Australian Consumer Law.

Organisations that participate in the advertising self-regulation system administered by the Advertising Standards Bureau rules will need to monitor and moderate all content posted on their Facebook pages and other social media tools to ensure compliance with the requirements of the advertising codes.

A promotional competition may also require prior permit approval (effectively a licence to run the competition) from State lottery regulators (depending on the nature and prize value of the competition). This is an emerging and complex area of law. State regulation may be extended to neighbour states if competitions are run through social media and are accessible in other states and therefore exceed traditional state boundaries and may constitute advertising in many states and not just the one where the competition or promotional activity was originally devised.

That is not the only set of rules you must comply with. The major social media providers regulate the use of advertising and promotional campaigns conducted through them. It is common for businesses to use their branded social media pages as a vehicle for these activities.

You must take care when promoting products and services through social media platforms as these activities are often affected by specific terms of use that govern promotion and advertising through social media sites.

For example, Facebook allows promotions to be run on business pages or within its Apps site (for example, “comment/like our Page to enter” is permitted), but not on personal pages (for example, “share on your Timeline to enter” or “share on your friend’s Timeline to get additional entries” is not permitted). Facebook also has specific requirements regarding liability.

Continuous disclosure obligations and social media

Under its revised guidance note on continuous disclosure, ASX is now requiring listed companies to more actively monitor what is being said about the company on social media. The need to do so is of particular importance where a listed company is withholding material price sensitive information from the market on the basis of the exceptions to the continuous disclosure obligations, one of the requirements for which is that the information is confidential. ASX says that, in these circumstances, companies need to monitor social media where it knows there are regularly discussions about the company to ensure that there has been no leak of that information. If the information appears on social media, ASX considers that confidentiality has been lost and the company will be required to immediately disclose the information to the market.

Despite this, both ASIC and ASX have warned companies that they cannot use social media outlets such as Twitter and Facebook as primary communication channels for the release of material price sensitive information.
That said, they have stated that social media may be used as a secondary communication channel so long as the first announcement is made to the ASX, and that care is taken to ensure the social media channel is able to convey the announcement accurately and is not misleading.

Their principal concern is the use of Twitter with its 140 character limit, which may lead to the truncating of the announcement in a manner that may mislead the public. Effectively, both regulators have suggested that the use of social media for secondary announcements be limited to statements that the listed company has made an announcement to the ASX.

Discrimination

Various forms of discrimination may arise through the misuse of social media. Comments and material that is aimed at certain individuals that may constitute discrimination may be particularly damaging to an organisation and if not dealt with appropriately may bring into question vicarious liability for that discrimination. Organisations should seek to monitor for such content and act appropriately (with legal advice as required) when it occurs.

In 2012, in an Australian case that dealt with breaches of the Racial Discrimination Act 1975 (Cth), the vicarious liability for publication and moderation of online content point was further examined.

Case studies: Francesca Holdings and Netflix

Francesca Holdings is a listed clothing company in the US. Its chief financial officer, Gene Morphis, shared his thoughts on Twitter and Facebook about many things, including his company’s financial position, often before it was released to the market, such as:

“Roadshow completed. Sold $275 million of secondary shares. Earned my pay this week.”

“Board meeting. Good numbers=Happy Board.”

“Earnings released. Conference call completed. How do you like me now Mr Shorty?”

He was terminated for improperly communicating company information.

A US listed company, Netflix was recently investigated by the SEC over comments made about the company’s performance by its CEO through his own personal Facebook page. While no enforcement action ensued, the SEC did make it clear that while it regarded the use of branded or official social media outlets as appropriate vehicles for information that would be of importance to its investors, it warned that the use of personal social media accounts of company executives was unacceptable.

In Clarke v Nationwide News Pty Ltd t/a The Sunday Times [2012] FCA 307, the conduct which was found to be unlawful was the publication of comments made by readers (ie. third parties) of the online news service operated by the respondent on its perthnow.com.au website.

The statements that were published and which were approved by a moderator of the defendant (which is a subsidiary of News Limited) were found to have caused lasting offence, humiliation and intimidation to the complainant.

Why you should monitor your own social media sites for objectionable content

A number of recent decisions involving user generated content posted to social media pages has brought into question the legal liability for publication. The role a site administrator or moderator might undertake when dealing with user generated content could be problematic.

As a result you should monitor and, where necessary, moderate or remove users’ posts on your own sites.

This will involve the setting up of policies so that there is constant monitoring of brand use and customer feedback and other comments posted or blogged on branded social media sites, and appropriate procedures for dealing with them.

Monitoring of sites is now a serious consideration for branded pages and reputation management generally, so you will need to pay careful attention to how it will be conducted, who will do it, and the level of internal reporting of content.
This should include considering monitoring of social media traffic outside business hours as many social media disasters occur late at night or over the weekend.

The ACCC views posts to branded social media pages as advertising and will consider whether such posts breach consumer law if a complaint is made. Any false or misleading comments that appear on social media pages as part of a business’s marketing communication, regardless of whether it is user-generated or generated by the business, may be held to breach consumer law.

The ACCC has warned businesses that they are responsible for making sure that the content on their social media pages is accurate and that it expects well-resourced companies to take down misleading comments within 24 hours of publication, with more flexibility given to smaller businesses depending on when they become aware of the comments.

To comply with that obligation may well require extensive and sophisticated monitoring to the point where a business may not have sufficient resources to be able to do so.

Case study: ACCC v Allergy Pathway (No.2) [2011] FCA 74

The Australian Competition and Consumer Commission (ACCC) alleged that Allergy Pathway was in breach of an earlier undertaking to the Court that it would not publish misleading representations about the company’s services, by publishing offending representations in statements posted on its website and its Facebook and Twitter pages.

The publications included testimonials written and posted by clients on Allergy Pathway’s Facebook wall. Allergy Pathway knew that people had published testimonials on its Facebook page and it took no steps to have them removed.

The Court concluded that although Allergy Pathway was not responsible for the initial publication, Allergy Pathway accepted responsibility for the publications when it knew of the publications and decided not to remove them. It therefore became the publisher of the testimonials, and in breach of its undertaking to the Court.

Although this case focused on whether Allergy Pathway could be said to have published the testimonials, it seems to stand for the wider proposition that an organisation may be found liable for misleading or otherwise unlawful content posted by a third-party on its social media site if it knows about the content and chooses not to remove it, because in those circumstances it may be regarded by users as having adopted the content.

What should you do when you find objectionable content?

First, report the content to the appropriate communications team and or legal department immediately and continue to monitor social media sites for further activity. There will be a different approach depending on whether the content is posted to a social media page owned by the business or on a third party site over which the business will have no control.

You must act promptly to review content if a complaint is received from a third party (in particular, the complaint will be evidence that the business is now aware of the relevant content).
Responding to negative comments

This will involve establishing policies and procedures that ensure that moderation/removal or response to content is effectively and quickly dealt with.

Those policies should incorporate a clear procedure to provide a mechanism through which an official response to any criticism levelled at the business is properly handled by the right person in the business.

Should you remove content?

Consider removing the content from the website or social media pages you have access to. Consider any likely repercussions once material is removed. Adopt a clear communication strategy to deal with any backlash.

You should be mindful that preservation of the social media content may be vital if later proceedings are likely to ensue. You may need to seek specialist IT assistance before removing content from the site.

Recordkeeping

Since social media platforms are usually hosted by third parties and are web-based, businesses can’t rely on them to capture and record both their use and third-party interactions because:

- typically under their terms of use, the user who posts material retains ownership in that material, but doesn’t have access to the native format of the information and its metadata; and
- there is no guarantee of long-term access to material posted online.

It is imperative for businesses to record their social media communications for a number of reasons.

Firstly, communications on social media platforms are of corporate value to businesses as they express corporate thinking and knowledge.

Furthermore, recordkeeping is essential as evidence of social media communications can be required in a number of forums, including litigious proceedings. For example, in a defamation action, a business may be asked to provide detailed evidence of Facebook messages and responses to demonstrate if the business published defamatory material.

In this context, the only way to manage these social media risks is to have recordkeeping policies that enable businesses to accurately capture their communications and third-party interactions.

Currently, there is no uniform record-keeping standard in Australia. At present, policies released by the Queensland Government and the Public Record Office of Victoria provide the most guidance on establishing efficient recordkeeping practices. For example, the Queensland Government Enterprise Architecture policy concerning the Official Use of Social Media Guideline recommends capturing:

- the date of discussion or business activity;
- the name of the person who used the social media;
- the name of key stakeholders involved;
- the main discussion points;
- the details of instructions or advice provided; and
- any approvals, decisions or recommendations made.

Creating and maintaining a social media presence

Remember...

Work out who in your organisation will be responsible for your social media presence and ensure they understand what they can and cannot say.

Social media is not the Wild West – the same law applies to your comments whether you’re online or offline.

You might be responsible for others’ posts on your social media sites, so ensure they are moderated.
Protecting your reputation from attacks by others on social media

“Falsehood flies, and the truth comes limping after it.”
– Jonathan Swift

Whether your business is on social media or not, others are, and not everything they say about you will be true.

The disparagement of businesses by employees and third parties through social media is prevalent and affects businesses across the globe. Where it attracts media headlines, conduct of this type can be very damaging. Not only can it go viral very quickly, as with any other type of online information, material posted to social media sites can resurface long after it was deleted from its original location. Its potential for damage is therefore far greater and longer lasting than that of damaging print publication.

Social media may pose significant reputational risk to organisations, but protecting the reputation of a business may be difficult. It is important that every organisation has in place internal procedures to enable a timely and swift response when facing a reputational attack or crisis.

What types of attacks could be made?

Trolling
Trolls are individuals who have established campaigns against certain types of economic, political, or commercial activities and regularly engage in online forums and internet exchanges to harass or discredit those with whom they communicate.

They post offensive, defamatory and inappropriate content to deliberately provoke an emotional reaction from those who administer the site and/or the group members belonging to the site.

Sock puppets
Sock puppets are fake identities created to inflate a product or service, or offer praise or condemnation for a politician or other person. Some notorious examples have included well known writers who have posted comments praising their own work via their pseudonym.

They differ from pseudonyms used online in that they are deliberately adopted to deceive the reader into thinking they are genuine users or supporters of a product or service.

Astroturfing
Astroturfing is engineered or commercially obtained fake support for a cause, product or even political campaign.

It is not an exclusive social media issue but is easier on social media and can be very cleverly disguised, especially if created by well funded PR companies.

One example is the creation of multiple online identities that are then used to flood a corporate social media page with false or inflated claims.

Where astroturfing is deployed to falsely advertise a product or service it may be misleading and deceptive advertising under the Australian Consumer Law and it may also breach the codes of conduct of Australian advertising associations and PR associations.
Case study: Greenpeace’s orchestrated attacks through social media

Greenpeace targets Nestlé

Nestlé uses palm oil from Indonesia. Greenpeace argued the destruction of Indonesian rainforests to make way for palm trees reduced the orang-utan’s natural habitat. Greenpeace uploaded a spoof advertisement based on the KitKat advertising slogan “Have a break” to YouTube. In addition, the Kit-Kat logo was altered to read “Killer”. The YouTube advertisement attracted over a million views in the short period of time it remained on the site and was swiftly picked up by the media.

Nestlé managed to have the advertisement removed from YouTube (partly on the basis of infringement of the use of its logo). That outcome led Greenpeace to encourage its supporters to bombard Nestlé’s Facebook page and website with written protests urging Nestlé to stop buying palm oil from its supplier. Again, Nestlé responded by threatening to remove any comments left there that allegedly infringed its logo. Many Greenpeace supporters when posting comments did so by adopting the altered “Killer” logo as an avatar accompanying the comment. It did not stop the protest action and Nestlé eventually retreated from the position it had adopted. Further, Nestlé stopped buying palm oil and set up a collaboration with The Forest Trust to work towards a zero deforestation policy.

Greenpeace and Shell Oil

Greenpeace was again involved in a sophisticated and orchestrated attack on Shell Oil via social media.

Fake but provocative Shell Oil advertisements created by Greenpeace were set up to look like official Shell advertising campaigns lampooning the Shell Oil slogan “Let’s go”. They deliberately adopted an uncaring attitude towards the environment and the impact of global warming on the loss of the Arctic glaciers. Shell media threatened to take action against UGC posters commenting on the fake sites and fake adverts – all of which was quickly picked up and widely reported in traditional media. Shell threatened breach of trade marks, and action for the defamatory nature of the fake advertisements. Shell used the self-help regime for reporting and instigating take down procedures to have the fake advertisements taken down from YouTube.

Intellectual property and confidentiality

There are two forms of intellectual property that are likely to be relevant in dealing with social media.

Copyright

Of particular relevance in the social media context is copyright. For years, social media sites (for example, YouTube) have grappled with users uploading huge amounts of content which infringe the rights of third parties.

The company will own copyright in all the documents produced by its employees or produced by contractors where there is a copyright assignment in place. Therefore, if a social media attack involves misuse of company documents, it is more than likely that the company will own copyright in those documents and this copyright ownership can be asserted as a means of having the document removed from the social media site in some circumstances.

The primary reason for social media providers taking swift action against content which allegedly infringes a third party’s copyright is that it is necessary for them to do so to rely on the safe harbour protections contained in statutes such as the Digital Millennium Copyright Act (US).

Trade marks

The company’s various brands are valuable intellectual property rights. Brands include registered trademarks but it can also include unregistered marks which are used by the company and are distinctive of its goods and services. These are valuable property rights and the value needs to be
protected. Simply reproducing a registered mark will not necessarily infringe the owner’s trade mark rights. If, however, a user pretends to be a representative of the company, this may well infringe a trade mark.

Breach of confidential information

Confidential information is often thought of as an intellectual property right, but commercially sensitive information, while potentially very valuable, is not property and it is not treated in the same way as the intellectual property rights of trade marks and copyright.

The key to dealing with breach of confidential information is urgency. The intentional or unintentional disclosure of confidential information needs to be removed swiftly. The self-help mechanisms that social media sites provide will be beneficial here. Following removal of the content, consideration should then be given to the appropriate action.

Fake pages and fraudulent accounts

There has been a rise in the number of false or fake social media accounts created in the name of a business or an individual and websites that use the trade marks of a business. Some of these websites are sophisticated and structured in such a way that the fake site is the first site returned in the search results generated by search engines such as Google.

Monitoring third party social media sites for content

You will need to monitor third party sites for mentions of the business and its products and senior employees. This may require the use of social media monitoring tools and help from your IT department.

At the most basic level you can rely upon social media providers’ simple email alerts sent whenever content is added to a page. At the other end of the scale there are sophisticated third party software products that constantly monitor both branded and third party sites for specific content and alert you to new content.

As with your own social media sites, third-party sites will be actively used out of business hours, so you will need to pay careful attention to how you will cover this on the weekend and late at night, and be ready to respond swiftly.

What are your options for defending yourself?

Who’s liable for content?

First and foremost, social media providers disclaim ownership of the material posted to their sites. Generally, most social media providers’ standard terms of use state that a registered user grants the social media providers a licence to host and publish the material, but ownership of material is retained by the poster.

The main social media providers disclaim liability for the use of the services they provide and limit their responsibility extensively as set out in their terms of use.

Self-help mechanisms

All social media companies have significantly tightened up their self-governance regimes in the face of numerous attempts worldwide to find them vicariously liable for the content they host on social networking sites. Social media providers will take action against those who infringe the rights of others, including removing content that is said to infringe copyright or other intellectual property rights.

Invoking the various self-help procedures remains the most effective way of getting content removed from sites that a business has no control over.

The major social media providers have adopted detailed self-regulatory and other voluntary methods to assist those who complain about content of the information posted to social media sites.

Exerting pressure on social media operators to take down damaging content is often the most effective way of securing its removal unless the poster of the information is known to the organisation and direct negotiation with the poster of the information is likely to be successful.

These procedures allow for:

• reporting fake accounts or other offensive material;
• take-down policies for the removal of damaging or offensive material;
• infringements reporting and take down of intellectual property rights;
• complaint handling processes for disputes, including processes for breach of intellectual property rights; and
• blocking or banning of persistent offenders.

To seek removal by the social media provider itself, you must report that material as containing content that is offensive or otherwise contrary to the social media provider’s terms of use or guidelines. All social media sites have procedures to deal with copyright or other intellectual property rights infringement.

There is also the Cooperative Arrangement for Complaints Handling on Social Networking Sites to consider. This voluntary and non-binding arrangement brings together Facebook, Google (YouTube), Microsoft, and Yahoo! (as at 16 January 2013) who have agreed to a cooperative arrangement in an effort to promote digital citizenship. As yet, Twitter has yet to commit to the arrangement, although the Government has indicated that the parties are in discussions and has placed public pressure on Twitter to embrace the protocol, singling it out as a popular medium for cyber-bullying and trolling.

The Cooperative Arrangement stipulates that these Social Networking Sites have in place complaint mechanisms for reporting inappropriate content, contact or behaviour, and review processes for reviewing and acting on complaints promptly.

Taking down fake sites
Fake sites can be removed by a social media provider. Often you will need to invoke their reporting and take-down procedures. It is possible to deal directly with a social media provider but this is complex. Very serious matters, eg. hate sites may need to be removed very quickly and often it will be necessary to involve the police to exert pressure on the social media provider.

A registered user responsible for the fake site may be blocked by the social media provider from establishing a further site in the same or similar names. Fake sites frequently involve intellectual property breach. Social media providers generally act in these sorts of matters as they wish to preserve legislative protection afforded to them under local laws that will ensure they are not held responsible for vicarious breach of intellectual property rights.

Defamation and corporations
Most corporations1 cannot sue for defamation following the passing of the uniform defamation legislation in Australia. That said, corporations of any size may still avail themselves of the statutory defences to defamation. For example a company may claim the defence of innocent dissemination in relation to liability for defamatory comments it hosts on its website or through social media.

Accordingly, there have been limited matters alleging business defamation brought under the uniform defamation legislation. Where executives of a business have been closely connected to or identified with the defamatory material posted they may be able to bring a claim for defamation in a personal capacity under the uniform defamation legislation.

Pursuing a claim in defamation is expensive and is subject to only limited damages awards for a successful plaintiff. Further and significantly, only in very exceptional circumstances would an individual be able to have a defamatory statement or publication immediately removed or withdrawn on an urgent interlocutory basis.

There may also be problems in pursuing a publisher of user generated content where the provider has disclaimed ownership and responsibility for the content of the information hosted or published on their sites. That said, there have been a number of examples of people claiming to have been defamed by users of social media pages commencing actions against social media providers.

For example, Joshua Meggitt from Melbourne has commenced a claim against Twitter Inc. in the US for comments (wrongly) attributed to him by the writer Mareike Hardy in a case of mistaken identity. Hardy named Meggitt as the person responsible for hateful comments made about her. She encouraged her many Twitter followers to join her in naming and shaming Meggitt.

She later apologised to Meggitt and they reached an out of court settlement. Meggitt has now also sued Twitter as a publisher of the tweets and retweets that defamed him. It should be noted that even if Meggitt’s claim is upheld in the US, Twitter is likely to rely on its indemnity under the terms of use for third party claims for user generated content.

1 There is a distinction made between corporations and not-for-profit companies – the latter may sue. Corporations with 10 or fewer employees may also sue.
The approach to examining whether an action for damage to business reputation arising through online publication (be it through social media or a traditional website) involves the consideration of three questions:

- Who is the publisher?
- Does the published content contain defamatory imputations?
- Is there a defence?

Misleading and deceptive conduct

There is a general prohibition on misleading and deceptive conduct in trade and commerce under section 18 of the Australian Consumer Law. While this could be an alternative to a traditional defamation claim for a company, it will not always be an appropriate or effective alternative to pursuing redress for business defamation, given the difficulty in establishing that the other party’s conduct was “in trade or commerce”.

Injurious falsehood

Corporations have another potential cause of action through the tort of injurious falsehood.

A company may bring an action in tort for damage to business reputation claiming injurious falsehood.

This is not the same as a defamation action and the defences available in defamation do not apply (for example, the defence of innocent dissemination is not available). In order to bring a successful claim based on injurious falsehood, however, it is necessary to satisfy the court not just that the alleged infringing statement is false, but also that there was malicious intent on the part of the party making the statement. This may be very difficult to prove.

Accordingly, the avenues of legal redress available to corporations in respect of damaging statements that may be made about them on the internet are sometimes limited and, to the extent that they are open, sometimes difficult to advance.

Discrimination

To the extent that social media content is discriminatory of the organisation’s employees, it may be necessary to rely upon the provisions of the Racial Discrimination Act 1975 (Cth), the Disability Discrimination Act 1992 (Cth) and the Sex Discrimination Act 1984 (Cth) and other State and Territory equivalents for the purposes of proving unlawful content and in aid of swift removal from the social media platform with the co-operation of the social media provider.

Criminal sanctions for trolling

Where individuals have posted damaging or hurtful content to social media sites and a criminal offence is alleged, local police might assist with the removal of that content by the perpetrator under their direction.

In the UK, a number of people have been convicted for trolling using section 127 of the UK Communications Act 2003 (improper use of public electronic communications network). The equivalent offences in Australia relate to the misuse of carriage services or the internet and exist under the Commonwealth Criminal Code (Part 10.6) as well as under a number of state criminal codes. For example, the first Australian to be jailed for trolling in 2011 was convicted under the Queensland Criminal Code, section 474.17(1) for offences that included the use of a carriage service in an offensive way.

Case study: Adam Kaplan & Anor v Go Daddy Group Inc

Adam Kaplan & Anor v Go Daddy Group Inc [2005] NSWSC 636 was an action for the tort of injurious falsehood. The defendant created a website using the domain name www.hunterholdensucks.com.au and a disparaging blog about the plaintiff that encouraged other users to post derogatory comments about the plaintiff’s business. Comments were posted to the blog, all of which contained defamatory comments about the plaintiff’s business. The plaintiff applied to the NSW Supreme Court for an injunction to prevent the Go Daddy company that hosted the website, from maintaining the defamatory blog.

The Court granted the injunction saying that there was a serious question to be tried as the defendant had committed and threatened to commit the tort of injurious falsehood by posting the false comments about the plaintiff in his blog. The matter did not proceed any further after the initial injunction application, so there was no further consideration as to the vicarious liability of the website host for defamatory comments posted on the blog.

Protecting your reputation from attacks by others on social media
Practical steps and matters to consider

Litigate or engage?

Before embarking on litigation, a business should first consider enlisting the help of the social media platform to remove content posted by another user.

If the poster is known, you should also consider whether a direct approach and request for removal might be a more practical way to have the material removed or a site or page sufficiently altered so that there is little danger of confusion arising as to the genuine social media site or page. As noted above, all the major social media providers have self-help mechanisms that deal with the reporting of and take down of material that is in breach of intellectual property rights owned by others.

In addition a business will need to consider carefully the right approach to adopt. A heavy-handed approach may be unwise if it alienates the followers of a satirical Twitter profile, whose unhappiness could then pique the media’s interest. Unless the material is significantly damaging and offensive it might be more appropriate to acknowledge the joke and seek some clarification or assistance from the poster if there is a likelihood that the fake site may be confused with the genuine site.

It should be noted that most social media providers are not willing to assist one registered social media user in a dispute against another social media user. It may be difficult to seek their specific assistance and obtain a response from their legal department.

A business should in this case consider seeking external legal advice.

Developing a crisis management plan

Developing a crisis management plan or procedure will assist the business in its response to any attack.

An effective Crisis Management Procedure that can be implemented swiftly to protect the company’s reputation might:

- list the key managers and contact details for out of hours emergencies, particularly IT assistance;
- document the main administration accounts and passwords for all the company’s social media accounts and its website; and
- set out the communications policy for reputation management through dialogue and responses to bloggers and tweeters. Who is responsible within the organisation, and what strategies might be adopted to assuage negative sentiment or expressions of dissatisfaction and complaint?

As it may be important later if legal action is contemplated, additional steps may need to be documented to maintain evidence of material and provide some guidance about seeking expert forensic IT assistance to not only preserve that material as evidence but also possibly to identify the perpetrator.

Case study: The Streisand effect

In 2003, Barbara Streisand reacted strongly to what she considered to be a gross invasion of her privacy.

Photographer Kenneth Adelman and Pictopia.com had included an aerial photograph of her mansion in a publicly available collection of 12,000 California coastline photographs. Adelman defended his action by stating that he was photographing beachfront property to document coastal erosion as part of a government commissioned project.

Streisand sued them for US$50 million in an attempt to have the photograph removed. Before she commenced her proceedings, the photograph had been downloaded only six times; two of those downloads were by Streisand’s lawyers. As a result of the case, public knowledge of the picture increased substantially, resulting in more than 420,000 people visiting the site in the following month.

To add insult to Ms Streisand’s sense of injury, not only had her litigation led to more exposure, not less, of her property, it was also thrown out of court. Ouch!

Protecting your reputation from attacks by others on social media
Assessing the risk in user-generated content on third-party sites

Is the content satirical or otherwise harmless (albeit undesirable)?

Is the content about an unsatisfactory customer experience, or employee-related but otherwise not hateful or defamatory?

If the content is considered damaging, gather the appropriate response team, which may be part of a crisis management plan developed by the business to follow when a social media site is under attack.

Can you identify the perpetrator (poster of the information)?

Is the perpetrator known to your organisation? Can you persuade the perpetrator to take it down? Refer the matter to your in-house legal team or corporate communications team first.

How will you respond?

Is the perpetrator or poster of information an organisation that stands for social change or environmental protection? Is it a legitimate organisation or a troll posing as an entity with legitimate social justice or human rights causes? Ensure that those with responsibility for official comment within the business are kept informed and monitor all activity through social media initiated by the organisation.

All activity must be closely monitored and a strategic approach taken to responding. In some cases a direct response will be extremely unwise. In particular, avoid a “shoot from the hip” response however provocative the material – it is posted with the intention of producing an emotional reaction and in all probability it is the emotional reaction that will be exploited by further action from the troll or rager. In such cases, once a response is given, the troll’s campaign is likely to be stepped up and could end up in mainstream media if not handled with care.

It will be important to engage appropriately. For example, if legitimate concerns are being raised, acknowledge the importance of the issues that have been raised and offer to discuss or engage positively to assist the resolution of the matter. It may be preferable to seek to engage on the issues raised rather than seek resolution by threatening to take action against any breach of intellectual property rights or raising question marks over defamatory content, etc. Be sure to keep the relevant communications team informed and be prepared for media interest.

If the posted material is factually inaccurate or even wrongly attributed to the business then it might be appropriate to thank the poster for their concern and point to where the inaccuracies lie and correct that information.

In addition, if the posted information has been wrongly attributed to the business, that fact should be corrected. Consider referring the poster to the entity or organisation that is responsible for the concerns that have been raised.

If the content or publication of the material is likely to constitute a criminal offence consider involving the police. Discuss with your in-house legal team or corporate communications team first and report to the Board or General Counsel as required. You should also consider external legal advice where appropriate. For example, there are penalties imposed in NSW for failure to report a crime. It may be preferable to liaise with authorities before seeking the assistance of the social media provider in removing the content. There is a risk that the social media provider will alert the registered user of the request to remove the content before the authorities have time to effect an arrest.

Are the press involved? Get a media spokesperson lined up and briefed to plan a strategic response to the attack and to deal directly with mainstream media to mitigate the impact of negative press exposure.

You should consider engaging an expert PR consultant to assist with a planned response.

Steps to take to get material removed from third-party sites

Report content to the appropriate communications team and or legal department immediately but continue to monitor social media sites for further activity.

Assess the relevant reporting mechanism operated by the social media provider and report the content through it.

Assess the steps necessary to invoke the social media provider’s relevant take-down and reporting procedures.

Where is something “published”?

The question concerning the jurisdictional reach of defamatory comments hosted on a foreign based website was considered in Dow Jones and Company Inc v Gutnick (2002) 210 CLR 575. In this case, the High Court
of Australia held that a plaintiff could bring an action in Australia for defamation in respect of content that was published on a website based in another jurisdiction but which was accessible in Australia and therefore constituted publication within Australia of the offending comments.

Without further court decisions, it can only be said that a website host might be at risk for publishing defamatory material on the internet. However, the defence position of website hosts is further bolstered by the existence of a number of available defences, including the defence of innocent dissemination (at common law and under the Broadcasting Services Act 1992 (Cth)) and the defences of fair comment and opinion.

It should be noted however, that vicarious liability for the hosting of online material that offends other legislation for example, discrimination legislation (that additionally, may or may not be defamatory) has been found. An example of this is Clarke v Nationwide News Pty Ltd (t/as The Sunday Times) which we discussed on page 6.

**Obtaining social media content for use in litigation**

When a business is involved in litigation that involves social media content as part of its evidence, it is important to realise the business may have very limited access to the relevant social media site and may be unable to obtain the content on individual accounts in the way it would be able to obtain the content of other types of electronically stored information.

As most social media content is stored on overseas servers (mainly in the US), there is real tension as to who actually has possession, power and control over that information.

While social media operators state clearly in their terms of use that the registered user who posts that material retains ownership, that registered user does not have access to the necessary metadata to provide unequivocal evidence of the material itself.

In addition, social media pages are not highly secure and are subject to potential unauthorised use (login and password breaches are well documented). A registered user may claim that they did not post the material complained of.

**Issuing subpoenas on social media operators**

It is very difficult for a foreign-based entity such as an Australian business to issue a subpoena for social media content on any of the social media companies based in the US. Most of the social media operators say they will disclose personal information on a valid request such as a subpoena or search warrant issued by a foreign entity.

The reality is they will not respond to a civil subpoena without the consent of the registered user because of the impact of the US Federal Stored Communication Act.

**Remember...**

Even if your organisation doesn’t have a social media presence, you will need to monitor what is being said about you.

Your organisation might have several options for dealing with harmful and untrue comments, but you need to choose the right one as an over-the-top response might be counter-productive.
Social media impacts the employer-employee relationship in a few ways:

- who owns an employee’s social media account?
- can employees use social media in work time, and if so, how?
- if your employees interact with each other on social media inappropriately, is there potential liability for workplace harassment?
- could employees disclose confidential information deliberately or accidentally?
- an employee denigrates you on social media. Is this acceptable venting or a disciplinary offence?

In this section we’ll set out what you need to do to establish some ground rules in your own business. We’ll then look at the overlap between personal and professional use of social media, and the complex questions of managing employees whose use of social media is considered unacceptable.

**Employee social media policy**

You will need a separate policy that governs employees’ use of social media policy and sets out the ground rules, such as:

- the ownership of a social media account on which the employee interacts with clients;
- when an employee can use social media during work time; and
- the consequences for breaching the policy.

It should include specific obligations not to use social media:

- to damage the business’ reputation and interests (eg. disparaging the business, products/services or clients);
- to disclose the business’ confidential information; or
- to harass or bully work colleagues.

Depending on the nature of the services they provide, some sub-contractors and others who provide your business with services and products should also be made aware of your social media policies. As your rights against a contractor’s employees will be more limited than those in relation to your own employees, you will need to make sure your contracts specifically bind contractors and their employees to comply with your social media policies.

An employee’s misuse of social media may breach both the social media policy and their obligations of trust, confidence and good faith to their employer.

As we’ll see below, applying these rules in practice can be challenging.

**Case study: Using LinkedIn to solicit your employer’s clients**

Bradford Pedley v IPMS Pty Ltd T/A peckvonhartel [2013] FWC 4282 illustrates how an employee’s private use of social media can lead to adverse consequences for their employment.

Bradford Pedley was a Senior Interior Designer with an architecture and design company, PVH. When he took the job, he told PVH he would to continue carrying out private design work in his own time through his own business. PVH did not try to stop him.

He sent a group email to some LinkedIn connections which explained that he had his own business, that he wanted to expand it, and no job was too big or too small. When PVH learnt of this, it fired him.

The Fair Work Commission rejected Mr Pedley’s claim that his dismissal was harsh, unjust or unreasonable. It held that the LinkedIn email was a clear attempt to solicit business from PVH’s clients for his own business, which breached his obligation to PVH to faithfully promote PVH’s interests. This was serious misconduct, and was a valid reason to terminate the employment contract.
Awareness training
You should take active steps to educate your staff and emphasise that the policy, like all employee policies, is important and a breach of it may result in disciplinary action.

It is not enough to email or advertise on your intranet that the company has adopted social media policies – you need to bring the policies to the attention of the workforce and provide training, and deliver concise advice about the adoption of a social media policy as a specific term of employment for all employees. If you don’t, then it will be very hard, if not impossible, to discipline an employee for breaching it.

Who owns an employee’s social media profile or connections?

Branded feeds on Twitter and customer lists
Many executives now have an active social media presence and a number of Twitter followers. If an executive with a Twitter account leaves the organisation, many questions will arise, including:

- What is the nature or purpose of the employee’s Twitter profile? Is it an entirely private profile and not connected to the business or is it closely associated with, and therefore indivisible from, the business?
- If the followers of the executive’s Twitter account can be characterised as a customer list, is it the property of the employer organisation?
- How do you protect the executive’s following so that it is not lost when the executive departs the business?

This area of law is unsettled but there is an emerging view that where Twitter followers are clearly following the brand of the business, not the person or executive, then arguably there is intellectual property in the profile, and therefore by analogy the followers may be regarded as customers and should be protected in the same manner as a customer list.

These issues should be considered and then provided for by the inclusion of specific terms within employment contracts.

Case study: Policies and training
In Stutsel v Linfox Australia Pty Ltd [2011] FWA 8444, an employee was reinstated following termination for allegedly posting derogatory and harassing comments about managers on his Facebook page.

Linfox argued that a sufficient nexus existed between Mr Stutsel’s conduct and the workplace because:

- Mr Stutsel had Facebook friends who were employees of Linfox;
- the comments were made in respect of various Linfox managers; and
- Mr Stutsel’s Facebook profile picture featured a Linfox truck.

Commissioner Roberts found the comments to be akin to “a group of friends letting off steam and trying to outdo one another in being outrageous”, and while in poor taste, did not amount to serious misconduct.

In concluding that Mr Stutsel had been unfairly dismissed and ordering his reinstatement and back pay, the Commissioner gave weight to Linfox’s lack of a dedicated social media policy at the time of Mr Stutsel’s termination or by the date of the hearing, and that Linfox merely relied on its induction training and relevant handbook to ground its action against Mr Stutsel. In addition, the importance of employee awareness and training was highlighted:

“In this current electronic age, this [induction training and the handbook] is not sufficient and many large companies have published detailed social media policies and [have] taken pains to acquaint their employees with those policies. Linfox did not.”

Note: Clayton Utz acted for Linfox in this matter.

An employee’s LinkedIn profile
While LinkedIn content is generally more benign and less scandal-prone than that its social media counterparts Facebook or Twitter, the often inextricable blending of the personal and professional on LinkedIn might mean it turns out to be the platform that most frequently gives rise to issues of this kind.
Some of the questions about a person’s LinkedIn profile that can arise when they leave the organisation include:

- Is the profile a record of the organisation and therefore belongs to the business?
- If so, should the profile be deactivated when the employee leaves?
- Should the employee be allowed to maintain the profile if it’s updated to record the date upon which the employee left the organisation?

These are all questions on which there is currently limited guidance from the courts. In many cases, what is right for a particular business will depend upon their commercial needs and the sector in which they operate. At this stage, businesses should consider questions such as these and then ensure they have policies in place to reflect their commercial decisions and manage any risks.

**When does personal comment become professional misconduct?**

Employees’ expression of dissatisfaction and explicit examples of disloyalty to their employers through comments and other material posted to social media sites are frequently raised in unfair dismissal claims.

This requires answering the difficult question of what is “private comment” and publication of dissatisfaction, which often turns on the use of social media privacy settings. Unfortunately the case law on privacy settings and their effect on the extent of publication is inconsistent.

In Fitzgerald v Dianna Smith t/as Escape Hair Design [2010] FWA 7358 a dismissal that followed an employee’s very public Facebook complaint was ruled harsh, unjust and unreasonable, as there was no evidence the post had damaged the employer’s business.

This can be contrasted with the decision in O’Keefe v The Good Guys [2011] FWA 5311, in which an employee’s threatening Facebook posts made with very high privacy settings led to a dismissal that was found to be valid.

While The Good Guys case suggests that it will be possible to dismiss employees for inappropriate conduct involving social media, it is an area with which the courts are still coming to grips, and it may be some time before the law in this area becomes settled.

What we can learn from these cases is that businesses must establish policies that clearly set out the employer’s

---

**Case study: Connection with business**

The case of Fitzgerald v Dianna Smith t/as Escape Hair Design [2010] FWA 7358 dealt with an employee of a hair salon who posted the following comment on Facebook:

“Xmas “bonus” along side a job warning, followed by no holiday pay!!! Whoooooo! The Hairdressing Industry rocks man!!! AWESOME!!!”

She was then dismissed for unauthorised removal of property, lack of punctuality, unauthorised rescheduling of appointments and public display of dissatisfaction with the employer on Facebook.

Commissioner Bissett recognised the seriousness of her Facebook post, and the increasing tendency of employees to use social networking sites to display their dissatisfaction with their employer. In a concise statement about the nature of social media comments, Commissioner Bissett explained that “Posting comments about an employer on a website that can be seen by an uncontrollable number of people is no longer a private matter but a public comment” and that a Facebook post “remains on Facebook until removed”.

In effect, Fair Work Australia emphasised that in certain circumstances, a Facebook post by an employee may be sufficient to warrant dismissal. However, this depends on whether the post will adversely affect the employer’s business.

The Commissioner ruled that the dismissal was harsh, unjust and unreasonable as the employer failed to demonstrate that the comment damaged business, notwithstanding that it certainly damaged the employer’s trust and confidence in the employee. The employer was ordered to compensate the employee $2,340.48.
Employee use of social media – and these policies must be brought to the attention of the workforce.

Case study: Threatening behaviour and out of hours posting

In O’Keefe v The Good Guys [2011] FWA 5311, Fair Work Australia found that the dismissal of the employee was justified notwithstanding the fact that the employee had applied the most stringent privacy settings to his Facebook account.

It would appear that the decision was based upon a number of factors including:

- the extremely offensive nature of the allegations and threats made on Facebook; and
- the fact that the employee’s comments could be seen by his colleagues as they were Facebook “friends”.

The Commissioner also held that it did not matter that the comments were made on a private (as opposed to a business) computer and that they were posted out of hours.

Remember...

The law is still evolving.

Clear policies on appropriate social media use should be developed, and your staff trained in them.

Be particularly careful when an employee’s social media use is the basis for disciplinary action.
Key contacts

Gary Berson  
Partner – Perth  
T +61 8 9426 8420  
F +61 8 9481 3095  
gberson@claytonutz.com

Jamie Doran  
Partner – Brisbane  
T +61 7 3292 7196  
F +61 7 3221 9669  
jdoran@claytonutz.com

Steven Klimt  
Partner – Sydney  
T +61 2 9353 4133  
F +61 2 8220 6700  
sklimt@claytonutz.com

Doug Bishop  
Partner – Sydney  
T +61 2 9353 4673  
F +61 2 8220 6700  
dbishop@claytonutz.com

Karen Evans-Cullen  
Partner – Sydney  
T +61 2 9353 4838  
F +61 2 8220 6700  
kevans-cullen@claytonutz.com

Chris McLeod  
Partner – Melbourne  
T +61 3 9286 6214  
F +61 3 9629 8488  
cmcleod@claytonutz.com

Ian Bloemendal  
Partner – Brisbane  
T +61 7 3292 7217  
F +61 7 3221 9669  
ibloemendal@claytonutz.com

Kym Fraser  
Partner – Melbourne  
T +61 3 9286 6913  
F +61 3 9629 8488  
kfraser@claytonutz.com

Simon Newcomb  
Partner – Brisbane  
T +61 7 3292 7243  
F +61 7 3221 9669  
snewcomb@claytonutz.com

Scott Crabb  
Partner – Perth  
T +61 8 9426 8430  
F +61 8 9481 3095  
scrabb@claytonutz.com

Richard Hoad  
Partner – Melbourne  
T +61 3 9286 6936  
F +61 3 9629 8488  
rhoad@claytonutz.com

Alexandra Wedutenko  
Partner – Canberra  
T +61 2 6279 4008  
F +61 2 6279 4099  
awedutenko@claytonutz.com

David Benson  
Senior Associate – Perth  
T +61 8 9426 8586  
F +61 8 9481 3095  
dbenson@claytonutz.com

Eleanor Dickens  
Senior Associate – Brisbane  
T +61 7 3292 7127  
F +61 7 3221 9669  
edickens@claytonutz.com

Julia Virgo  
Special Counsel – Sydney  
T +61 2 9353 4896  
F +61 2 8220 6700  
jvirgo@claytonutz.com

Michael Byrnes  
Special Counsel – Sydney  
T +61 2 9353 4723  
F +61 2 8220 6700  
mbyrnes@claytonutz.com

Sharon Segal  
Special Counsel – Melbourne  
T +61 3 9286 6323  
F +61 3 9629 8488  
ssegal@claytonutz.com

Jason Walsh  
Senior Associate – Sydney  
T +61 2 9353 4880  
F +61 2 8220 6700  
jwalsh@claytonutz.com

Joseph Collins  
Senior Associate – Sydney  
T +61 2 9353 4759  
F +61 2 8220 6700  
jcollins@claytonutz.com

Jason Shailer  
Special Counsel – Sydney  
T +61 2 9353 4789  
F +61 2 8220 6700  
jshailer@claytonutz.com

Timothy Webb  
Special Counsel – Sydney  
T +61 2 9353 4778  
F +61 2 8220 6700  
twebb@claytonutz.com