TRENDS AND LEGAL OBLIGATIONS
Before analysing the current position of social media within Defence and offering suggestions about strategy for enhancing the organisation’s response, it is necessary to establish a baseline of general data and information.

This section is in two parts, each with a logical part to play in that task:

### 2.1 Trends

This section examines social media trends in Australian society in general, who is using social media and what they are using it for. It discusses sites that are attracting attention, and a timeline shows the global evolution of social network sites. The section also looks at some recent success stories, when social media have acted as conduits in times of crisis.

### 2.2 Legal obligations

This overview examines the laws that may influence and restrict Defence participation and engagement in social media. It is a high-level examination primarily of Defence and its members' engagement with a broad internal and external community of organisations and individuals that are interested in the activities of Defence. In considering social media use from a legal perspective, this section offers suggestions for ‘engagement principles’.
2.1 TRENDS

Australians’ interest in and use of social media have increased over recent years. Since 2009, we have been among the world’s heaviest users of such sites. The trend towards going online and communicating via the internet has meant that social media have become a part of everyday life for many, but youth are the highest consumers in terms of usage, frequency of use and time spent online. The integration of social media into life has affected a wide variety of societal aspects, including news reporting, technology, crisis communication, privacy, and even what it means to be someone’s ‘friend’.

2.1.1 Trend: Australians among the heaviest users

The global social media landscape has evolved rapidly over the past five years. The use of social media has become a mainstream activity and arguably part of the everyday life of many people. The number of Australian internet users aged 14 and over who went online during the December quarter of 2010 was approximately 15.1 million, up from 14.2 million for the same period in 2009 (ACMA 2011:2). According to comScore (2011), social networking ‘accounts for 1 in every 5 minutes spent online in Australia’.

By the end of 2009, Australians had become some of the world’s heaviest users of social media, spending an average 6 hours and 52 minutes a month on social sites (Table 2.1).

<table>
<thead>
<tr>
<th>Country</th>
<th>Unique Audience (000)</th>
<th>Time per Person (hh:mm:ss)</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States</td>
<td>142,052</td>
<td>6:09:13</td>
</tr>
<tr>
<td>Japan</td>
<td>46,558</td>
<td>2:50:21</td>
</tr>
<tr>
<td>Brazil</td>
<td>31,345</td>
<td>4:33:10</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>29,129</td>
<td>6:07:54</td>
</tr>
<tr>
<td>Germany</td>
<td>28,057</td>
<td>4:11:45</td>
</tr>
<tr>
<td>France</td>
<td>26,786</td>
<td>4:04:39</td>
</tr>
<tr>
<td>Spain</td>
<td>19,450</td>
<td>5:30:55</td>
</tr>
<tr>
<td>Italy</td>
<td>18,256</td>
<td>6:00:07</td>
</tr>
<tr>
<td>Australia</td>
<td>9,895</td>
<td>6:52:28</td>
</tr>
<tr>
<td>Switzerland</td>
<td>2,451</td>
<td>3:54:34</td>
</tr>
</tbody>
</table>

Source: The Nielsen Company

The frequency of consumption of social media by Australians is evident in the Sensis social media report (Sensis 2011), which was targeted at social media users and conducted through phone interviews. Some 30% of survey participants made use of social media every day, with an overall average for all survey participants of 12.4 times per month (Figure 2.1).
The Sensis report further segmented the frequency of use of social networking sites by age and gender, as shown in Table 2.2.

### Table 2.2: Social networking usage, by age and gender

(Source: Sensis 2011:10)

<table>
<thead>
<tr>
<th>Frequency of Use</th>
<th>Total (613)</th>
<th>Male (482)</th>
<th>Female (131)</th>
<th>18-19</th>
<th>20-29</th>
<th>30-39</th>
<th>40-49</th>
<th>50-64</th>
<th>65+</th>
</tr>
</thead>
<tbody>
<tr>
<td>Everyday</td>
<td>30%</td>
<td>25%</td>
<td>36%</td>
<td>70%</td>
<td>52%</td>
<td>59%</td>
<td>14%</td>
<td>15%</td>
<td>5%</td>
</tr>
<tr>
<td>Most days</td>
<td>10%</td>
<td>5%</td>
<td>11%</td>
<td>15%</td>
<td>20%</td>
<td>9%</td>
<td>11%</td>
<td>5%</td>
<td>3%</td>
</tr>
<tr>
<td>A few times a week</td>
<td>8%</td>
<td>8%</td>
<td>8%</td>
<td>7%</td>
<td>12%</td>
<td>10%</td>
<td>7%</td>
<td>7%</td>
<td>5%</td>
</tr>
<tr>
<td>Once a week</td>
<td>5%</td>
<td>6%</td>
<td>5%</td>
<td>1%</td>
<td>6%</td>
<td>6%</td>
<td>5%</td>
<td>5%</td>
<td>8%</td>
</tr>
<tr>
<td>Less than weekly</td>
<td>9%</td>
<td>10%</td>
<td>7%</td>
<td>0%</td>
<td>4%</td>
<td>9%</td>
<td>22%</td>
<td>5%</td>
<td>10%</td>
</tr>
<tr>
<td>Never</td>
<td>38%</td>
<td>42%</td>
<td>34%</td>
<td>7%</td>
<td>7%</td>
<td>27%</td>
<td>41%</td>
<td>6%</td>
<td>69%</td>
</tr>
</tbody>
</table>

Average times per week: 12.4, 10.6, 14.1, 24.9, 21.4, 15.2, 7.9, 6.5, 3.1

It is evident from Table 2.2 that 14–19-year-olds are the most frequent users of social networking sites; some 70% of those surveyed in this age group stated that they accessed such sites every day. The second most frequent users are 20–29-year-olds; 52% of those surveyed indicated that they used social networking sites every day. This is an important finding for organisations that have a need or desire to target ‘youth’. The survey results indicate that more than 59.5% of 14–29-year-olds access social networking sites every day, indicating that social networking sites are key channels for sending messages to young audiences (Sensis 2011). While the number of survey participants in each age demographic was not high, there is nothing to suggest that the results are not broadly reflective of the overall population of social media users.

It is also important to determine which social media sites experience the highest frequency of usage by Australians, in order to understand the best platform for communicating with them. The data in Figure 2.2, taken from this review’s public survey, shows that the most frequently used social media site was Facebook; 32% of respondents said they used it several times a day, and 99% of respondents were aware of the site.
2.1.2 Trend: Social media during natural disasters

In 2011, social media became increasingly important places for Australians to turn to in times of natural disaster. In January, Queensland experienced flooding in many areas, including Toowoomba and Brisbane. When the Brisbane City Council (BCC) website crashed due to an overload of traffic, the council used Facebook and Twitter to send information about, for example, areas being evacuated and those that were flooded. The public responded by ‘liking’ the BCC Facebook page and/or following the BCC Twitter account in order to remain informed about the unfolding crisis. The Facebook page had 761 likes at the beginning of January but 12,648 by the end of the month.

BCC was not the only entity that used social media to communicate during the floods. The Queensland Police Service (QPS) also used them to communicate with the public and to correct false rumours. The community needed timely, relevant and accessible information, and that was provided through social media. According to Larkin (2011), the QPS Facebook page went from under 25,000 likes to 165,000 likes during the floods. The QPS Twitter account (@QPSMedia) used the hashtag ‘#mythbusters’ to deal with misinformation or disinformation during the crisis. QPS’s Facebook page dealt with false information in a similar way. This obviously helped to ensure that the general public were up to date with all information (including false information).

Although the QPS broadcast information about the hardest hit areas, residents in local communities were looking for more localised material, relevant to them. Where local or regional councils did not provide that information, communities created their own social media platform to discuss and share their experiences of the floods. The community took the responsibility for information into its own hands: several ‘area’ or ‘shire’ pages surfaced, such as the Caboolture Shire and Surrounding Suburbs Floods page (Figure 2.3).
The page was created by a member of the community to publish:

- photos of flooded or damaged areas
- requests by the community for help
- offers to help or donate materials
- updates on what roads were open or closed
- information about official channels
- criticism of the regional council for not setting up a page similar to those created by the QPS or BCC
- false rumours about the floods, some of which were corrected by fellow community members.

People who lived outside the affected communities also used the page to check whether family and friends were safe. The page had approximately 13,000 likes by the end of the week of the floods.

Another example of the use of social media during times of natural disaster was during Tropical Cyclone Yasi, which crossed the North Queensland coast on 3 February 2011 (Colgan et al. 2011). This natural disaster was not centred on a metropolitan area, so different methods of communication were used to communicate with people who were or would be affected by the cyclone. Social media played a part in getting information about Yasi to the public outside the affected areas.

A Twitter account, @cycloneupdate, was established by a local weather enthusiast, who monitored cyclone activity and broadcast it to the world. The owner of the account was approached by media outlets requesting interviews, and the information provided by this unofficial source was even retweeted by major news outlets (Figure 2.4).
Social media are becoming an important part of crisis management for governments and communities, particularly during natural disasters. Where the authorities are not communicating through Facebook and Twitter, the community creates an information and content sharing environment, using social media to fill the gaps.

### 2.1.3 Trend: Conversation drives interaction

Before Facebook, it was Myspace, and before Myspace it was Friendster – social media is about people and their need and desire to communicate, not specific platforms (which so far have been transitory). This is a critical factor when formulating and implementing social media policies and regulations covering social media behaviour: social media usage is driven by people's need to converse and interact.

According to the Sensis report (2011), the main reason Australians use social networking sites is to catch up with friends and family (Figure 2.5). Conversing with friends online can be as important as communicating offline, particularly for people separated by distance. Social media allow users to create a life and personality online, which often reflects their offline presence. Social networking can be seen as a digital extension of the ‘real’ self.

![Reasons for using social networking sites](source)

**Figure 2.5: Reasons for using social media**

(Source: Sensis 2011:18)
2.1.4 Trend: Emerging platforms

The trend towards increased use of social media has also meant a trend in emerging platforms, as technology businesses strive for a slice of the social media phenomenon. The most recent platform that has emerged is Google+ (Google plus). The timeline in Figure 2.6 provides some insight into the abundance of social network sites over the years. Most notably, the most popular social network site at the time of writing this report, Facebook, is the only one with a staggered release over time.

![Timeline of social media platform releases](image-url)
2.1.5 Trend: Facebook dominates

Facebook currently dominates social media use in Australia. It is the social media site with the highest recognition, highest number of users and highest frequency of use. The Sensis social media survey found that the average time spent on Facebook was 21.1 minutes on each occasion (Figure 2.7).

![Figure 2.7: Time spent on social networking sites](Source: Sensis 2011:15)

The Sensis data also shows the frequency of use of Facebook among respondents; 18% said they used it more than 20 times a week, and the average use was 16.2 times per week (Figure 2.8).

![Figure 2.8: Frequency of use of social networking sites](Source: Sensis 2011:14)

On average, people in the 14–19 year age group access social networking sites more than others, and people in Victoria have marginally higher Facebook usage.
The comparison of metropolitan and non-metropolitan groups shows that the more geographically distant from major areas/cities, the higher the usage of Facebook (Figure 2.9), which is possibly driven by a greater need for technology in order to keep in touch.

This review's public survey supports the Sensis data findings: younger people are the most frequent users of Facebook. Sixty-seven per cent of 18–24-year-olds access the site several times a day (Figure 2.10).

It is estimated that around 10 million Australians are on Facebook (Lee 2010). Facebook’s own statistics in the Facebook advertising section support this estimate: at 21 July 2011, 10,436,860 people on Facebook stated that they lived in Australia (Facebook 2011). Facebook penetration, by state and territory, is shown in Figure 2.11.
It can be concluded from the above chart that the penetration by state suggests communication through Facebook may not be as effective for the Northern Territory as in New South Wales due to a lower percentage of the population with a Facebook account.

**Facebook moves beyond Facebook**

Facebook is also moving beyond its own site through the use of Facebook Connect, which allows Facebook’s technology to be integrated into third-party web content. This enables Facebook likes, shares, recommends, and logins to be used across the web. Facebook is open to third-party developers via the Facebook API (application programming interface), which allows for access to Facebook databases, enabling thousands of applications to be developed (Facebook developers 2011).

At the start of 2010, Facebook connected itself to the wider web via a button labelled ‘Facebook Like’, which enables hundreds of millions of Facebook users across the globe to ‘endorse’ websites and web pages. The endorsements are automatically posted to users’ Facebook walls. This created a massive infrastructure of interlinks between the ‘social web’ and what’s been described as the ‘searchable web’ (Elowitz 2011). In June 2011, Facebook integrated into WordPress (an open source blog tool and publishing platform) through the WordPress Facebook and Twitter plugin, allowing people to use their Facebook accounts to login and leave comments on WordPress websites (Figure 2.12).
Facebook, the integrated social network

Sean Parker, one of the original investors in Facebook, was recently interviewed about why Facebook ultimately dominated Myspace. His insight is that Facebook grew organically from a niche market, then slowly went mainstream in a staged, geographically and, ultimately, dominating way (Tsotsis 2011).

“Nobody actually believed, outside of us three or four people in Palo Alto, that you could enter the market through this niche market and then gradually, through this carefully calculated war against all the social networks, become the one social network to rule them all.”

- Sean Parker, Facebook investor

(Tsotsis 2011)

One reason why Facebook is ‘sticky’ (that is, able to attract users to return frequently) is that most users’ social networks of ‘friends’ are in the one place, making it easy to communicate with them. Facebook captured the user interface, then went on to incorporate the best features of any social network (such as Twitter’s ‘What are you doing now?’ and foursquare’s geo-location check-ins). Possibly in response to Facebook’s dominance of the digital social space, Google’s new social network, Google+, contains similar features to Facebook, but with the inclusion of ‘circles’ to group friends. Circles have been better received than the Facebook lists (Solis 2011).

The success of Facebook may be attributed to its integrated nature: it includes elements of some other social media sites, amalgamating some of the key features into one social media platform (Figure 2.13). The Facebook platform is in a constant state of development and innovation, and new features are launched frequently, although their reception by Facebook users is often mixed.
2.1.6 Trend: Social media are mobile

Social media usage is increasingly carried out through portable or ‘mobile’ devices. Over the past 12 months, many Australians have upgraded to smartphones, and are moving away from standard text-and-call mobiles or web-enabled feature phones. Research by International Data Corporation indicates that the Apple iPhone leads the Australian smartphone market with 40% of market share in June 2011 (CNET Australia 2011). A 13% increase in iPhone shipments in the first quarter of 2011 puts the iPhone at nearly a third of the entire mobile phone market; Nokia’s Symbian platform lost 9.5% of its market share (CNET Australia 2011).

Greater access to smartphone technology has helped Australians become more mobile in their social networking activities. In 2010, the most downloaded free iPhone ‘app’ (application) was the Facebook app (Gizmodo 2010). Mobile browser access to social networking sites is also rising. Global figures from January 2010 indicate that social networking access via mobile browser increased by 4.6% from the previous year, to 11.1% (comScore 2010). The tablet market is increasing: International Data Corporation forecasts strong growth in Australia and New Zealand in 2011 (CBR Communications Mobility 2011).

The Sensis social media report indicates that 34% of Australians surveyed used a smartphone to access their social media sites. The proportion was 52% for the 14–19 age group and 42% for 20–29-year-olds (Figure 2.13). This reflects the preference of the younger market, which increasingly has internet access most of the time.
It was evident from this review’s public survey that access to social media is mainly by a laptop or desktop computer, followed by mobile devices (Figure 2.14). For the purposes of this review, laptops were not considered to be mobile devices, as they are being overtaken by next generation devices specifically designed for mobile use and convenience.

The retail sector is being affected by social media users’ ability to shop ‘on the go’. Mobile shoppers are able to research purchase decisions, ‘check in’ (geographically), meet up with friends via ‘People Nearby’ on Facebook, and look for online deals, all while away from their main computer. Exploiting that mobility for marketing purposes is currently being trialled by foursquare through a partnership with ‘daily deals’ companies such as LivingSocial and Gily Groupe (Hutchings 2011). With the impending launch of QuickerFeet (an iPhone app for location-based promotions), this type of marketing may develop rapidly in the future (QuickerFeet 2011).

Figure 2.13: Devices used to access social media
(Source: Sensis 2011:17)

Figure 2.14: Devices used to access social media
From which of these devices have you accessed social media sites in the last 3 months?
2.1.7 Trend: Social media integrate with technology

Social media are increasingly becoming integrated into daily routines and are being made easier to access through their integration into technology. There are two emerging methods for social media integration: pushing social networking sites on the public by forcing the sites into people’s line of sight, and pulling people towards social media by creating exclusive content.

**HTC mobile – the Facebook button**

![HTC mobile with Facebook button](image1)

Given that social media mobile activity is on the rise (Net Marketing Strategies 2010), HTC has brought out a mobile phone with a Facebook button. This makes Facebook even easier to access than through the use of apps or web browsing. The button allows users to share information from their phone, such as photos, videos and messages, immediately. The phone also contains a Facebook chat widget, allowing users to connect with their Facebook friends who are online while on the go (HTC 2011). This is an example of Facebook being placed in the line of sight of the mobile phone owner or potential buyer. There is no option to remove the button or to make it inactive.

**Mobile phone plans – free social networking**

![Telstra Tribe](image2)

A number of phone companies now include free social networking as part of their mobile packages (Vodafone 2011). This is used to target heavier social media users, who would be wary about the amount of data usage on their phones when accessing social media. Telstra Tribe is a social platform that allows users to sign in to Facebook, Twitter and Myspace in the one place, free of charge (Telstra 2011). This type of social media technology integration can be seen as a push method, forcing social media onto the network user, as the Tribe platform cannot be removed from the phone plan.
Angry Birds – Facebook and Twitter to unlock levels

Facebook and Twitter accounts are required to unlock certain levels of the mobile game Angry Birds. This forces users to have a Facebook or Twitter account, or forgo the bonus levels (Games Blog 2011). This is an example of pulling the user towards social media by providing content that is available only to those connected to Facebook and Twitter. It is highly likely that this type of social media integration is designed to drive ‘viral’ awareness of the applications to ‘friends’ of the game’s current user base.
2.1.8  Trend: Privacy is the new battleground

Different social networks provide different fields for information about users. Often, the more information provided, the higher the level of security and privacy required. Facebook asks for a person’s first and last names, email address, birthday (for age verification purposes) and gender in order to create an account. Facebook also provides fields on a person’s profile for friends and family, education and work, contact information and more (Figure 2.15).

![Facebook fields](Source: Facebook, 18 July 2011)

Twitter, on the other hand, asks for only a name and an email address to sign up for an account and does not require that the account represents a real person, which is a requirement of Facebook. There are fewer opportunities on Twitter to provide information about a personal or organisational account holder, as the ‘bio’ (biography) section is limited to only 160 characters (Figure 2.16).

![Twitter bio section](Source: Twitter, 18 July 2011)

A number of social networking sites are similar to Twitter, requiring and providing for only limited information about the account holder. Others, such as Facebook, LinkedIn, Myspace and Google+, require and provide fields for detailed information about the account holder. This is why users have higher privacy expectations on some social media sites than they might on others.
To an extent, Facebook changes its privacy settings to fit the requirements of the community, although some information must remain available to the public eye. Because many types of personal information can be uploaded onto Facebook, the privacy settings are more complex than those of some other social networking sites. Interestingly, Facebook uses an ‘opt out’ approach for any new features to the site, such as Facebook Places and automatic photo-tagging. With Facebook Places, users can be ‘tagged’ by friends at certain locations without their permission, showing their exact geographical location to all of their Facebook friends and the friends of the person who tagged them. To opt out and ensure that their location is not disclosed by friends, users must go to their Facebook privacy settings and disable the feature.

Automatic photo-tagging on Facebook was released in Australia in early June 2011 but suffered negative backlash from the public, prompted by a blog post by Graham Cluley of the security firm Sophos, criticising the opt-out nature of the feature (ABC 2011). The feature prompted an investigation by European Union data-protection regulators as a potential privacy risk, the concern being that the opt-out process means users have not specifically consented (Schroeder 2011). Of the respondents to this review’s public survey, 46% did not know whether automatic photo-tagging was enabled on their account. Facebook often puts the onus of privacy and security of information on the account holder.

This review's public survey asked participants when they had last reviewed or altered their privacy settings on Facebook (Figure 2.17). Nine per cent indicated that they did not know how to review or alter their settings.

Most respondents indicated that their Facebook profile settings are generally set to friends only, although 5% had most of their information viewable by the public.
2.1.9 Trend: Social media alter news reporting

Social media are increasingly becoming methods for journalists to collect and communicate information. Most Australian news networks have a presence on social media, primarily on Twitter. Realtime updating means that news companies are able to break stories as soon as they happen. Online news sites, newspapers, TV news and radio are using social media both to get their messages out and to be the first to market with information. Individual journalists are also using social platforms such as Twitter to communicate news (Figure 2.18).

![Figure 2.18: Twitter accounts of news organisations and individual journalists](Source: Twitter, 20 July 2011)

Social media have become so important to journalists and news companies that they have prompted the development of guidelines and education for journalists using them to report news. For example, Reuters (2011) has produced a guide called ‘Reporting from the internet and using social media’ (Figure 2.19).

![Figure 2.19: Guide to social media use for journalists](Source: Reuters 2011)
One of the most interesting sections of the Reuters guide is ‘1.5 Is it a hoax?’. Hoaxes have been a problem for some journalists who have failed to verify facts found in social media before broadcasting the story, either in social media or through traditional media channels (Mashable 2011).

‘Jeff Goldblum dead’
In 2009, an entertainment reporter took from Twitter the assertion that actor Jeff Goldblum had died in an accident in New Zealand, and reported it on a morning news show. The report claimed that the New Zealand police had confirmed the death of Goldblum after he had fallen from a cliff during a film shoot. However, Goldblum was alive and well (Daily Telegraph 2009). It took an email from a viewer to prompt the TV show to dismiss the story as a hoax (Newsphobia 2009).

‘Queensland floods – crocodile in Gympie’
The 2011 Queensland floods were covered extensively by news reporters. Local authorities’ tweets about the floods, safety, evacuation and road closures, and Premier Anna Bligh’s Twitter account, became important sources of information. On 11 January 2011, an image surfaced on Twitter allegedly showing a crocodile brought into Gympie by the floodwater (Figure 2.20). The image received more than 30,000 views and was featured in the main news flood coverage, including television news. The image was a hoax: it had been adapted from a commercial.

Social media is changing news reporting forever, by giving journalists and news networks a new platform to communicate to many people, with real-time updates. Speedy supply of information is important for journalists, but it must be noted that the use of social media for information-gathering does have its pitfalls and can result in false information being further dispersed, if it is not verified prior to re-broadcast.
2.2 LEGAL OBLIGATIONS

The following has been prepared for the review by Stephen von Muenster, Principal, von Muenster Solicitors & Attorneys.

Stephen von Muenster
Principal von Muenster Solicitors & Attorneys

Overview

Forming part of the George Patterson Y&R, Department of Defence (Defence) Social Media Review Scope of Work, this brief overview is divided into nine sections and is designed to examine the laws that may influence and restrict Defence participation and engagement in social media. This review is a high level examination and is primarily aimed at Defence and its members’ engagement with a broad internal and external community of organisations and individuals that are interested in the activities of Defence.

Firstly, we introduce the concept of social media and explore the notion of user-generated content. What this overview understands to be participation and engagement in social media by Defence and its members is then placed into context through a classification of professional use and private use of social media.

We then examine the laws that have the potential to impact upon such professional and private use. Given the time available to prepare this overview, specific defence and public service legislation, including freedom of information, public records management and archiving requirements, are not considered in detail and are beyond the scope of this brief overview. The same applies to extant defence policies and guidelines, including for example equity & diversity and information & operational security. The specific application of such legislation and policies are best examined and will need to be considered further once Defence has indicated how it intends to embrace and engage in social media as an organisation following consideration of the preliminary George Patterson Y&R Social Media Review.

Finally, we suggest a holistic risk management based approach to legal compliance in social media engagement. Such an approach is necessary as there is no specific law in Australia governing social media – the current state of the law is evolving, uncertain and remains largely untested in the Courts - and the application of the complex coalition of laws and private contracts that do apply are generally misunderstood in the social media space. The reality that social media engagement results in instantaneous global communication resulting in the possibility of attracting the jurisdiction of current and emerging overseas laws and regulations unfortunately adds to this complexity.
Our legal overview concludes with some suggested practical approaches and risk treatment strategies when Defence and its members engage in social media (termed ‘Social Media Policies’) and when Defence allows third parties to engage with the Defence through an exchange of user-generated content (termed ‘Engagement Principles’). It is suggested that such an approach will go a long way to increasing confidence in the use of social media whilst removing uncertainty and reducing the likelihood of the occurrence of identified and unidentified legal and reputational risks in social media engagement.

The sections of this overview are as follows:

Introduction
Social Media Engagement in Context
User-generated Content
 Regulation of Social Content
  • Introduction
  • Internet Content Regulation
Laws Influencing and Restricting Defence Engagement in Social Media
  • Introduction
  • Who might complain?
  • International laws that may apply to social media engagement
  • Consumer protection laws
  • Passing off
  • Trade marks
  • Copyright
  • Moral rights
  • Defamation
  • Discrimination, hate speech & causing offence
  • Injurious falsehood
  • Privacy laws
  • SPAM laws
The Rules of Proprietary Space
Social Media Engagement Principles
Social Media Policies
Closing Observations
Introduction

We are in the midst of a social media revolution. Social media is a revolution in the way in which individuals, consumers, government, business, non-government organisations and the media engage and communicate with each other.

Social media is often understood to describe media or content that is authored or generated by a user and can take numerous forms. Social media includes forums, bulletin / message boards, blogs, wikis, podcasts, posts, threads. Social media sites or applications such as Google, Facebook, Linkedin, Twitter and YouTube provide a social networking environment enabling community engagement and interaction between individuals and groups.

Social networking sites continue to evolve as integrated hubs for entertainment, information and communication. Social sites are becoming increasingly integrated. Blogs, posts, tweets and videos created by users and their friends can be broadcast simultaneously for example on Facebook, Linkedin, Twitter and YouTube. As individuals, consumers, government, business, non-government organisations and the media are dynamically engaging in social media, it has become the new reality that the reputation of organisations or individuals can be harmed or enhanced though the socialisation of good and bad experiences on social networking and social media sites.

Openness is a feature of internet technology and such openness underpins its original architecture, software development and open access. Given this foundation, it must be understood that engagement in social media necessarily involves an organisation relinquishing some control. In the past, organisations were able to determine the relationship with its members or the public. Thanks to social media, it is the members and other individuals who increasingly are defining how an organisation is perceived. Instead of being simply passive receivers of information, individuals of today are actively engaged and are participants in a conversation with the organisation. Rather than trying to remain in control, organisations must embrace the opportunity whilst adopting an altered set of internal policies and external engagement principles that ensure compliance with the current and emerging legal obligations that apply in social media. Such an approach will go a long way to reducing legal and reputational risk.

The aim of this review is to provide Defence with a highlights tour of the Australian laws and regulations that may, on a case by case basis, influence and restrict Defence participation and engagement in social media. This overview does not attempt a comprehensive or ‘deep dive’ review of each of the applicable laws as such an examination is presently beyond the George Patterson Y&R Scope of Work. Furthermore, this legal overview does not examine the complex art of social media marketing and consumer engagement, as such an enquiry is best left to the experts.
Instead the intent of this overview is to raise the general level of awareness of the applicable laws and regulations as well as identify some of the risks inherent in social media engagement. In turn this may promote legal compliance and thereby reduce legal and reputational risks to Defence and its members when engaging in social media.

Finally, as each social media channel and communication is different and raises its own legal and compliance challenges, it would be impossible for this overview to provide specific legal advice. Therefore it is important to understand that this overview is intended as a guide only and should not be relied upon in substitution for seeking appropriate legal advice on a case by case basis.

**Social media engagement in context**

Use of social media and the procedures and policies designed to regulate the manner of its use will be largely be dependent on the nature and interests of a given organisation, the type of community that may engage with the organisation and the practices and needs of its members. There is no standard or ‘one-size fits all’ approach.

For the purposes of examining the Australian laws that may influence and restrict Defence participation and engagement in social media, we have considered it necessary to take a broad view of the types of Social Media use that may involve Defence and its members. The following possible scenarios involving Defence and its members are considered:

The following nature of use referred to in this overview as **Professional Use:**

- Defence as an organisation maintaining its own socially enabled website and having an active presence via pages on the social media sites or applications. Examples include the Army internet site and Army Facebook, Flickr, Twitter and YouTube pages.

- Defence engaging in various mainstream and niche social media channels via participation and conversations on other social media sites, the pages or channels of other organisations or the media and forums, bulletin / message boards, blogs, wikis, podcasts, posts, threads and the like.

The following nature of use referred to in this overview as **Private Use:**

- Defence members with their own active presence on the social media sites and participation in the mainstream and niche social media channels where members refer to their involvement with or employment by Defence in any way, including identifying themselves as Defence members, discussing their activities and the activities of other Defence members and posting user-generated content related to their Defence activities.

- Defence members engaging and participating in social media without any reference to Defence; although the Defence member may be known
in his or her community to be a Defence member, or an association with Defence may be inferred.

The Australian laws and regulations discussed in this overview may apply in varying degrees to the type of engagement in social media identified in each of the above scenarios. Further, the distinction between Professional Use and Private Use is very important when considering the content of a Defence Social Media Policy (discussed in greater detail below).

User-Generated content

Engaging in social media is all about sharing and collaboration. Social media involves a conversation – a ubiquitous, borderless, worldwide multi-way conversation with potentially an unlimited number of individuals conducted through a combination of written, visual and aural material. The result is the generation of user-generated content by the individual or organisation who engages in social media.

Today individuals are experimenting with and creating user-generated content. Empowered individuals modify, edit and change existing content as well as create a wide variety of their own material through the combined effect of personal computers, digital cameras, digital video recorders, technology rich mobile devices, the internet, enabling software and the various formats offered by purpose created websites. User-generated content includes combinations of written posts and comments, data, text, software, speech, music, sounds, visual images, photos, video (animated or otherwise), and other creations and combinations generated by an individual.

File sharing and social media sites are available to any individual with an internet connection enabling them to instantaneously upload and post their social content creations to share with their online communities. Individuals are also creating new types of content by incorporating their own material with commercially created film, music and other content (sometimes referred to as ‘mashups’). This is often done without any regard for copyright laws (discussed further below).

For Defence and its members such user-generated content will be generated as a result of both Professional Use and Private Use. As engagement in social media and the creation of user-generated content are inextricably linked, Defence must establish community requirements or engagement principles for user-generated content submissions that prohibit infringing and offensive content. Defence Social Media Policies for Professional Use and Private Use (discussed below) regulating and suggesting appropriate creation of user-generated content by Defence members and Engagement Principles applicable
to third parties’ engagement with Defence (also discussed below) will assist with legal compliance and significantly reduce the risks of engagement in social media.

**Regulation of Social Content**

**Introduction**

Content laws to refer to the coalition of Australian laws, regulations, determinations, standards and industry codes that directly impact upon the nature and type of content (written posts and comments, images, photos, video and other creations and combinations) that can lawfully be seen, heard, communicated, broadcast, streamed or downloaded via social media.

Content laws can apply equally to repurposed traditional content, premium content, advertising content, branded content and even to user-generated content. Therefore if Defence itself creates content or invites user-generated content during Professional Use, Defence will need to consider the application of content laws on a case by case basis. The content laws also apply to Private Use.

In Australia, the Australian Communications and Media Authority (ACMA) is responsible for regulating the nature and type of content that may be published online including internet and mobile social content, and enforcing Australia’s anti-spam law. Content is primarily regulated through a number of Commonwealth laws, regulatory standards determined by ACMA, and industry initiated mandatory and voluntary industry codes of practice.

There are numerous regulatory standards and codes that apply to the broadcasting, telecommunications, radiocommunications and internet industries and it is beyond the scope of this overview to provide a review. In this section we only seek to overview the regulation of social content to the extent that such regulation is likely to impact upon Professional Use and Private Use in social media.

**Internet Content Regulation**

ACMA administers a national co-regulatory scheme for internet content which is governed by the [Broadcasting Services Act 1992](https://www.legislation.gov.au), and is designed to address community concerns about offensive and illegal material on the internet. A regulation of content framework came with the introduction of Schedule 7 to the [Broadcasting Services Act 1992](https://www.legislation.gov.au) which commenced on 20 January 2008.

Internet content is regulated under the national co-regulatory ‘Online Content Scheme’. The internet content regulations apply to all hosting, content and links service providers, and providers of live (streamed) content from Australia. This generally means any person
or organisation that makes internet content available, but not producers of internet content or persons who uploaded or accessed internet content.

**Internet Content** is defined in Schedule 5 of the **Broadcasting Services Act 1992** as information that is kept on a data storage device and is accessed or available for access through an internet carriage service (a service that enables end users to access the internet). This includes websites, usenet newsgroups, peer-to-peer file sharing applications, live content such as ‘live’ streaming audio/video and adult chat services, and other types of content that can be accessed online or on a mobile phone, but does not include email.

Under the **Broadcasting Services Act 1992**, the following categories of internet content are prohibited:

- Any online content that is classified RC (Refused Classification) or X 18+ by the Classification Board (formerly the Office of Film and Literature Classification). This includes real depictions of actual sexual activity, child pornography, depictions of bestiality, material containing excessive violence or sexual violence, detailed instruction in crime, violence or drug use, and/or material that advocates the doing of a terrorist act.

- Content which is classified R 18+ and not subject to a **restricted access system** that prevents access by children. This includes depictions of simulated sexual activity, material containing strong, realistic violence and other material dealing with intense adult themes.

- Content which is classified MA 15+, provided by a mobile premium service or a service that provides audio or video content upon payment of a fee and which is not subject to a **restricted access system**. This includes material containing strong depictions of nudity, implied sexual activity, drug use or violence, very frequent or very strong coarse language, and other material that is strong in impact.

Classifications are based on criteria outlined in the **Classification (Publications, Films and Computer Games) Act 1995**, **National Classification Code** and the **Guidelines for the Classification of Films and Computer Games 2005**.

If the content is hosted in or provided from Australia and is prohibited, or is likely to be prohibited, ACMA will direct the content service provider to remove or prevent access to the content on their service.

If the content is not hosted in or provided from Australia and is prohibited, or is likely to be prohibited, ACMA will notify the content to the suppliers of approved filters in accordance with the Internet Industry Association’s Codes of Practice.
Laws Influencing and Restricting Defence Engagement in Social Media

Introduction

In this section of the overview, we will examine the legality of the information, claims, messages and elements contained within social media communications.

There exists a coalition of Australian laws and regulations that can influence and restrict claims, messages and desired take outs – achieved via a combination of content including moving and still images, text, logos, music and voice - contained within social media communications.

The laws that apply to communications upon conventional media also apply to social media communications. However, Defence and its members, when using social media for Professional Use and Private Use, face challenges in seeking to apply the existing laws to their communications due to the unique and evolving nature of social media.

As the social space is still being defined, any attempt to lay down a precise formula or code for Defence to follow on how to apply the existing laws to social media risks becoming obsolete by the time this overview is reviewed. Social media technology, platforms, applications, sites and communications techniques are simply evolving too rapidly.

Instead, in this section of the overview, we provide a social media flavoured overview of the relevant laws that exist today together with impending areas of law reform for Defence to bear in mind as it plans and executes social media campaigns and for Defence members to have regard to when they engage in social media.

Who might complain?

Social media communications are likely to impact upon a diverse range of interests and not all will be charmed by the social media message. There are numerous organisations, businesses and individuals that may feel aggrieved by the communication and who may wish to seek some form of legal or quasi-legal remedy to challenge the campaign or engagement, for instance:

- consumers who are misled or deceived by the message or are simply displeased by what they see;
- competitors who see their market share under threat;
- celebrities, character or brand owners whose ability to profit from endorsement may be diminished by an unauthorised use of their image, character or brand;
- community interest groups who may be particularly enraged by the message;
- individuals who may have their reputation and character brought into question by the message;
individuals who may claim that their privacy has been unfairly compromised; artists, musicians or writers whose original work may appear in the communication without their knowledge or consent; and Government bodies such as the ACCC who monitor communications and protect consumers.

To avoid costly court proceedings, adverse publicity or even the expense of discontinuing or modifying a campaign, any social media engagement that Defence intends to conduct should be cleared by Defence Legal or an external experienced legal professional to ensure compliance with the laws outlined in this overview that may impact upon the engagement.

**International laws that may apply to social media engagement**

Before launching into an overview of the laws that might apply to a proposed campaign or engagement, it is perhaps worth stating the obvious by noting that the internet and other digital technologies have brought about dramatic changes in the way individuals interact. Business can now be transacted all over world, transcending distance, time, borders and nationality. This is the realm of cyberspace.

Accordingly, a particular Australian campaign or engagement conducted via the social media channels or other digital technology has the distinct possibility of attracting ‘global liability’ where Defence or its members could potentially be subject to the laws of any country or state in the world. Still very much evolving are worldwide legal principles that determine whether a given country’s laws apply to a given site or communication originating in another part of the world, but viewable and able to be interacted with within a different country.

Defence must be alive to the possibility that use of the internet and social channels for a campaign or engagement intended for Australia, may not only attract individuals in another part of the world but might also result in organisations, businesses or individuals feeling aggrieved by the communication and therefore the risk of the application of foreign laws and regulations.

Evolving Australian and worldwide laws tell us that there are steps that can be taken to reduce the risk of global liability:

Subject to specific legal advice to the contrary, take the initial view that if the website or other social media can be accessed by individuals in a given country, then that country’s laws may apply to the media, the content of the communication and the message. If Defence or a Defence member is breaching one of the applicable Australian laws outlined in this overview, it is quite possible that an equivalent law will be breached in the overseas country.

To avoid being taken to court in the USA (and possibly in an increasing number of other countries), Australian websites need to ensure they do not create a campaign that somehow ‘targets’ the USA generally or one of its States, cities, geographical or cultural icons or persons resident. However, passive communication by itself is usually not sufficient to attract the reach of USA courts.
Consider prominent notices or country and state disclaimers about the reach and target of the site or page – what countries it is intended for and limitations based on nationality, language, currency or post code.

Consider limiting the nationality of the people that can actually access a website or alternatively, subscribe to online services available via the website.

Consider including appropriate choice of law and choice for forum (place for determination of disputes) conditions in the Engagement Principles that must agreed to in advance.

Consider using appropriate IP address blocking technology.

**Consumer protection laws**

The **Australian Consumer Law** (ACL) contained within Schedule 2 to the **Competition and Consumer Act 2010 (Commonwealth)** is now the preeminent piece of legislation that protects consumers against false communication and promotion.

The ACL applies as a law of the Commonwealth under the **Competition and Consumer Act 2010** and as a law of each Australian State and Territory by virtue of separate application legislation. As a result there is now one uniform consumer law throughout all jurisdictions in Australia.

Under the former **Trade Practices Act 1974**, the consumer protection provisions applied to corporations only. The equivalent provisions in the ACL are now directed to the conduct of ‘persons’, which include corporations, a body politic and individuals. Under Section 2A of the **Competition and Consumer Act 2010**, it is clear that, in so far as they carry on business, the Commonwealth and Commonwealth authorities are subject to the act.

A detailed examination of whether future engagement by Defence in social media has the potential to be caught by the **Competition and Consumer Act 2010** is beyond the scope of this overview. However, it is sufficient for our purposes to observe that provided the conduct has a sufficient trading and commercial character and a nexus with trade and commerce, there always exists the possibility that Professional Use and Private Use of social media may be caught by the ACL.

Adopting policies, practices and engagement principles in social media that are designed to comply with the ACL will go a long way to reducing the legal, commercial and reputational risks that may arise in social media.

The following are the primary consumer protection Sections of the ACL that may impact upon social media engagement and of which Defence and its members should be mindful:

- **Section 18** prohibits conduct that is misleading or deceptive or is likely to mislead or deceive. The remedies for a breach of Section 18 include injunctions, damages and corrective advertising.
Section 29 prohibits false or misleading representations, for example, false claims as to association, sponsorship, approval or affiliation, false claims as to price, false claims as to standard, quality, value or grade, false claims as to whether a product is ‘new’ or false testimonials. A breach of Section 29 may attract criminal penalties under Chapter 4 of the ACL, such as fines.

Section 48 ‘Clarity in Pricing’ provides that promoters must ensure ‘all-inclusive’ pricing in consumer campaigns. In order to prevent the creation of an impression that a product is being offered for a sale at a lower price than it actually is, advertising must prominently feature, as one price, the total amount a consumer must pay. That price must include all mandatory charges, taxes, duties, levies and all amounts payable under law. In other words, any cost that can be assigned a dollar value must be included in that one price. However, if elements of the price cannot be determined ahead of time or will vary depending upon the customer’s choice (i.e. they cannot be ‘quantified’ or will genuinely vary) those elements do not need to be included in the single price. In such cases it would be acceptable to state a ‘from’ price, provided of course that the price stated is accurate and it is clear that other price elements will depend on certain disclosed consumer choice or location factors (for example).

Section 32 states that it is illegal when promoting products to offer rebates, gifts, prizes or other free items with the intention of not providing them, or of not providing them as offered. A breach of Section 32 may also attract criminal penalties under Chapter 4 of the ACL.

Section 35 renders the practice of ‘bait advertising’ illegal. A breach of Section 35 may also attract criminal penalties under Chapter 4 of the ACL.

Section 49 prohibits businesses representing to consumers that they will receive a rebate on the agreed price of products or some other benefit in exchange for the names of other prospective customers if the receipt of the rebate or benefit is conditional upon a future event occurring. A breach of Section 49 may also attract criminal penalties under Chapter 4 of the ACL.

Section 18 Australian Consumer Law – Misleading or Deceptive Conduct

Section 52 of the former Trade Practices Act was one of the most litigated provisions existing in any Australian law. Section 18 of the ACL is in identical terms and the body of decided case law applying to Section 52 now applies to Section 18.

Section 18 is likely to be used by the organisations, businesses and individuals identified above if they feel sufficiently aggrieved by a social media engagement so as to commence legal proceedings.

To ‘mislead or deceive’ means to lead into error. This means that to infringe Section 18 the message in the social media communication would usually contain some form of misrepresentation. A message that merely causes a person to wonder or be somewhat
confused or uncertain will not usually be misleading or deceptive. People are accustomed to ‘puffing’.

In the social media communications context, a misrepresentation giving rise to breach of Section 18 can be caused or conveyed by one or a combination of written words, spoken words, images, graphics, video, animations, action sequences, music and silence.

It will be important for Defence during Professional Use of social media to objectively scrutinise any proposed communication or received communications from third parties for claims and representations that may be misleading or deceptive to the target audience.

Determining where to draw the line as to what is misleading or deceptive and what is not can be notoriously difficult in the social media communications context. There will of course be conduct and claims that are clearly deceptive in a given circumstance and conduct and claims that are clearly not. It is the edgy social media engagement mechanics and messages designed to draw people in that highlight the positives and understate the limitations that ‘sail close to the wind’ from a consumer protection perspective.

**Examples of a Section 18 breach in Social Media**

**Comments by Third Parties on Facebook and Twitter pages: ACCC v Allergy Pathway Pty Ltd [2009] FCA 960**

Allergy Pathway operates clinics for the diagnosis and treatment of allergies. In early 2009 the ACCC commenced proceedings against Allergy Pathway in respect of representations concerning its allergy diagnosis and treatment services. The representations were made in a series of publications. At the hearing Allergy Pathway did not contest the ACCC’s allegations and the court found that it had engaged in misleading and deceptive conduct in contravention of the then Section 52 of the *Trade Practices Act 1974*. Undertakings were given that the same or similar representations would not be made again for a period of three years.

Subsequently, the ACCC became aware that Allergy Pathway had continued to make representations concerning its services that were in breach of the undertakings given. The representations were found to have occurred in social media via the following channels:

- statements and links to statements posted by Allergy Pathway on its website, Facebook and Twitter pages and in a video posted on YouTube and on its Facebook and Twitter pages;
- testimonials written by Allergy Pathway’s customers and posted by Allergy Pathway on its website, Facebook and Twitter pages;
- Allergy Pathway’s responses to queries posted by members of the public on its Facebook ‘wall’; and
- testimonials written and posted by Allergy Pathway’s customers on its Facebook ‘wall’ – in this instance Allergy Pathway was found liable for the postings of third parties on Facebook because it knew that misleading testimonials had been posted on Facebook and Twitter and it took no steps to have them removed.
The significance of this decision is that organisations that promote themselves via social media channels including Facebook, YouTube and Twitter are now responsible for monitoring the content of their social networking sites and in particular user-generated content that is posted by third parties. If such content is misleading or deceptive, it should be removed.

Fake Profiles: Australian Competition and Consumer Commission v Jetplace Pty Ltd [2010] FCA 759

Jetplace operates an adult social networking and dating site known as ‘redhotpie’ that is used for social, dating and entertainment purposes. Members of the website create individual user profiles describing their characteristics and exchange ‘flirts’ and customised messages with other members.

The directors of Jetplace developed and implemented a formal policy at Jetplace surrounding the creation of fake profiles that were programmed to automate and schedule the sending of flirts and other messages to members and to appear in the visitor history of member profiles. Despite the creation of more than 1300 fake profiles, Jetplace represented on its website that:

‣ every profile had been created by a visitor to the site;
‣ any profile identified in a member’s search was created by another member; and
‣ every message received from a profile provided an opportunity to socialise on the website and potentially meet with another member.

The Federal Court found this conduct to be misleading and deceptive and that the website contained false and misleading representations. The site had to undertake corrective advertising by telling each user of the deceptive conduct when they logged on and also by sending a copy of a court imposed notice to the email address of each user.

This decision is important as it confirms that organisations must not mislead or deceive individuals during the process of social media engagement. For instance, organisations
would not be able to create false comments or posts to their site or Facebook page that purport to be from individuals when in reality they were created by the owner of the site or page. The same would apply to the uploading of fake user-generated content by the site or page owner that purports to be from a genuine third party who has an interest in the organisation.

**Passing off**

The old passing off tort action under the common law is different from the consumer protection laws discussed above and instead is designed to prevent a trader from damaging another trader’s reputation or goodwill by causing potential consumers to associate one trader’s product or business with another trader’s where no such association exists.

The passing off action can be used to protect brand and business names as well as a product’s ‘get up’ and even a distinctive social media campaign. The passing off action can be used by one trader against another, if:

1. the innocent trader’s get-up, including the brand name or business name is recognised by consumers as having a distinct and established reputation;
2. there has been a misrepresentation by the offending trader to consumers leading consumers to believe that the products offered by the offending trader are in fact the innocent trader’s products; and
3. the innocent trader has suffered or is likely to suffer damage to its business by reason of the erroneous belief created by the offending trader’s misrepresentation that the source of the offending trader’s products is the same as the source of those offered by the innocent trader.

Organisations need to bear the passing off action in mind when developing social media campaigns, particularly when the intended product to be promoted directly competes with another established brand or utilises the reputation of a well known brand or personality and the intention is to piggy back or cash in to a certain degree upon the established brand’s or personality’s identity and reputation.

For example, the tort of passing off and breach of the Trade Practices Act was used by Lara Bingle in a 2006 Federal Court action against a men’s magazine which published topless photos of her without her consent or permission. Similarly, the uploading of content by individuals and organisations to social media sites or pages in the form of images of well known celebrities or brands may result in a passing off action if there is a sufficient commercial nexus and the elements of passing off can be established.

**Trade marks**

Trade mark law in Australia is governed by the Trade Marks Act 1995 (Commonwealth). By virtue of Section 3, the Trade Marks Act applies to the Crown in the right of the Commonwealth.

A trade mark is any *sign* used to distinguish goods or services of one trader from those of
Trade marks are a vital tool in the brand protection arsenal. Most are familiar with Apple’s registered trade mark ‘iPod’ and other ‘Pod’ or ‘i’ related branding and Apple’s battle to stop other organisations laying claim to ‘pod’ and to prevent ‘pod’ falling into general usage.

It is also possible for phrases and slogans to be registered as trade marks, and for trade marks to play a significant role in the legal protection of celebrity personality in Australia. Increasingly, celebrities are turning to the protection offered by trade mark registration to prevent the unauthorised exploitation of their personalities in the commercial realm. Trade mark registration can protect various indicia of celebrity personality such as their name, signature and likeness.

When a trade mark is registered with the Trade Marks Office, it is registered in either one or more particular classes of goods or services that closely relate to the business that the proposed trade mark will promote in the marketplace. There are 45 different classifications of goods and services pursuant to which trade marks may be registered.

A trade mark owner has, subject to certain exceptions, the exclusive right to use and apply the trade mark to particular goods and services and to authorise other persons to use the trade mark by way of a licence.

Trade mark infringement can occur if an individual or organisation, without the consent of the trade mark owner (for instance without a licence deal), uses in social media communications a ‘substantially identical’ or ‘deceptively similar’ sign as a trade mark (i.e. used to indicate the origin or source of the products), in one of three ways:

- in relation to the goods and services in respect of which the mark is registered;
- in relation to goods or services which are the ‘same as’ or ‘closely related to’ the goods or services for which the mark is registered; or
- in relation to ‘unrelated’ goods or services, if the registered mark is well known or iconic in Australia and if the use is likely to suggest a trade connection with the trade mark owner.

Protection is absolute in the sense that that once wrongful use of the trade mark has been established by the trade mark owner, infringement is proven and there is no need to prove that there is confusion in the marketplace or damage as is the case with the tort of passing off (discussed above).

Defence members engaging in social media for Private Use need to ensure that they do not use the registered trade marks of others (particularly famous or well known trade marks) in their communications where the use may be seen to be use ‘as a trade mark’.

In circumstances where Defence invites the uploading of user-generated content from third parties as part of Professional Use, it will be very important to have clear rules of posting and then to censor the content to ensure that no well known trade marks are uploaded by third parties (see Engagement Principles below). While such use would often not be use ‘as a trade mark’ in the requisite commercial sense, and therefore would not
result in trade mark infringement, rules preventing the use of trade marks will go a long way to reducing the risk of complaint by trade mark owners and any associated adverse publicity.

To date, there have been no decided Australian cases in respect of the liability of social site or page owners arising from acts of trade mark infringement perpetrated by users. Clearly published Engagement Principles and a functional complaint and take down mechanism will go a long way to reducing any legal liability.

Copyright

Introduction

Copyright law in Australia is governed by the Copyright Act 1968 (Commonwealth). By virtue of Section 7, the Copyright Act binds the Crown.

Copyright protects from unauthorised reproduction or adaptation of original creations such as books and other literary works, computer programs, scripts, lyrics, paintings, sculptures, drawings, photographs, musical scores, films, videos, broadcasts, sound recordings and the choreography of a performance. The copyright owner has the exclusive right to reproduce, copy, publish, perform, broadcast, adapt, sell, licence and import copyright protected creations. The copyright owner also has the exclusive right to communicate the work to the public (broadcast or place on the internet) and to reproduce the work in a material form.

The general rule is that the ‘creator’ of a literary, artistic, dramatic or musical work and the ‘maker’ of a film, sound recording, broadcast or published edition are the copyright owners. Exceptions to this general rule include situations where the creator is an employee of an organisation.

For example, copyright can exist in logos and marketing designs, compilations of data, advertising material, computer programs, digital images, digital video content and video games. Film may have up to seven different copyrights and music up to three different copyrights.

Copyright laws in Australia only protect the form of certain works, not the ideas, concepts, formats or themes behind them.

Copyright in original work or material may be infringed where an organisation or individual, without the copyright owner’s permission:

- reproduces the work in a material form;
- publishes the work;
- communicates the work to the public;
- performs the work in public (literary, dramatic and musical works);
- adapts the work;
- makes a copy of a sound recording, film or broadcast;
- communicates a sound recording, film or broadcast to the public; or
- causes a recording or film to be heard or seen in public.
Professional Use and Private Use – Use of Content in which Copyright Subsists

Defence will generally need to comply with copyright laws during Professional Use when uploading content to its own socially enabled websites, blogs and social media site pages. The same will apply to Defence members engaging in social media for Private Use. There is a common misconception that just because content can be freely viewed online, it can then be freely used. As indicated above under the heading User-Generated Content, this occurs regularly in ‘mashups’ posted in social media by individuals and sometimes commercial and non-commercial organisations.

Unless one of the exceptions outlined below applies in respect of a given piece of content, in order to avoid potential liability for copyright infringement, it is best practice to assume that copyright will subsist in most items of original content that were not created by Defence or its members and obtain permission for its use from the creator. Permission should be in writing from the copyright owner or a person who has the right to deal in the copyright, and one must satisfy themselves that the person they are dealing with actually has the right to deal with the material in this way. The permission obtained needs to cover the particular use as well as allowing publication on the required social media channels.

Whilst an item of content may enjoy copyright protection, infringement of copyright will only occur where a **substantial or important part** of an original work is copied. When assessing whether a ‘substantial’ part of a work has been copied, the rule of thumb is to consider the quality of the element that has been reproduced rather than the quantity of the original work that has been copied. A common example given to illustrate this point is reproducing the smile of Mona Lisa - while the smile itself is not a sizeable portion of the painting, its significance and intrinsic value to the painting renders it to be a substantial part of the original work.

Further, if there has been a commercial purpose for the use of the copied part, if the copied part has been taken to save labour or if the owner’s and copier’s works compete, this may also have a bearing on whether the part taken is ‘substantial’.

The courts have consistently held that names, titles, slogans or phrases are not protected by copyright, as commonplace words or sentences will not be ‘original’ for the purposes of copyright law. Longer quotes can be reproduced provided the quote is not a substantial part (defined as an essential, distinctive or important part) of the original literary work, or if the literary work from which the quote came is no longer protected by copyright). However, the **Competition and Consumer Act 2010**, trade mark laws and the laws of passing off discussed above often restrict the way an organisation or individual can use a quote, name, title or slogan, particularly if the organisation complaining has established a reputation in what has been reproduced. It is worth observing that simple descriptive or editorial references to well known names, titles or slogans in social media (e.g. in a blog post or comment on Facebook) are unlikely to attract the attention of such laws.
If content is no longer protected by copyright, then it may also be freely used by Defence or its members in social media. Generally, the rules prior to 1 January 2005 were that copyright lasted until 50 years from the end of the year in which the creator died, or for some material, until 50 years from the end of the year in which the material was first published. Since 1 January 2005, works created or published on or after 1 January 1955 enjoy copyright protection to 70 years from the end of the year in which the creator died or 70 years from the end of the year in which the material was first published.

As far as content to be used in social media is concerned, the general rule is that if the creator of the content died before 1955, copyright in the content is likely to have expired under Australian law. While the expiry of copyright may be useful for some who wish to upload vintage content in social media, the vast majority of those engaged in social media seek to upload contemporary and relevant content. Subject to this content being an original work, copyright is likely to subsist in the content and care must be taken with its use.

It is recommended that Defence and its members ensure that they have permission (i.e. a licence) to use content that may be subject to copyright before creating user-generated content and deploying such content in social media. If unsure as to who might own an item of content or if you do not know who is in the image or video, it is best practice not to use the material in social media.

**Social Media Sites: Linking & Framing**

The essential architecture of the Web itself enables users to ‘surf’ the Web by clicking hyperlinks within website pages or from website to website through the use of hyperlinks. It may be of importance to Defence in its Professional Use of social media to be associated with other government organisations, NGO’s, businesses and individuals with whom Defence has established relationships. Through hyperlinks, legitimate associations between Defence and such organisations can be promoted via the Web. Furthermore, engagement in social media often involves the provision of links to newspaper stories, other blogs, content on YouTube and so on.

Where a website hyperlinks to the homepage of a target website, this is often referred to as **surface linking**. Framing occurs where a website contains a hyperlink to another site and when an individual clicks the link, the new site opens up in its own window but within the existing screen (i.e. the original website remains in the background and is clearly visible). This is the ‘frame’. Numerous frames can be viewed in separate parts of the screen at the same time while still functioning independently of each other.

Hyperlinks and framing also provide an opportunity for some organisations to derive a benefit or advantage by associating themselves with another organisation or their Web content without permission. For some time now, a rogue practice known as ‘deep linking’ has been utilised. As opposed to surface linking, deep linking occurs where an offending website links to an internal page within a target website that is not the target website’s homepage. Often the target website’s internal page is framed upon the offending website’s page making it look like they are part of the same website. The offending website often
obtains a benefit from the association or the content that resides within the target website. Further, the practice of deep linking usually bypasses the disclosures, terms and conditions and disclaimers that appear on a homepage, and therefore individuals also have the potential to be misled.

The Australian authorities support the view that linking or deep linking on its own is unlikely to raise issues under copyright law. This is because an organisation that provides hyperlinks on their website to content stored on remote websites does not make that content available, rather it is the remote website that makes the content available and thus there is no reproduction (one of the exclusive rights). However, if the links are to target sites that host infringing content there may be liability for authorising infringements (see below). Furthermore, unless embedding is expressly allowed by the social media site owners (e.g. the YouTube Embeddable Player) framing may also raise copyright concerns, as the viewer of the framed content may not be aware that the content has been drawn from a different source. This may result in the communication of a copyright work (another of the exclusive rights) albeit not a reproduction of that work.

It is therefore best practice to link and frame with the permission of the target site or in accordance with the target sites published rules and policies. As there is always a risk in social media that people will post links to infringing material, procedures need to be in place to manage risk if Defence is inviting or allowing such posts (see Engagement Principles below).

The practice of unauthorised linking or framing may result in an infringement of the other relevant laws, including:

**Moral rights.** The framing of or linking to content on a target website may lead to confusion as to ownership, which may infringe the copyright owner’s right of attribution or the right not to have authorship falsely attributed. If framing results in the target website’s content being displayed in close proximity to offensive content upon the offending website, the copyright owner’s right not to have work subject to derogatory treatment may also be infringed.

**Trade mark infringement.** Usually the mere use of a trade mark as a bare link will not be use ‘as a trade mark’ in a way that gives rise to infringement under the Trade Marks Act. However, if framing occurs and the target website’s trade marks are displayed within the offending website’s screen, this may result in use as a trade mark. Further, if the target website’s frame within the offending website suggests some form of association between the trade mark and the products promoted on the offending website, trade mark infringement may occur.

**Consumer protection laws.** Under the Competition and Consumer Act 2010 all that needs to be shown is that the nature of the linking and framing (including appearance of logos, titles and URLs) may result in a person being misled (Section 18). This could occur if the person is unaware that he or she has accessed the target website. In addition, the proximity and representation of the content, logos and trading names of the offending and innocent websites may suggest an association that does not exist (infringing Section 29).
Passing off. The elements of a passing off action may also be established by the owner of the target website in circumstances where the proximity and representation of the content, logos and trading names of the offending and innocent websites transgresses upon the innocent party’s goodwill.

When establishing links and frames on and from a website:
- always obtain permission from the target website;
- ensure that the organisation’s webpage does not imply an endorsement or connection with a target website, a personality, an individual or another business or the products of others unless there is permission;
- do not use names, trade marks, brands, products and slogans of other organisations; and
- do not use deep linking where the hyperlink avoids important disclosures or conditions of the target website’s homepage (or similar).

Authorisation Liability for User-generated Content

As discussed above, engagement in social media necessarily results in the creation of user-generated content. One of the risks Defence and Defence members face in inviting or allowing user-generated content during both Professional Use and Private Use is that of copyright infringement as an ‘authoriser’ of primary copyright infringement.

The exclusive rights of a copyright owner include the right to authorise another person to do any of the acts falling within the scope of the copyright owner’s exclusive rights (discussed above). So if a person or organisation authorises another person to do the acts without the licence or consent of the copyright owner, ‘authorisation liability’ may arise.

Whilst well known commercial content mashed up or contained within a content submission will readily be detected and intercepted, it is possible that ordinary or unknown content submitted by an individual will not be owned by that individual or used with the owner’s permission, resulting in copyright infringement. As this type of content is almost impossible to detect during the censorship process, it is likely that it will be published by Defence on the site and this is the likely point that authorisation liability may occur.

In such circumstances Defence may also be directly liable for copyright infringement by reproducing the material on its servers or for communicating the work.

Under Section 36(1A) of the Copyright Act 1968, the following matters will be taken into account in determining whether or not a person has authorised the doing of any act comprised in the copyright in a work:
- the extent of the person’s power to stop the infringement;
- the nature of the relationship;
- whether the person took any reasonable steps to prevent or avoid the doing of any act comprised in the copyright in a work.
The likelihood of copyright infringement taking place and the degree of indifference displayed by the organisation alleged to have authorised the infringement are relevant in determining liability. The Engagement Principles recommended below will assist greatly in this regard.

It is outside the scope of this overview to enter into a detailed examination of the so called ‘safe harbour’ provisions under the Copyright Act 1968 (Part V, Division 2AA) that received detailed attention in the much publicised iiNet cases (Roadshow Films Pty Ltd v. iiNet Ltd (No.3) [2010] FCA 24 and on appeal Roadshow Films Pty Ltd v. iiNet Ltd [2011] FCAFC 23). In short, these provisions limit the remedies available against carriage service providers for copyright infringement that occurs in connection with carrying out certain specified online activities. Generally such carriage service providers are often internet service providers (such as Telstra, Optus, Vodafone, iiNet and AAPT). The safe harbour provisions do not extend to organisations that own or run websites.

In circumstances where Defence invites the uploading of user-generated content from third parties as part of Professional Use it will be very important to have clear rules of posting and then to censor the content and include a functional copyright complaint mechanism to deal with allegations of copyright infringement on the site (see Engagement Principles below).

It is worth mentioning that there are a number of ‘fair dealing’ provisions in the Copyright Act that provide that certain acts will not constitute infringement of copyright. Such provisions can apply to the user-generated content environment and in certain circumstances may apply to Professional Use and Private Use of social media by Defence and its members.

The relevant ‘fair dealing’ provisions are as follows:

- **Reporting the News:** the use of the material must be ‘fair’ and the primary purpose must be to report or comment on news and not for example to entertain. It is also necessary to ensure that an acknowledgement of the person who created the content and any title is given unless the content is anonymous.

- **Criticism or Review:** the use must be ‘fair’ and the criticism or review must involve making a judgment upon the content concerned or the underlying ideas. The purpose of the criticism or review must be genuine. A commercial motive underlying the criticism or review may still result in copyright infringement.

- **Parody or Satire:** there is no definition of parody or satire in the Copyright Act so we must wait until a court has decided the meaning, although the Macquarie Dictionary defines ‘satire’ as the use of irony, sarcasm, ridicule denouncing vice or folly etc. and ‘parody’ as the humorous or satirical imitation of a serious piece of literature or writing. The use must be ‘fair’ and this may depend upon how much content is used, the context and if the copyright owner may suffer some form of commercial disadvantage. Just because an individual uploads user-generated content that has used copyright material in a humorous way does not necessarily mean that the use is covered by this exception. The ability to rely upon this exception must be balanced against the moral rights provisions (see Moral Rights below).
For the fair dealing provisions to apply the use must be ‘fair’ in the requisite sense. The Courts will look at whether the use was genuinely for one of the above fair dealing exceptions and the circumstances of the use including whether the use of the content was for commercial purposes, the circumstances of acquisition of the content and any detriment to the copyright owner.

**Moral rights**

In Australia there is a parallel set of rights to copyright which authors, creators and performers enjoy, known as moral rights. They were introduced into Australian copyright law by the [Copyright Amendment (Moral Rights) Act 2000 (Commonwealth)](https://www.legislation.gov.au/Details/C1992C01585).

Moral rights exist independently from the copyright that may exist in original material and may continue to be exercised by an author or performer even though the copyright ownership has transferred to another person. The key moral rights recognised are:

- The right of attribution of authorship or performership – i.e. the right to be identified as the author of a work or performer of a live or recorded performance.
- The right not to have authorship or performance falsely attributed – i.e. the right to prevent a person falsely suggesting or stating that they are the author of a work or performer.
- The right of integrity of authorship or performership – i.e. the right not to have the work or performance subject to any derogatory treatment.

Moral rights only apply to individuals and these rights can be waived by the person who holds the rights. Further, the holder of the rights can consent to a breach of the holder’s moral rights on a case by case basis. Recent changes to the Copyright Act have granted moral rights to performers such as dancers, actors and musicians as well as the original group of writers, composers and directors.

For the right of integrity to be infringed, the distortion or alteration to the material must be prejudicial to the author’s honour or reputation. Further, there is no breach of the right of attribution or of the right of integrity if an organisation or individual is able to establish that in the circumstances it was reasonable not to identify the author or that it was reasonable to subject the work to derogatory treatment, as the case may be.

Defence and its members who engage in social media for both Professional Use and Private Use have to understand that they may have to attribute third party material and be particularly careful if their intention is to retouch, edit, alter or distort third party content as part of mashups with their own user-generated content. Again, it is best to seek permission from the rights holder or alternatively, ensure that the alteration to the material or any derogatory treatment is reasonable in the circumstances.

In *[Meskenas v ACP Publishing Pty Ltd*](https://www.fedcourt.nsw.gov.au/search/index.html?Approved%20Rulings%20-1&Search%20Terms=Meskenas%20v%20ACP%20Publishing%20Pty%20Ltd)[2006] FMCA 1136, one of the first cases of its kind in Australia, ACP Publishing was found to have infringed an artist’s moral rights to be...
attributed as the author of a painting. ACP published a photo in Woman’s Day magazine of Princess Mary during a visit to the Victor Chang Cardiac Research Institute in Sydney. The photo showed the princess standing in front of a portrait of the late Dr Chang painted by the artist but the caption to the photo incorrectly attributed the painting to another artist. ACP failed to publish an apology in time and had to pay the artist damages.

Defamation

Defence and Defence personnel need to be conscious of the possibility that their social media communications in both Professional Use and Private Use may offend a particular individual or group of individuals to such an extent that they allege that they have been defamed as their character and reputation has been diminished by the portrayal of them.

Defence will need to be particularly vigilant to ensure that user-generated content uploaded to Defence sites or pages by individuals during Professional Use of social media does not defame an individual. This would apply in particular where a communication portrays a well-known public figure, corporate figure or celebrity.

Defamation occurs where one person communicates, by words, photos, video, illustrations or other means content which has the effect or tendency of damaging the reputation of another. Every person who authorises the publication of defamatory material or contributes to the publication of defamatory material, regardless of the precise degree of involvement, may be liable. Liability for participating in the publication can extend to organisations and individuals who own and operate traditional websites, chatrooms, blogs, wikis, podcasts or pages on the social media sites (for example, Twitter and Facebook).

Australia adopted uniform Defamation Acts in 2006 as part of ongoing law reform. Broadly speaking, under the uniform defamation laws you can say whatever you like about someone, no matter how private, sensitive or personally damaging it may be, as long as it is true and the truth can be proven if the matter goes to court.

Liability for a defamatory publication may also extend to situations where there has been a failure to prevent or terminate a publication by a third party, for example in the case of a defamatory statement posted for example to an internet bulletin board, blog site or social media site. If the owner of the website or social media page that allows user-generated content including commentary and postings, exercises or should be able to exercise editorial control over the postings and then allows defamatory material to remain on the website, the site or page owner could also be liable for defamation.

Notwithstanding a uniform national approach, defamation law remains very complex and a full discussion of defamation is well beyond the scope of this overview. However, Defence and its members need to be aware that the possibility of defamatory statements being published over the internet is very high due to the ease with which statements can be made and communicated.
For example, the humorous or satirical portrayal of well known public figures, corporate figures and celebrities remains popular in social media. Whilst there is a defence of ‘triviality’ in the Defamation Acts – if you are able to prove that the publication really caused no harm - merely because something is published in jest does not prevent cartoons, caricatures, jokes or satire from being subject to the laws of defamation.

It is the interpretation of the ordinary reader/listener/viewer and not the intention of the author that matters. If the ordinary person would interpret the communication as mere jest there will be no defamation. However, if the communication holds its subject up for ridicule (which is often the case) or where the attempted humour promotes a sinister underlying assumption of truth which might be defamatory, the author cannot claim that the communication was no more than comic nonsense.

It is worth mentioning that since the adoption of uniform laws in 2006, it is generally only living individuals that can sue for defamation and corporations are now unable to sue for defamation except if they employ fewer than 10 persons.

There are currently no decided Australian cases on the liability of internet intermediaries (internet service providers e.g. Telstra or iiNet and internet content hosts e.g. Facebook or Flickr) or site owners generally for defamation that is perpetrated by another person using their services or facilities. It is however well established in Australian law that the law of defamation applies in cyberspace and to internet publications and that the place of the defamatory publication will be the place where the online material is read or heard in a comprehensible form (High Court in Dow Jones & Company Inc v Gutnick (2002) 210 CLR 575).

The situation of anonymous posters on third party owned internet sites was recently considered in Moir & Datamotion v Gladman. In January 2010, IT company Datamotion Asia Pacific Limited (Datamotion), and its managing director, Mr Ron Moir commenced proceedings in the Western Australian Supreme Court in relation to defamatory material published about them on the internet forum HotCopper Australia (HotCopper). HotCopper is a forum in which online discussions take place in relation to companies whose securities are traded on the Australian Securities Exchange.

The defamatory material consisted of a series of defamatory posts by an anonymous user in various HotCopper discussion threads about Datamotion and Mr Moir.

Due to its privacy and confidentiality policy, HotCopper would not voluntarily disclose details it held in relation to the anonymous poster. Datamotion and Mr Moir obtained court orders against HotCopper’s owner which required disclosure of information about the anonymous poster under a pre-action discovery process. The information provided by HotCopper started a train of inquiry which led to the uncovering of the anonymous poster’s identity, proceedings for defamation being issued against him and the case quickly being resolved.

Analogous to defamation is the action of injurious falsehood, with an example of the risks website owners face highlighted under the Injurious Falsehood discussion below.
It is important to remember that social media has a very long memory and user-generated content is likely to remain embedded in cyberspace for a very long time. Further, the ubiquitous nature of social media increases the likelihood of a defamatory communication spreading quickly across the globe and being 'published' to many people, particularly if the content goes 'viral'. This can only increase the liability of an organisation or individual in the event that a communication contains defamatory content.

As with copyright, in circumstances where Defence invites the uploading of user-generated content from third parties as part of Professional Use, it will be very important to have clear rules of posting and then to censor and remove offending content and include a functional complaint mechanism to deal with allegations of defamation (perceived or real) on the site (see Engagement Principles below).

The case of Moir & Datamotion v Gladman demonstrates that Defence members when engaging in Private Use in social media may not be able to hide behind handles and anonymous postings should they decide to defame or ridicule an individual or organisation. Likewise Defence may be required to disclose the identities of contributors to its websites or social pages if posted user-generated content is defamatory and an individual brings Court proceedings, notwithstanding privacy obligations upon Defence (see below).

The implementation of appropriate Social Media Policies covering Professional Use and Private Use and Engagement Principles (discussed below) will assist in educating Defence members and third parties alike on appropriate social media conduct.

**Discrimination, hate speech & causing offence**

Defence and Defence personnel also need to be conscious of the possibility that their social media communications in both Professional Use and Private Use may be caught by the various Commonwealth, State and Territory discrimination and racial vilification laws and possibly even the Commonwealth Criminal Code.

In addition to censoring for defamatory statements, Defence will need to be particularly vigilant to ensure that user-generated content uploaded to Defence sites or pages by individuals during Professional Use does not contain content that is discriminatory or harassing or contain statements based on racial or religious grounds. Such content must be immediately removed from the site or page.

For example the **Racial Discrimination Act 1975 (Commonwealth)** provides in Section 18C that it is unlawful for a person to do an act, otherwise than in private, if:

- the act is reasonably likely, in all the circumstances, to offend, insult, humiliate or intimidate another person or a group of people; and
- the act is done because of the race, colour or national or ethnic origin of the other person or of some or all of the people in the group.

In **Jones v Toben** [2002] FCA 1150 the Federal Court found that the respondent had breached Section 18C by publishing material online which was reasonably likely, in all of the circumstances, to offend, insult, humiliate and intimidate Jewish Australians
or a group of Jewish Australians. The Court was further satisfied that the respondent published the offending material because of the ethnic origin of Jewish Australians. The Court made an order declaring that the respondent engaged in conduct rendered unlawful by the Racial Discrimination Act and made orders requiring the respondent to remove the offending material, and any other material the content of which is substantially similar to the offending material, from all internet sites controlled by the respondent and not to publish or republish such material.

The Commonwealth Criminal Code, updated through the Crimes Legislation Amendment (Telecommunications Offences & Other Measures) Act (No. 2) 2004, features offences of using a carriage service ‘to menace, harass or cause offence’.

The offence is found in Section 474.17 of the Code:

474.17 Using a carriage service to menace, harass or cause offence

(1) A person is guilty of an offence if:

(a) the person uses a carriage service; and

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

Penalty: Imprisonment for 3 years.

‘Carriage service’ has the same meaning as in the Telecommunications Act 1997 (Commonwealth) Section 7, being a service for carrying communications by means of guided and/or unguided electromagnetic energy. This definition is broad enough to capture telephone calls, email, SMS and other online communications. Individuals using social media and other related communications channels to menace, harass or cause offence may be liable to prosecution under this offence provision.

The implementation of appropriate Social Media Policies (discussed below) covering Professional Use and Private Use will assist in educating Defence members on appropriate statements to make in social media.

Finally, it is worth mentioning that extant Defence policies on equity and diversity may also need to be examined and revised in order to ensure that Defence members understand their responsibilities to each other during Personal Use of social media. Equity and diversity in Defence as an organisation is an important but broad area that encompasses legal as well as cultural issues. The impact of social media upon equity and diversity policy in Defence is presently beyond the scope of this overview and will need to be examined in greater detail once Defence has indicated how it intends to embrace and engage in social media as an organisation following consideration of the preliminary George Patterson Y&R Social Media Review.
Injurious falsehood

Whilst defamation is primarily concerned with the protection of reputation of an individual, Defence and its members also need to be conscious of a related legal action known as the tort of ‘injurious falsehood’ that can be brought by commercial entities.

An injurious falsehood case may be brought against an organisation or individual where it is alleged that their communications contain false statements concerning the property, goods or services of another person or entity.

An aggrieved person or entity will succeed in such an action where:

- the communication contains a false statement concerning the person’s products or business;
- the communication is published in the marketplace;
- the organisation or individual acted with some malice; and
- as a result of the false statement, the person has suffered some actual financial loss.

Kaplan v Go Daddy Group Inc [2005] NSWSC 636 involved the tort of injurious falsehood. The defendant created a website with the domain www.hunterholdensucks.com.au and a disparaging blog about Hunter Holden that encouraged other users to post derogatory comments about this business. Comments were posted to the blog, all of which contained defamatory comments about the business. The plaintiff applied to the Court for an injunction to prevent the defendant 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 derogatory comments about the plaintiff in his blog.

Again, the law of injurious falsehood is complex and a full discussion is well beyond the scope of this overview. However, Defence and its personnel need to be aware of the possibility of injurious falsehood being alleged in response to social media communications. Clearly published and enforced Engagement Principles will go a long way to reducing risk in this regard.

Privacy laws

Many individuals are concerned about the collection and use of their personal information, particularly in respect of the internet and mobile technologies.

For instance, social media has the ability to create sophisticated consumer profiles
from the information provided unknowingly by internet and mobile users. As technology enables large volumes of data to be collected, stored and accessed quickly and easily, organisations have been quick to capitalise upon the different ways in which personal information can be used.

In addition, individual privacy has been further eroded by the proliferation of digital cameras, mobile devices with camera and video capabilities, the rise of user-generated content websites, improved search engines and the indexing of internet content. Personal information can now be captured in digital form, uploaded and then retrieved with ease.

Many of these technologies have a real or potential impact upon privacy. New challenges to privacy are now presented by digital rights management, geo-location technologies and computing in the ‘cloud’. Concerns continue to be raised due to high profile incidents involving the disclosure of personal information such as names, addresses, credit card details and social security numbers. The information disclosed by users of the social media sites, particularly Facebook and Twitter, has also raised privacy concerns. Individuals that engage with social media post a significant amount of information about themselves and others online that can be collected and reassembled to create accurate profiles of individuals and their lives, habits and preferences.

At this time there is no general right to privacy under Australian law. Personal information is protected under a mix of Commonwealth, State and Territory laws and the actions for breach of confidence and if applicable, contract law. Furthermore, some recent lower Australian court decisions have recognised a limited tort of invasion of privacy in Australia.

The privacy laws that predominantly impact upon the activities of the private sector are to be found in the Privacy Act 1988 (Commonwealth) which was amended in late 2001. On 21 December 2001 the private sector amendments to the Privacy Act became operative. The amendments provided for ten National Privacy Principles (NPPs), found in Schedule 3 of the Privacy Act, which apply to the private sector. At this time the Privacy Act does not apply to organisations that are small business operators (a business with an annual turnover of $3 million or less) or registered political parties.

The Privacy Act also applies to Australian and Australian Capital Territory government agencies through the Information Privacy Principles (IPPs) set out in Section 14 of the Privacy Act. There are 11 IPPs that set out how government agencies may collect, use, store and disclose ‘personal information’ which is defined in Section 6.

The 11 IPPs are as follows:

- Principle 1 - Manner and purpose of collection
- Principle 2 - Solicitation of personal information from individual concerned
- Principle 3 - Solicitation of personal information generally
- Principle 4 - Storage and security of personal information
- Principle 5 - Information relating to records kept by record-keeper
- Principle 6 - Access to records containing personal information
- Principle 7 - Alteration of records containing personal information
Principle 8 - Record-keeper to check accuracy etc. of personal information before use
Principle 9 - Personal information to be used only for relevant purposes
Principle 10 - Limits on use of personal information
Principle 11 - Limits on disclosure of personal information

Whilst the IPPs apply to Defence, including any engagement in social media for Professional Use where personal information may be collected, it is unlikely that the NPPs would apply to Defence members collecting personal information during Private Use of social media.

Government agencies are expected to set high standards for information handling. This is because, unlike other sectors such as the private sector, individuals may not have alternatives or substitutes to the services performed or provided by government and may have no choice other than to provide their personal information. Thus in the social media context it will be particularly important for Defence to publish privacy notices that comply with the IPPs at the point of collection of personal information.

**Privacy Law Reform**

At the time of writing, the Privacy Act is limited in its application to the protection of ‘personal information’, which is defined in Section 6 as:

‘information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.’

The problem with the definition as it currently stands is that it is unlikely to apply to technology which makes it possible to process data relating to individuals that is not linked to their immediate identity. While the definition covers a person’s name, address date of birth, telephone number, family members, photos or videos, most commentators are of the view that the definition does not cover an individual’s IP address, mobile telephone number and email address.

On 31 January 2006, the Australian Law Reform Commission (ALRC) commenced an enquiry into the extent to which the Privacy Act and related laws continue to provide an effective framework for the protection of privacy in Australia. A final report was delivered to the Australian Attorney-General in late 2008. The Government released the first stage of its response to the ALRC Report 108 on 14 October 2009.

On 24 June 2010, the Government released exposure draft legislation containing an important element of the first stage response – the proposed Australian Privacy Principles (APPs), which unify the current Information Privacy Principles and the National Privacy
Principles. These proposed principles were tabled in the Senate for referral to the Senate Finance and Public Administration Committee. The Committee held public hearings on the Principles on 25 November 2010, and the Committee's report was tabled on 15 June 2011, with a final reporting date of 30 September 2011. On 31 January 2011, the Government referred the second component in the first stage of the Government's privacy reforms, the credit reporting provisions, to the Senate for tabling, and for referral to the Finance and Public Administration Committee to consider. Stage 2 of the Government’s response will consider the remaining recommendations in the ALRC report once the first stage reforms have been progressed.

The 13 new APPs apply to ‘entities’, that is, Federal Government agencies and private sector organisations. The APPs expand the obligations upon government and business and increase privacy protections from that currently existing in the IPPs and NPPs.

One element of Privacy Act reform is the new definition of ‘personal information’. The new definition contained in Section 15 of the APP's provides as follows:

‘Personal information means information or an opinion about an identified individual, or an individual who is reasonably identifiable:

(a) whether the information or opinion is true or not; and

(b) whether the information or opinion is recorded in a material form or not.’

It is likely that this definition will result in a significant expansion of coverage of the Privacy Act as the test for what is ‘personal information’ moves away from precise identity to simply being able to identify a person indirectly. This is likely to occur when an individual visits a website on more than one occasion and through the use of IP addresses, cookies, web bugs, Hypertext Transfer Protocol (HTTP) and spyware the individual is reasonably identifiable through his or her browsing behaviour.

If personal information is being collected during social media engagement, then the APPs will need to be complied with. Of particular importance to Defence during Professional Use include the following proposed APPs:

**APP 1** – Open and transparent management of personal information. This principle expressly mandates that an entity must have a clearly expressed and up to date privacy policy covering specified matters including how information is collected, how to complain and the purposes for which the entity collects, holds, uses and discloses personal information.

**APP 2** – Anonymity and pseudonymity. This principle provides that individuals should be permitted to interact with entities while not identifying themselves or by using a pseudonym, where it is lawful and practical to do so.

**APP 3** – Collection of solicited personal information. Entities must not collect
personal information unless it is reasonably necessary for, or directly related to, the entity’s functions or activities. Defence will need to carefully consider this on a case by case basis.

**APP 4** – Receiving unsolicited personal information. If an entity receives unsolicited personal information, the information is still afforded privacy protection and the entity must then determine if it had the right to collect the information under APP 3 and if so the balance of the APPs would apply. It is important to consider APP 4 in the context of social media engagement where unsolicited personal information may be disclosed by individuals to Defence.

Thus in the course of engaging in social media for Professional Use, Defence will need to ensure that an up to date privacy policy is available for viewing and download (free of charge) at the point of collection of personal information. Further, Defence will need to carefully consider in light of APP 2 whether it will mandate the need for individuals to disclose their identities if they wish to post comments, blogs or upload user-generated content during social media engagement. Defence may not consider it practical to allow pseudonyms due to the risks of copyright infringement, defamation or a breach of one of the other laws identified in this overview. Indeed, the disclosure of identity is recommended in the Engagement Principles outlined below.

**Images of Third Parties in User-generated Content – Privacy Considerations**

Often user-generated content uploaded during the course of social media engagement will contain images of individuals who may not necessarily be the individual uploading the content. Such individuals will often be the uploader’s friends or family members but on other occasions the individuals may also be unknown third parties that were caught in the background or were deliberately captured by the uploader during an event of interest.

The Engagement Principles suggested below make it a positive obligation upon the uploader to agree that no content will be uploaded unless all individuals depicted in the content have granted their consent or would otherwise expect their image to be used by the uploader in social media. However, it will not usually be practicable to confirm such consent. If Defence invites image-based user-generated content during Professional Use the privacy implications need to be considered if the third parties have not provided the necessary consent to the upload.

In this context it is important to ask whether there are any rights in Australia that people have to protect their ‘personality’ or their ‘image’ from use in social media. Under Australian
law there is no specific law aimed at preventing the unauthorised use of a person’s image (unlike the United States which has *right of publicity* laws which provide that an individual has the right to control and profit from the use of his/her name, likeness and persona).

Copyright law is of little assistance in preventing unauthorised use of an image because the person who owns the copyright in the social content will generally be the person that created and uploaded the content rather than the person who appears in the content.

The areas of law in Australia which may be used by an individual to try and prevent the unauthorised use of his or her image are as follows:

- **Defamation.** The publication of a person’s image without their consent is not in itself proof of defamation. The unauthorised use of the image would need to either lower the public’s estimation of the person, expose the person to hatred, contempt or ridicule, or cause the person to be shunned or avoided.

- **The Competition and Consumer Act 2010.** Sections 18 and 29 prohibit commercial conduct which misleads or deceives consumers. To prevent the unauthorised use of an image under this law it is necessary to show that the use of the image would mislead or deceive consumers. The mere use of a person’s image is unlikely to be found to mislead or deceive under this area of law unless that person is a celebrity or well-known endorser of products. If a person is a celebrity or otherwise well-known, then the unauthorised use of their image in connection with trade or commerce may constitute misleading or deceptive conduct. This is because the public would be led to believe that the celebrity is endorsing the product or is connected somehow with the site upon which the image was uploaded. If there is nothing in the unauthorised use of the image which misleads or deceives a court would not find in favour of the person whose image is used.

- **Passing off.** The law of passing off is designed to protect the reputation of a business from misrepresentation and the possibility of an opportunity to exploit a person’s image for gain. To succeed in an action for passing off the complainant must have a reputation and there must be a misrepresentation which causes damage or the likelihood of damage to the individual. Because a reputation is required to successfully establish passing off, this law is of limited use for the ‘average person in the street’.

- **Privacy Act.** If the image of the third party and any associated text or content results in the individual being ‘reasonably identifiable’ then this may constitute ‘personal information’ for the purposes of the new APPs. If so, the image may be unsolicited personal information for the purposes of APP 4 and would need to be handled in accordance with the APPs.

- **Invasion of privacy.** Whilst there is no right to privacy in Australia, some recent developments in the Australian courts leave open the possibility of a future or limited tort of invasion of privacy in Australia. A tort is a private, civil wrong or injury for which the court may provide a remedy for any damage caused. The tort would only apply where the information disclosed was of a private nature and often images of persons are taken with their knowledge for the purpose of being shown.
As with the other laws influencing and restricting Defence engagement in social media for Professional Use, where Defence invites the uploading of user-generated content from third parties as part of Professional Use, it will be very important to have clear rules of posting and then to censor and remove offending content and include a functional complaint mechanism to deal with privacy complaints on the site (see Engagement Principles below).

**SPAM laws**

The sending of ‘commercial electronic messages’ in Australia is governed by the SPAM Act 2003 (Commonwealth).

A basic definition of ‘commercial electronic message’ is provided by Section 6 which essentially provides that some commercial nexus is required, through offering to supply goods or services or advertising or promoting goods, services, land, prospective suppliers or business opportunities. Under the SPAM Act, commercial electronic messages include messages sent by way of email, IM (Instant Messaging) and Mobile Wireless Technology (MWT) including SMS (Short Message Service), MMS (Multimedia Message Service), Wireless Access Protocol (WAP) and 3G.

The SPAM Act prohibits the sending of commercial electronic messages to an individual unless that individual has consented to receiving such communications. That consent can take the form of ‘express consent’ or ‘inferred consent’.

Whilst the Spam Act binds the Crown in each of its capacities and applies to government departments, the occasions upon which Defence would actually need to send commercial electronic messages may be somewhat limited. To prevent any unintended restriction on communication between Government and the community, the Spam Act contains a limited exemption for some commercial electronic messages sent by government bodies. These messages are called ‘designated commercial electronic messages’. Defence will need to consider the application of the Spam Act on a case by case basis.

In the social media context it is unlikely that Private Use of social media would often attract the requirements of the Spam Act. Defence may need to consider the application of the Spam Act if, as part of its Professional Use, it collects through social media engagement email addresses and mobile telephone numbers in order to generate a database of individuals who are interested in Defence and its activities and wish to be kept up to date with Defence related matters including news, articles or recruitment drives.

Whilst such communications may not often have a sufficient commercial nexus to be caught by the definition of 'commercial electronic message', Defence should be seen to meet and exceed the high standards expected of business. Thus it is always best practice to comply with the Spam Act requirements for individuals to have ‘opted in’ to receiving such communications from Defence to confirm consent and for each electronic message to contain accurate sender information (including how Defence can be contacted) and contain a functional unsubscribe facility.
**Recordkeeping Obligations**

Defence should also be aware that its social media communications arising from Professional Use are likely to generate Commonwealth records that will attract auditing, recordkeeping and disclosure obligations under the numerous Commonwealth acts and regulations that can apply to Defence.

Key auditing, recordkeeping and disclosure legislation applicable to Defence includes the following:

- Archives Act 1983;
- Freedom of Information Act;
- Privacy Act 1988;
- Evidence Act 1995;
- Public Service Act 1999;
- Financial Management and Accountability Act 1997;
- Auditor-General Act 1997; and

Given the dynamic nature of social media communications and the collaborative approach to the creation of user generated content, Defence will need to take particular care to ensure that such content is properly identified as a Commonwealth record as and when it is created. An accurate and authentic copy of such content will need to be captured and saved as a record so as to ensure that obligations under the relevant auditing, recordkeeping and disclosure legislation can be met. This is likely to require the development of a specific Defence social media records policy that provides guidance for each particular social media channel to be used by Defence during Professional Use.

The specific application of such legislation and the development of policy to regulate Professional Use of Social Media by Defence should be examined and will need to be considered further once Defence has indicated how it intends to embrace and engage in social media as an organisation following consideration of the preliminary George Patterson Y&R Social Media Review.

**The rules of proprietary space**

The numerous mainstream and niche forums, blogs, file sharing and social networking sites are all owned and operated by entities and companies who govern the terms and conditions of use and set rules that the user community must follow. As such this property may be referred to as ‘proprietary space’.

Defence will be well aware that most social sites offer their own unique social media communications options and solutions. Organisations no longer have to encourage
individuals to independently visit their Facebook page, YouTube channel or Twitter site. Today we see the social media sites becoming a key part of an organisation’s site and this is in turn broadening their engagement and exposure in social media. For example, the Defence homepage at www.defence.gov.au already has links to its Flickr, Twitter and YouTube pages.

As a condition of using proprietary space for communications, Defence must not only comply with the applicable laws discussed in this overview, but must also agree to the legal terms, conditions and policies set by the propriety space owners. As such terms and conditions constitute a contract between the site and user, they act in a very real way to influence and restrict communications activities upon proprietary space.

The particular rules of each proprietary space site are important for Defence to understand as they often reinforce the applicable laws and the consequences of a breach of the rules of proprietary space can sometimes be quite severe, including suspension and account termination. The rules must be examined carefully as they are prepared by the owners of proprietary space and are always drafted in their favour. These rules govern all aspects of use and are often changing.

As Defence continues to engage with individuals and other organisations on the social media sites for Professional Use it must constantly monitor the current rules and terms of use to ensure that the intended use is permitted and to determine what limitations on the use of the social media features may apply.

**Social media engagement principles**

The ‘Engagement Principles’ refer to terms and rules upon which Defence agrees to allow individuals and other organisations to engage with Defence in social media. In a similar way to the operation of the rules of propriety space employed by the social media site owners, the Engagement Principles should reflect the applicable laws and regulations that apply to Defence and operate in a practical way as part of an overall strategy to reduce the legal and reputational risks associated with the social media engagement identified.

Furthermore, the Engagement Principles form part of a suggested holistic approach to risk management in social media. Whilst the Engagement Principles govern how the outside community may engage with Defence, the Social Media Policies discussed below govern how Defence and its members engage with the outside community and with each other. This combined approach will enhance legal compliance and reputational awareness, engender a culture of appropriate ‘netiquette’ and reduce the risks for all stakeholders.
The suggested Engagement Principles for Defence to consider before committing to a social media communication or engagement campaign for Professional Use are as follows:

To minimise legal risks, Defence should be prepared to consistently monitor its sites and pages for derogatory or otherwise harmful content and if such content is posted remove it immediately, block the offender (if possible) and take any other reasonable action.

Each social media site or channel is unique enabling Defence to engage with individuals in different ways. Furthermore, each social media communication will also be unique. Therefore Defence will need to conduct an appreciation to consider applicable laws, assess risks and thereby determine most appropriate courses of action. Defence must assess the suitability of the social media channel for its intended communication and ask the question – ‘is social media suitable?’

As part of this process Defence will need to assess the type of individual that will be engaged and the reaction and participation of the individual. As part of this process it is vital that Defence has a public relations engagement plan ready to go once a social media campaign goes live that provides guidance how to respond to:

- praise;
- complaints;
- questions; and
- general conversation.

A public relations plan that addresses response times, issue resolution protocols and provides a process for handling enquiries will ensure that any emerging legal and publicity issues are diffused if possible and not compounded.

Where possible do not allow user-generated content to be posted anonymously by requiring individuals to identify themselves through a registration process. This will act as a strong deterrent against breaches of the Engagement principles. Such identifying information should include real names, address and telephone number as well as email address although this information should not be available to third parties.

Ensure that banner ads, Facebook ads, YouTube links / channels and all other seeds in social media that grab the attention of individuals to drive them back to Defence’s ‘home base’ website, Facebook page or blog do not contain tricks or other deceptive elements.

Beware of tricky communications that may go beyond mere wonderment or confusion and become misleading to others.

Ensure that all user-generated content is censored before being allowed to ‘go live’ or at least monitored for obvious legal infringements or breaches of the
Engagement Principles Defence has set. Obvious legal infringements should be immediately removed.

Remove obvious infringements of commercial content in ‘mashups’ (written, aural or visual).

Remove content that tends towards being defamatory to an individual, injurious to a business or contains discriminatory or racially intolerant remarks – remember unlimited scope for re-publication in social media.

If there is to be an extended or expanded use of the content then Defence should obtain talent and property releases of people and property appearing in content.

Defence must be careful not to directly encourage breaking of the law via its engagement mechanics.

Defence must obey its own published Engagement Principles.

Suggested Engagement Principles to be published to the community that seeks to engage with Defence are as follows:

- If applicable, convey rules around use of Defence trade and service marks and iconic defence related images by individuals (e.g. the rising sun badge or the Army logo).
- To avoid copyright infringements set clear rules about not using commercial content (unless Defence has a licence to certain content that individuals may access and use for the purposes of the particular engagement).
- To avoid copyright infringements set clear rules around not using any form of content unless the content was entirely created by the individual or is being used with the express permission of the content owner. This must apply to all elements in the content including for example any music that is playing as background to audio-visual content.
- Provide content rules applicable to the engagement and expressly state that Defence is able to remove content in its discretion.
- No uploading of content that contains images of third parties unless the uploader has permission from persons appearing in content or would otherwise expect due to the relationship that their image would be shared in social media.
- Provide behaviour rules and codes of conduct to be observed during content creation.
- Outline any applicable safety issues and guidelines.
- Clearly deal with the question of who owns the intellectual property rights in any user-generated content posting. If Defence will own the content then this should be stated, otherwise it should be clear that Defence is granted a licence to use the content for the intended purpose and any other future intended purpose.
To avoid intermediary liability have an obvious and functional complaint and take down mechanism to provide a channel for third party complaints around privacy, copyright infringement, trade mark infringement, defamation, falsehoods and discrimination.

Provide disclosures and disclaimers around any links to third party sites existing on the Defence site.

Have very clear upfront ‘opt-in’ consents and disclosures around future electronic and physical communication with the individual if the intent of the campaign is to build or expand a database of individuals interested in Defence - this will ensure best practice Spam Act and Privacy Act compliance.

Have a comprehensive and easy to understand APP compliant privacy policy that is readily accessible at the point of engagement that clearly explains the purpose of collection of personal information and how it will be used in the future.

If Defence is establishing a blog on its own website then it should establish an appropriate code of conduct for contributors, addressing for example:

- who the code applies to and when it applies;
- copyright ownership in posts and ability to maintain and re-post the posts as required;
- general ‘netiquette’;
- outlawing personal attacks and defamation;
- outlawing unacceptable / inappropriate content;
- outlawing racism, sexism, ageism and religious intolerance and vilification;
- rules on inappropriate and foul language (swearing);
- rules on identifying or referring to third parties;
- rules on providing personal information that may lead to identifying the individual and third parties; and
- outlawing illegal content and activities.

The Engagement Principles outlined above are by no means exhaustive and are provided as a suggested checklist that Defence may consider when it engages in Professional Use of social media and invites or allows the uploading of any form of user-generated content. The Engagement Principles may have general application or may be created for a specific social media engagement activity or promotion.

It is most important that Engagement Principles are clearly brought to the attention of individuals at the point of engagement with Defence via the social media channel. If the rules are only available via an obscure hyperlink or buried in fine print it is unlikely that they will be read by most users and Defence’s ability to rely upon them thrown into doubt. Best practice is for the rules to be ‘accepted’ by ticking a check box (or similar) before being allowed to participate.
Social media policies

a Social Media Policy may govern how Defence and its members engage with the outside community and with each other during Professional Use and Private Use. Such a policy is a conscious effort to inform members about what is appropriate behaviour in social media.

The objective of a Social Media Policy is to set parameters on the use of social media, whether as part of a member’s professional responsibilities or in a personal capacity and to limit the risk of damage being caused to Defence and members arising out of such use.

A properly drafted and enforced Defence policy on the use of social media by members is Defence’s most effective risk management tool in protecting itself against legal liability and harm to its reputation from the use of social media in during both Professional Use and Private Use.

Some general considerations in creating and implementing a social media use policy include:

- Stressing the ownership and ability to monitor Defence networks and systems and related equipment and explaining that privacy cannot be expected with the usage of such systems. The Federal Court has confirmed in *Griffiths v Rose* [2011] FCA 30 that the monitoring by a government department of its employees’ personal use of IT systems will not constitute an invasion of privacy provided employees are informed that such scrutiny will occur. However, the policies do have to be broad enough to cover the types of personal information that may be collected.

- The level of tolerance for personal use of social media by members during work times.

- How members will be trained once the policy is in place so that the intent of the policy can be explained and practised consistently by all members.

- Remind members to familiarise themselves with their terms of employment and all other applicable Defence policies and instructions.

- State that the policy applies to multi-media, social networking websites, blogs and wikis for both Professional Use and Private Use.

- Social media postings should not disclose any information that is not allowed by other policies and instructions, is confidential or proprietary to Defence or to any third party that has disclosed information to Defence, including the personal information of other Defence members.

- In Private Use Defence members should neither claim nor imply that they are speaking on the Defence’s behalf.
If a member comments on any aspect of Defence during Private Use they should clearly identify themselves as a member and include a disclaimer. The disclaimer may be as simple as: ‘the views expressed are mine alone and do not necessarily reflect the views of Defence.’

Social media postings should not include Defence logos or trade marks unless permission is asked for and granted.

Social media postings must respect copyright, privacy, defamation, trade mark, consumer protection and other applicable laws.

Defence will need to authorise specific members and approve member communications upon Defence blogs, Facebook pages, Twitter accounts, YouTube channels etc. for Professional Use.

Defence will need to ensure that the Defence records management policy is followed where Commonwealth records are created during Professional Use of social media.

Defence should reserve the right to request that certain subjects are avoided, and request that members withdraw certain posts and remove inappropriate comments as a result of Private Use when the interests of Defence and a member’s employment are involved.

Consider repercussions for policy violations for both Professional Use and Private Use of social media.

Ensure the policy is able to respond to the ever changing social media landscape. As required update the policy so that it remains relevant and ensure members are made aware of any changes. Additional training may be required.

Defence will of course need to consider its own unique requirements when developing a social media policy. Regard must be had to the extant Defence-specific laws, regulations, policies and guidelines that will shape and inform the content of a policy. Further, the laws and regulations discussed in this overview will also influence the policy and the outcomes Defence is seeking to achieve.

It would seem that there are two approaches to creating a social media policy. One approach is to prepare an all-inclusive policy that addresses all currently available social mediums or policies can be created that are specific to each social media network that are used for Professional Use and currently by members during Private Use. Different social media channels have different implications for Defence. Either way, a social media policy should contain some key ingredients and the following is a suggested list of issues that may form part of a policy:

- **Scope** - who the policy applies to and how is it incorporated.
- **Definition** – what is social media (as applicable to Defence) and list the forms it may take.
- **Consequences for failure to comply.**
- **Contact** – to report any inappropriate use of social media.
Clearly distinguish between Professional Use and Private Use of social media.

For Professional Use of social media:

- Only those authorised to comment may do so as a representative of the Defence;
- Explain process of authorisation;
- Follow Defence records management policy for Commonwealth records;
- Set out what can and cannot be done, for example:
  - disclose you are an employee/contractor of Defence, and use only your own identity, or an approved official account or avatar;
  - disclose and comment only on information classified as public domain information;
  - ensure that all content published is accurate and not misleading and complies with all relevant Defence policies;
  - ensure you are not the first to make an announcement (unless specifically given permission to do so);
  - comment only on your area of expertise and authority;
  - ensure comments are respectful of the community in which you are interacting online; and
  - adhere to the Terms of Use of the relevant social media platform/site, as well as copyright, privacy, defamation, contempt of court, discrimination, harassment and other applicable laws, and other Defence policies and guidelines.

- If you are authorised to comment as a Defence representative, you must not:
  - post or respond to material that is offensive, obscene, defamatory, threatening, harassing, bullying, discriminatory, hateful, racist, sexist, infringes copyright, constitutes a contempt of court, breaches a Court suppression order, or is otherwise unlawful;
  - use or disclose any confidential or secure information; and
  - make any comment or post any material that might otherwise cause damage to the reputation of Defence or bring it into disrepute.

- Set out a moderation policy and approval processes.
- Provide a frequently asked questions section.
- Provide examples of acceptable and unacceptable social media communications.
For Private Use of social media:

- Have a separate set of guidelines (best practice).
- Do not restrict use but encourage best practice behaviour.
- Provide a frequently asked questions section.
- Provide examples of acceptable and unacceptable social media communications.
- For example, state that members must:
  - take responsibility for what they post and exercise good judgment and commonsense;
  - only disclose and discuss publicly available information;
  - ensure that all content published is accurate and not misleading and complies with all relevant Defence policies;
  - expressly state on all postings (identifying you as a Defence member) the stated views are your own and are not those of the department or the government;
  - provide the suggested disclaimer;
  - be polite and respectful to all people you interact with;
  - adhere to Defence equity and diversity policy; and
  - adhere to the Terms of Use of the relevant social media platform/site, as well as copyright, privacy, defamation, contempt of court, discrimination, harassment and other applicable laws, and other Defence policies and guidelines.
- For example state that members must not:
  - post material that is offensive, obscene, defamatory, threatening, harassing, bullying, discriminatory, hateful, racist, sexist, infringes copyright, constitutes a contempt of court, breaches a Court suppression order, or is otherwise unlawful;
  - imply that you are authorised to speak as a representative
of Defence or the government, nor give the impression that the views you express are those of the department or the government;

- use their Defence email address or any Defence or government logos or insignia;
- use the identity or likeness of another member or contractor of Defence;
- use or disclose any confidential information or personal information of others obtained in your capacity as Defence member; or
- make any comment or post any material that might otherwise cause damage to the reputation of Defence or bring it into disrepute.

Set out what is reasonable/unreasonable Private Use and give examples.
Refer to privacy, confidentiality and information security in accordance with extant Defence policies and guidelines, including equity and diversity.
Address copyright and defamation issues.
Include a reference to all related Defence policies and guidelines.

CLOSING OBSERVATIONS

It can be seen from the topics discussed in this overview that the existing coalition of Australian laws and regulations have a broad application in social media, and are likely in some way to influence and restrict social media engagement for Professional Use and Private Use.

Defence and particularly its members need to understand that laws do apply to social media and members should be educated in their application and trained in what is appropriate social media conduct during both Professional Use and Private Use. Common misconceptions and attitudes towards social media use will need to be carefully identified and adjusted. It is likely that this will involve a review of extant Defence policies and guidelines coupled with the implementation of appropriate Engagement Principles and particular Social Media Policies reinforced by appropriate social media awareness training to engender a culture of obligation to Defence and personal responsibility within members. As indicated above, Defence will need to carefully examine and accommodate the impact of social media upon equity and diversity and its auditing, recordkeeping and disclosure obligations. Such an approach will reduce the legal and reputational risks that Defence will face in social media engagement.

Particularly during social media engagement for Professional Use, the very nature of social media – its collaboration, sharing and conversations – make it all the more important that truth and trust become guiding principles for communications upon and engagement within social media. Interaction with individuals and organisations including the personal
information that is collected and its use should always be permission based. Trust is the
currency of social media.

Compliance with the laws and adherence to applicable approaches and risk treatment
strategies will not only prevent breaches of the law and adverse publicity, but will assist
in establishing and maintaining an appropriate reputation that pervades the social media
space.

Stephen von Muenster LLB (Hons) LLM (Media, Communication & IT Law) Principal
VON MuenSTER Solicitors & Attorneys
19 July 2011