

Social Media legal issues – Part I

by Nick O'Connell - n.oconnell@tamimi.com -

February 2013

Some of us are employers, many of us are employees, and all of us are customers. Some of us are fans, pundits, critics and activists.

Depending on the role that we are fulfilling at the time, our use of Social Media can have different effects and repercussions. In this article, Part 1 of two-part series, we look at some general risks associated with the use of Social Media. Some of these are of broad relevance to all users of Social Media. Some are of particular relevance in a corporate environment, including use of Social Media on behalf of a company and use and misuse of Social Media by employees inside and outside company time.

In next month's Law Update, Gordon Barr, a Senior Associate in our Employment team, will outline some of the employment-related issues arising in respect of Social Media. The increasing accessibility of consumer electronics and the internet has meant that Social Media is becoming as common place as emails. According to the Arab Media Outlook report prepared by Deloitte in 2012, 86% of internet users in the Middle East use Social Media to access news, information advice, and 70% of users voice their opinions on Social Media sites.

Businesses are increasingly using Social Media as a business tool for internal communications, marketing and public relations. The rapid proliferation of Social Media in a corporate environment brings with it a variety of issues. News stories about Social Media blunders abound. These range from reports about Social Media misconduct by employees, errors in the way in which companies try to engage with their customers via Social Media, mismanagement of employees' use of Social Media, and a range of other problematic scenarios.

Broadly speaking, the key legal issues arising out of use of Social Media relate to offensive content and privacy and confidentiality.

OFFENSIVE CONTENT

The UAE Penal Code prohibits:

- making, through any means of publicity, a false accusation which dishonours or discredits a man in the estimate of the public, without imputing any specific incident to him; and
- charging, through any means of publicity, another person with an incident susceptible of making him subject to punishment or exposing him to public hatred or contempt.

The publication of such statements is considered to be an aggravating factor. The Cyber Crimes Law 2012, which replaced the Cyber Crimes Law 2006, contains a provision that basically mirrors this provision, confirming that defamatory statements published via Social Media are no less subject to sanction.

The Publications and Publishing Law 1980 is also relevant. Coming into force well before the rise of Social Media, it is no surprise that much of the language of the law is focussed on printing presses and newspaper distribution. Despite this, the language relating to materials, the publication of which is prohibited, is broader – and likely to extend to publication in the context of Social Media.

Examples of prohibited publications include:

- Any work instigating against Islam or the values of society, the system of ruling, or that harms the interest of the state; news that harms the national economy or currency; and opinions that violate public order or that circulate subversive ideas; and
- News, pictures, comments about an individual's private life meant to disgrace such individual, or any secret that may cause harm to the reputation of someone, his property, or his commercial name.

The Cyber Crimes Law also identifies a range of content, the on-line publication of which is prohibited. This includes content that blackmails or threatens a person, content that offends religious sanctities and encourages sins, content that insults others or makes them the subject of contempt, and content that criticizes the State or that calls for donations or demonstrations without a licence.

There are a number of examples in the UAE of instances that appear to fall within prohibitions set out in one or more of these laws.

- In February 2012 the Dubai Police chief pursued a defamation case against a 42-year-old Emirati, alleging the man had defamed him on Twitter with unfounded accusations of corruption and injustice.
- In May 2012, a man who posted images insulting Islam on Facebook was prosecuted after members of the public complained about the posts.
- In June 2012, a gymnasium caused controversy with its Social Media based advertising campaign, which included an image of an obese woman making offensive gestures at a fast food restaurant.

With regard to the latter example, we are not aware of any prosecution arising. Despite this, a local newspaper reported that the so called 'Middle Finger Campaign', which offered a week of free training to tackle the "obesity epidemic" in Dubai, caused outrage on Social Media websites. Noting anecdotally that this type of gesture often forms the basis for a prosecution in the UAE in the context of altercations between drivers, there is scope to conclude that the use of such a photograph may breach the prohibition in the Publications and Publishing Law on advertisements that include expressions or pictures that are inconsistent with public conduct.

The point with all these examples is essentially that the fact that the abusive or defamatory conduct has occurred on Social Media does not make the conduct any less offensive or defamatory – or any less vulnerable to prosecution under UAE law.

PRIVACY AND CONFIDENTIALITY

The Penal Code provides a punishment of confinement and fine shall be inflicted on any person who attacks the sanctity of individuals' private or family life by publishing, through any means of publicity, news, pictures or comments pertaining to the secrets of people's private or familial lives even if the same is true. The Cyber Crimes Law contains a provision that mirrors this Penal Code provision, confirming that infringing privacy by way of Social Media is no less subject to sanction.

In the UAE, there have been a number of cases involving the disclosure of secret information via Social Media. Articles telling of jilted lovers circulating compromising photographs via Social Media seem to be a regular feature in local newspapers.

In a commercial context, the example of a bank using Facebook to approach a UAE-based customer regarding outstanding loans is an example of what not to do. A local newspaper reported that the customer learned of the bank's approach when his daughter emailed him to ask why the bank had posted details of his outstanding loans on his Facebook wall, threatening to lodge a case against him for non-payment. While the newspaper's discussion was focussed on the threatening conduct of the bank's debt collection agency, our view is that there is a high possibility that

communicating with a customer, via a non-private Social Media forum, about something as sensitive as bad debts, runs a high risk of breaching the Penal Code prohibition on the disclosure of secrets.

Besides the issue of privacy outlined above, the use of Social Media in a corporate environment raises a number of other confidentiality-related issues. From an operational perspective, an employee's use of Social Media – either for work or in a personal capacity – could result in the disclosure of information that would be best kept confidential to the company.

USER GENERATED CONTENT

Many companies have adopted Social Media as a way of engaging with customers, allowing people to post comments directly onto corporate websites or Social Media sites. A simple example in a Social Media context would be comments made by customers on the Facebook page of a company. While allowing such User Generated Content may be an effective way of engaging with customers, it is not without risk.

In the UAE, there is some likelihood that User Generated Content that was offensive or breached privacy could attract liability both for the individual posting it and for the company that failed to act promptly in taking it down. For this reason, we recommend that any company that wishes to engage with customers via Social Media in this manner moderate User Generated Content – or, at least, act promptly the moment offending User Generated Content comes to the company's attention. Our view in this regard is supported by a new provision in the Cyber Crimes Law, which – broadly speaking – provides for the site operator's liability for offending content. Provisions of the Publications and Publishing Law also support this view.

USE OF THIRD PARTY SOCIAL MEDIA SERVICE PROVIDERS

The use of third party service providers for the management of Social Media content is another area of risk. Many of the points identified earlier will be applicable, including making sure that offending content is not posted – or not permitted to remain.

A key consideration when it comes to engaging a Social Media consultant is to appreciate that the industry is at a very early stage of development, so there will be varying expectations and varying degrees of professionalism. In this context, we recommend ensuring that arrangements with service providers are clearly set out in a suitable services agreement, specifying the scope of work, the service level expectations, and – ideally – some mechanism for addressing non-compliance with service levels.

Having said that, it is important to appreciate the limitations of service level credit type mechanisms when working with Social Media. If the end result of a Social Media 'fail' is that your reputation is damaged, then service level credits may be of little consolation.

Al Tamimi & Company's Technology, Media & Telecommunications team regularly advises on Social Media related issues. For any queries regarding this article, or Social Media issues in general, please contact Nick O'Connell – n.oconnell@tamimi.com