Social Media and Insurance Liability

J C Gibson[1]
4 September 2014

Introduction

One of the hot topics in insurance law at the moment is that, as new technologies such as social media emerge, so do new insurable risks[2]. Social media use is growing exponentially; currently, nearly 70% of Australians are using social media[3], both for personal contact and in business, for everything from purchase of goods, to advertising, exchanging information with professional colleagues, and keeping in touch generally with the business world and clients[4].

However, many lawyers, executives and insurers are still coming to terms with these new methods of doing business. While some companies are making maximum use of social media[5], others have no social media business practices or policies at all, let alone insurance for social media risks. In fact, only 36% of small businesses and

[1] Judge, District Court of New South Wales. Many thanks to Crystal Lawton (Clyde & Co) and Tim Griffiths (Ebsworths), who read a first draft of this paper and provided very valuable insight and advice about the topics covered.
[2] See, for example, Patricia Anne Tom, "Social Media creates new insurable risks, opportunities", *Insurance Journal,* January 22, 2010; Kendall Kelly-Haydon, "Social Media Users R U Insurable?" 96 *Texas Bar Journal* January 2011; A Herbst, "Social Networks: an insurable risk for local government", NLC-RISC Conference, May 2011; the entire issue of *Cyber Liability Journal* for June 2012, http://corner.advisen.com/pdf_files/CLJ_Q2_2012.pdf.
[3] *Sensis Yellow Social Media Report* , May 2014, http://about.sensis.com.au/IgnitionSuite/uploads/docs/Yellow-Social-Media-Report-2014.pdf . Facebook continues to dominate; 95% of users have an account.
[4] 30% of consumer users used social media or Internet advertising to compare prices or research items for purchase, according to *Sensis Yellow*. Of those surveyed who reported that their last purchase was made as a result, around half of the purchases made were made online.
[5] There are many early articles from insurance lawyers, particularly in the personal injury sphere, and bar associations, such as Evan E Knowles, "It isn't your Facebook Space Any More", (2009 – 2010) Kansas L Rev 1279; D Kittay, "Brave New World? Bars explore Facebook, Twitter and LinkedIn", (2009 – 2010) 34 B Leader 8.

48% of medium businesses even have a social media presence.[6] This is not due to backwardness on the part of Australians, who are at the forefront of social media use[7]. The sheer rapidity of change has caught many by surprise; for example, the World Bank's 2014 edition of its annual "Doing Business" report fails to refer to social media at all, and refer to the Internet only as a method for lodging tax returns electronically[8].

Yet the potential for business losses arising from use (or misuse) of social media is enormous. There are few policies available, and there are no "social media police"[9]; the solution in countries such as China[10] has been to ban Western social media entirely. As a result, social media sites are the ultimate in free enterprise: anyone can post damaging material, anonymously, that is instantaneously available everywhere, without the possibility of recall: "God forgives and forgets, but the Internet never does"[11]. Whether it is the possibility of office computers accidentally interfacing[12], loss of confidential information from an indiscreet employee Tweet, or a Facebook attack on a corporation going viral[13], many corporations lack not only business policies and strategies, but also insurance policies to cover the loss.

Many insurance companies are still deciding how to frame social media policies[14]. However, there is a more fundamental problem: businesses cannot insure their

---

[6] *Sensis, supra.* Similarly, DLA Piper's 2011 report ("Knowing your tweet from your trend") found that only 25% of companies had a stand-alone social media policy, and that 43% had one connected to IT or HR policies. For an interesting analysis of how many insurance companies use social media, see NAIC, "The Use of Social Media in Insurance", 2012, http://www.naic.org/store/free/USM-OP.pdf . They are "avid" users, according to this report (p. 3).

[7] See the monthly statistics at http://www.socialmedianews.com.au/social-media-statistics-australia-may-2014/ .

[8] See the World Bank "Doing Business" Report, 2014, http://www.doingbusiness.org/~/media/GIAWB/Doing%20Business/Documents/Annual-reports/English/DB14-Full-Report.pdf .

[9] Robert Shullich, "Risk Assessment of Social Media", 5 December 2011, http://www.sans.org/reading-room/whitepapers/privacy/risk-assessment-social-media-33940 .

[10] "China tightens grip on social media", Josh Chin, *Wall Street Journal*, September 9, 2013 http://online.wsj.com/news/articles/SB10001424127887324549004579065113098846226; http://bigstory.ap.org/article/china-courts-lift-veils-keep-courtroom-closed ; http://www.tealeafnation.com/2012/08/lawyers-decry-draft-rules-that-would-kick-social-media-out-of-chinese-court-rooms/. For the Mother Jones map of which countries ban social media, see http://www.motherjones.com/politics/2014/03/turkey-facebook-youtube-twitter-blocked .

[11] Viviane Reding, Vice-President of the European Commission, European Data Protection and Privacy Conference, 30 November 2010, http://europa.eu/rapid/press-release_SPEECH-10-700_en.htm .

[12] These problems can range from hackers accessing the office computer through Facebook posts from holidaying employees, to flaws in programs permitting vulnerable persons such as children access to unauthorised material, to the largely unexplored problem of cybersecurity flaws when devices connect (for example, remote-access devices): see Gregory J Millman, "Cyber Cavalry Rides to the Rescue of the Internet of Things", *Wall Street Journal,* May 5, 2014, http://blogs.wsj.com/riskandcompliance/2014/05/05/cyber-cavalry-rides-to-the-rescue-of-internet-of-things/ .

[13] "You can post but you can't hide: *Madden v Seafolly Pty Ltd* and the brave new world of corporate social media", Cate Nagy and Emily Rich (King & Wood Mallesons) (2014) 17 (4) INTLB 78.

[14] There were no underwriters in the US writing social media contracts as at June 2012, according to Graeme Newman, director for CFC Underwriting Limited (June 2012 Advisen's Spotlight editor: http://corner.advisen.com/pdf_files/CLJ_Q2_2012.pdf). As to their content, US insurance analyst Bradley S Shear suggested: "If and when the insurance industry develops specific product, my best guess is that we can look to how insurers treated online content for the last 15 years. Social media

social media policies if they don't have one, or know what their social media policies should cover.

The problem is partly the newness of social media (Facebook was set up in 2004 and Twitter in 2006) and partly the speed with which it has come to dominate our lives. The fuzzy borders between private and work use of networking sites such as LinkedIn, the potential for international publication, and the low barriers to entry to the social media workplace create a highly fluid marketplace for information exchange. There are many pitfalls for the uninformed and the unwary.

The burden of advising about these pitfalls will lie upon the corporation's in house and/or external legal advisors. How well-informed are in house counsel to advise their clients? The King & Wood Mallesons *KWM Compass Report* (30 August 2013)[15] surveyed in house counsel house dealt on social media issues and found:

- Almost one in five Survey Respondents indicated their legal team lacks a practical understanding of how social media works signalling that in-house teams need to come to grips with the new ways that their organisation and its stakeholders communicate.

- In-house teams are coming to grips with a new world and are adjusting to changes in the way that organisations and their stakeholders talk to each other.

- Legal compliance still seems largely tied to the creation and revision of internal social media policies.

- As regulators attempt to catch up with the pace of social media, lawyers are faced with new compliance issues. Almost half of the ASX-listed companies surveyed may need to revisit practice in light of ASX Guidance Note 8 by monitoring investor blogs and similar media.

Insurers, lawyers and business enterprises are all having to take the time to get up to speed on the impact social media is having on their activities. What are some of the most common areas for social media to lead to liability risks? How can businesses and individuals protect themselves from financial loss from use (or misuse) of social media?

This paper is only a short outline of some of the problems, so I shall start with looking at two of the most common problems: damage to business reputation and employee use/misuse of social media.

A. Damage to business reputation

---

insurance products are likely to mirror those from the era (1994-95) when law firms first started hosting websites." (Bradley S Shear: http://virtualmarketingofficer.com/2012/05/15/risky-business-is-a-social-media-policy-enough-do-law-firms-need-social-media-insurance/)

[15] http://reports.kwm.com/themes/social-media/

Many of the risks causing damage to business reputation may not be insurable risks in the first place, or (in the case of defamation) may be disproportionately expensive. Damages have been awarded in Australia for defamatory tweets (for example, in *Mickel v Farley* [2013] NSWDC 295, the plaintiff had only 69 followers, but $85,000 general damages and $20,000 aggravated damages were awarded). In practical terms, proactive steps to prevent misuse of social media may be of more assistance.

However, reputation-based damages claims are changing, with the shift being from defamation to privacy protection. Media law blogs such as *Inforrm* are reporting that the number of defamation actions in the United Kingdom are, following changes to defamation legislation, decreasing, and that the number of privacy and breach of confidentiality claims are growing and taking their place[16]. This is unlikely to happen in Australia. Despite the apparent interest the High Court showed in the subject in *Australian Broadcasting Corp v Lenah Game Meats* (2001) 208 CLR 199[17], there has, as yet, been no formal judicial development at appellate level of such a tort.

Business confidentiality is, however, another matter, and one where social media risks are high. Potential problems could include:

1. Breach of confidential information that may include a breach of privacy rights of the employer or a customer or client (as opposed to as-yet nonexistent tort of privacy). This may be social media related (for example, the photographs of patients under anaesthetic with funny face paint, released on Facebook) or it may be disclosure of sensitive information of the "hooray, the boss has been sacked today" type.

2. Liability for penalties or damages for the business corporation arising from employees' misconduct: *ACCC v Allergy Pathway Pty Ltd (No 2)* [2011) FCA 74.

3. Liability for breach of codes of ethics (Advertising Standards Bureau, Case report 0271/12, Advertiser: Fosters Australia, Asia & Pacific);

4. Copyright infringement. This is a massive topic, so I shall only briefly note that problems include copyright in photos posted in social media and copyright for the post.[18]

Case study: *Madden v Seafolly Pty Ltd* [2012] 297 ALR 337; [2014] FCAFC 30

Ms Madden thought that Seafolly, a business rival, had copied her designs. She used her personal and business Facebook pages (as well as sending emails to media outlets) to accuse Seafolly of a "rip-off" of designs from her own swimwear

[16] See Michael Cameron, "The fall of libel and the rise of privacy", published in both the *Gazette of Law and Journalism* and *Inforrm*: http://inforrm.wordpress.com/2011/03/01/the-fall-of-libel-and-the-rise-of-privacy-michael-cameron/ . The historical view has been that the development of such a tort was best left to the Bench: Mr Justice Eady in "Strasbourg and sexual shenanigans: a search for clarity", March 11, 2010, available at http://www/indexoncensorship.org/tag/mr-justice-eady.

[17] Despite the interesting throwaway line at (2007) 232 ALR 232 at [113], the High Court has never come close to canvassing the issue of creation of a tort of privacy.

[18] For recent cases, see Samantha King, "Recent legal developments involving Twitter: practical implications for lawyers", (2014) Internet Law Bulletin Volume 17 No 1 (January-February 2014).

collection, demonstrating this with a series of photographs of her own designs juxtaposed with Seafolly's swimwear. Ms Madden dropped some big hints that the fashion buyer who photographed her collection worked for Seafolly has passed these photos on.

Seafolly was furious. Its staff replied with a volley of press releases, and sued Ms Madden for misleading or deceptive conduct, injurious falsehood and breach of copyright (for the use of their swimwear photos). Ms Madden, unlike Seafolly, was not a prescribed corporation (s 9(2) *Defamation Act* 2005 (NSW)), so she cross-claimed for defamation and made a claim of her own for misleading or deceptive conduct against Seafolly.

After a torrid trial, only the Seafolly claim for misleading and deceptive conduct survived. The damages awarded ($25,000) were token, because there was no actual financial loss.

The appeal was even worse. The Full Court not only put this token sum down to $20,000 (at [117]), but held that Ms Madden's s 52 claim should have been allowed, and remitted the matter for assessment of damages (at [168]).

What was gained from this litigation? Perhaps not much for the parties, but some valuable insights for everyone else.

Lessons from *Madden v Seafolly Pty Ltd*

Tracey J's opening words, in the judgment at first instance, were to warn of the traps for companies attempting to bring defamation-style remedies when their commercial reputations were called into question and they were unable, if they were prescribed companies, to sue for defamation ([2012] FCA 1346 at [1]).

Seafolly did not suffer any pecuniary loss; the best the company did was to be awarded a token $25,000 in damages (reduced on appeal), an injunction, and declarations with an "educative effect" (at [196] – [107]) and a s 52 cross-claim from Ms Madden.

In their amusing case summary of the *Seafolly* decisions[19], Cate Nagy and Emily Rich point out:

> "While it may make sense to outsource social media to your interns (they understand all these newfangled platforms!), ensure that your legal team is sufficiently close to the relevant stakeholders and across potential legal risks. This should also be supported by a structured social media crisis management plan in order to quickly escalate and address any legal issues as they arise."

The case does raise interesting legal issues: how to distinguish between personal criticism and a statement made in trade or commerce; the difference between fact and opinion in an angry social media post; the difference between promotional and commercial speech; breach of copyright on social media; and so on.

[19] "You can post but you can't hide: *Madden v Seafolly Pty Ltd* and the brave new world of corporate social media", *loc. cit.*

These may be interesting topics for judges and academics, but they are also expensive for the clients. *Seafolly* is a good example of the need for lawyers, no matter how angry their clients are, to weigh up the potential legal risks, have a sound social media (and press release) policy for dealing with disputes, and to understand the potential risks of litigation over comments in social media, whether insurance is involved or not.

B. Employer/employee problems

When any relatively senior position is advertised and résumés sent in, most companies expect the interviewing staff to have checked out the candidates on social media. It is standard practice. Although the candidate with boring (or nil) social media entries may be looked at almost as suspiciously as the candidate with the rave party drunken snapshots, the logical consequence of this kind of inquiry – namely that this individual will continue to post on social media after being hired – seems to be given scant corporate consideration.

Problems with employees often fall into insurable risks. Commonly recurring cases that have come before the courts include:

1. Attempts to regulate social media use/unfair dismissal arising from social media use[20]. For example, many public service departments limit social media/banking use of work computers to one hour a month (usually in 6 or 10 minute lots), as was the case for the United Fire-fighters Union. This restriction is supposedly to aid productivity but, in an age where any mobile phone or iPad has access to social media, it merely means the worker is accessing social media on other equipment. What is more, the employees' private posts (rejoicing in his boss's retirement today, or calling his supervisor a "bacon hater" – see below) will be posted unknown to the employer – unknown until the court case, that is.

2. Posting bullying or discriminatory material. Unless proper procedures for social media use are in place, dismissing an employee for this kind of conduct may be held to be harsh, unjust or unreasonable (*Glen Stutsel v Linfox Australia Pty Ltd* [2011] FWA 8444; [2012] FWAFB 7097; [2013] FCAFC 157), which means not only the discriminated against employee but also the discriminator bring claims against their employer. Additionally, although the material may have been posted on the employee's private social media site - Mr Stutsel posted a series of discriminatory statements (including the "bacon hater" insult) on his own private Facebook page – the employer is stuck with the end result.

3. Employees posting material critical of the employer. The most recent case is *Banerji v Bowles* [2013] FCCA 1052, where a public affairs officer who tweeted criticisms of her department (under the pseudonym @LaLegale) was

[20] For example, the United Firefighters Union of Australia brought a complaint to the Fair Work Commission about a 60-minute restriction upon social media use: (2013) FWC 4758. The case settled at mediation.

in breach of the Australian Public Service (APS) Code of Conduct and the Department of Immigration and Australian citizenship's social media guidelines. Termination of her employment was upheld.

Case study: *Stutsel v Linfox Australia Pty Ltd* [2013] FCAFC 157

Mr Stutsel, a truck driver, was sacked after he made derogatory racist and sexist remarks posted on his own private Facebook account. There were no privacy settings, so his meandering and offensive comments about his supervisors could be read not only by his 170 "friends" (largely workmates), but by anyone. These views included expressing inordinate pleasure at Osama Bin Laden's death, calling one of his supervisors (a Moslem) a "bacon hater" and comments about a female supervisor tactfully referred to only as "disgusting".

The employer did not have a policy about social media use by employees. Mr Stutsel's legal team said that their client's remarks were intended as a joke, and for "letting off steam". Additionally, Mr Stutsel gave evidence (although contradictory in nature) that he thought the privacy settings prevented persons other than his Facebook friends seeing what he had written. He sought remedies under s 394 *Fair Work Act* 2009 (Cth).

The Commissioner held the dismissal was unfair, as the conduct did not amount to serious misconduct, and ordered reinstatement. This finding was upheld by the Fair Work Australia Full Bench. The employer was granted leave to appeal to the Full Court of the Federal Court.

The Full Court dismissed the appeal. They discounted the apparently inconsistent evidence of Mr Stutsel about what he thought were the privacy settings for his Facebook account. He had not been told what he should or should not post on his private account, or told about privacy settings. There was no social media policy or education at all provided by his employer.

What this shows is the importance of companies having a social media policy that includes education of employees about matters such as privacy settings for their personal accounts. If the employer had had a social media policy, and provided education and advice about statements on social media, the result in this case might have been different.

As it was, Mr Stutsel's obvious ignorance about how Facebook settings worked was in his favour. The Full Court quoted the findings of the Fair Work Australia Full Bench judgment at [34]:

> "[34] It is apparent from the recital of these matters that the findings of the Commissioner as to the Applicant's understanding about the use of Facebook were an important part of the circumstances taken into account in concluding that the dismissal was unfair. It is also apparent that, with increased use and understanding about Facebook in the community and the adoption by more employers of social networking policies, some of these factors may be given less weight in future cases. The claim of ignorance on the part of an older worker, who has enthusiastically embraced the new social networking media

> but without fully understanding the implications of its use, might be viewed differently in the future. However in the present case the Commissioner accepted the Applicant's evidence as to his limited understanding about Facebook communications. We have not been persuaded, having regard to the evidence and submissions presented, that such a finding was not reasonably open."

Other issues raised before the Full Court included "differential treatment" claims that other employees had been able to get away with similar conduct. This did not help the employer, and neither did the complaint that the Commissioner had been led down the wrong track on the issue of alleged "freedom of speech" (at [86] – [89]).

There are two points to note here. First, most companies already have policies about sexual harassment, bullying, racial discrimination and similar unacceptable work practices. Many of these activities spill over into social media. Companies without a clear social media policy which covers employees' private use of social media in which activities of this kind occur will find not only the sacked employee brings proceedings, but also the discriminated person. Mr Stutsel was criticising his supervisors, after all, which is not that far from being critical of his employer. However, the employer did not have a social media policy to rely upon. This is one of the reasons why the employer failed in Mr Stutsel's case, whereas the employer succeeded in *Banerjee v Bowles.*

Secondly, Mr Stutsel's employer was lucky that none of these remarks went viral. Let us not forget this famous example of an unfortunate employee tweet (sent by Justine Sacco, a US Internet PR executive with 200 followers, just before she boarded a plane):

"Going to Africa. Hope I don't get AIDS. Just kidding! I'm white!"

By the time Ms Sacco arrived at her destination, #HasJustineLandedYet was not only viral but front-page news – a problem for her employer, as well as herself. Ms Sacco has deleted her Twitter account[21], but the Internet, as has already been noted, never forgets – and that would apply to her employer as well.

C. Good news and bad news

I have only had time to outline briefly two examples to demonstrate the impact of social media on our legal system, from an insurance law point of view. Social media and the Internet will, however, completely change many areas of the law, ranging from ability of existing law to cope with new crimes and torts (such as breaches of privacy rights) to the very existence of common law (can a precedent-based legal system keep up the pace?). Do the risks outweigh the opportunities?

Social media law is the current hot topic. *Lexis Nexis* will publish a considered volume of essays on the topic in September; the Internet Law Bulletin is full of

[21] …and lost her job: http://www.independent.co.uk/news/people/news/pr-executive-justine-sacco-apologises-after-losing-job-over-racist-aids-joke-provoked-hasjustinelandedyet-twitter-storm-9020809.html . For the latest on Justine Sacco, see #hasjustinelandedyet on Twitter.

articles; everyone is worried that social media will impact on how they do business. However, social media is just another form of publication, albeit a more permanent and international form. To borrow the famous analogy of Sài Wēng[22] and his alternatively lucky or unlucky horse (the Chinese equivalent of the silver lining to the black cloud), social media, as a source of information, contains just as much good news as bad news, for insurers and lawyers alike.

Here are two examples.

- **The impact of social media on criminal law**

  Business is increasingly concerned about misuse of office equipment for criminal offences, although many of them currently fall outside the scope of their insurance policies. Entirely new crimes such as cyberstalking, cyberbullying, creepshots, trolling, virtual mobbing, revenge porn and reflectoporn are now coming before the court and the majority of them are committed by using social media. Businesses and their lawyers are understandably anxious about exposure to new forms of crime, much of which will be uninsurable.

  I cannot answer for the insurability of such crimes, but the good news, for companies terrified about the enactment of a raft of unexpected new criminal offences, is that criminal activity committed on social media should still be able to be prosecuted within the parameters of current criminal law provisions. The House of Lords Select Committee on Communications' 1st Report of Session (29 July 2014)[23] has examined the adequacy of criminal law in dealing with these new criminal provisions. This Report has concluded that, despite being almost entirely enacted before the invention of social media, criminal law provisions and penalties were "generally appropriate for the prosecution of offences committed"[24] and that no gaps in legislation, or inadequacy of penalty, had been demonstrated in any prosecutions to date.

  On a humorous note, the report concluded:

  "Just to show that nothing is ever really new, a man was convicted by magistrates in 1913 under section 4(1)(c) of the Post Office (Protection) Act 1884 for sending "grossly offensive" postcards to officials in Leeds in which he described an Alderman as an "insurance swindler"."[25]

  That will be reassuring to everyone in the audience.

---

[22] "塞翁失馬，焉知非福", (sài wēng shī mǎ , yān zhī fēi fú), *Huainanzi*《淮南子•人间训》d. 122. B.C.: 18:6a-b. When Sai Weng found a horse, everyone said he was lucky; when his son was injured riding it, everyone said he was unlucky, when his son escaped military service as a result, everyone said he was lucky, but Sai Weng was always wise enough not to jump to conclusions. This chéngyǔ (saying) is very popular in Chinese business negotiations.

[23] http://www.publications.parliament.uk/pa/ld201415/ldselect/ldcomuni/37/37.pdf . The committee did conclude, however, that "revenge porn" (posting naked or offensive photographs of ex-lovers) required further consideration.

[24] *Ibid*., p. 6.

[25] *Ibid*, p. 26.

- **Dealing with dishonest or inflated insurance claims**

  One of the first areas where the benefit of social media for insurers was rapidly appreciated was in the defence of personal injury claims, where a plaintiff's assertion of ongoing disabilities was difficult to challenge without surveillance evidence. The problem is that court rules, such as Uniform Civil Procedure Rules r 31.10, require disclosure of such material unless there are grounds for the court to dispense with such evidence. Surveillance evidence is costly, ambiguous (or simply unclear), and frequently explained away by the plaintiff as being the plaintiff's condition "on a good day". Social media evidence, however, is not only cheaply obtained, but more compelling.

  Is social media evidence admissible, and must it, like surveillance evidence, be disclosed beforehand?

  In *Royer v Blackman* [2014] WADC the plaintiff, a saxophonist, claimed neck and back problems. Pages from Facebook were tendered which showed her enjoying herself skiing, travelling overseas and teaching students (at [43] – [45]). As a result of adverse findings about her credit, the plaintiff was only awarded a small sum for out of pocket expenses.

  There is no reference in this judgment to objections to the tender of the plaintiff's Facebook entries, or to requirements for their early disclosure. They have been successfully tendered in the United States, but usually in circumstances where they are disclosed beforehand, primarily due to discovery obligations[26].

  What would be the position in New South Wales? Under UCPR r 31.10 notice for the tender of such material is necessary unless it falls within the exceptions noted. Is it the case that the plaintiff's authorship of such documents would warrant the exclusions being applied, in the interests of justice? If not, does r 31.10 need modifying so that the opponent does not have to disclose it if it is the party's self-created document? There is no easy answer to this.

  Additionally, the news about discoverability of social media is not all good. Companies which do not produce social media on discovery in commercial or other proceedings where discovery has been ordered may suffer the fate of Charmyne Palavi: *Palavi v Queensland Newspapers Ltd* (2012) 82 NSWLR 523. Emails, social media (*Ange v Fairfax Media Publications Pty Ltd* [2010] NSWSC 200) and even the actual mobile phones containing the social media messages (*Palavi, supra*) may be discoverable. In fact, failure to discover them cost Ms Palavi her court proceedings[27].

[26] Evan E Knowles, "It isn't your Facebook Space Any More", *loc cit, passim;*

[27] See also *Georgiou v Spencer Holdings Pty Ltd (No 4)* [2011] FCA 1222. Ms Palavi remains, however, the only example of such an extreme course. Other litigants who destroyed material did not have their claims struck out, and the discovery judgment relevant to the phone hacking claims (*Various Claimants v News Group News Limited & Glen Mulcaire* [2010] EWHC 2692 did not require

As was the case with the Chinese horse (lucky one moment, unlucky the next), whether the risks outweigh the opportunities depends upon how things look at the relevant time. Social media is, however, a commercial inevitability which businesses and lawyers have to understand, not only in its present form, but in relation to its impact on our methods of communication both now and in the future.

Conclusions: How should corporations (and insurers) deal with social media risks?

Working backwards from the kinds of problems commonly seen in insurance litigation, here is a checklist I have compiled, based on my reading of discussions in some of the insurance and Internet law journals as to the steps insurers and lawyers are looking at:

1. It will be up to the business to work out what kind of corporate social media is most effective for the individual needs of the business and its employees/agents. Given the wider scope of social media publications, greater care should be taken than might be the case with non-electronic publication; a newsletter to clients reporting a law firm's successful litigation may result in defamation claims if wider circulation brings it into less receptive hands: *Martin v Luxford* [2014] FCA 342. If Twitter is to be used, exercise caution in relation to advertising campaigns, or the company may end up on Mashable's Annual Social Media Disaster List[28].

2. Have a policy about when social media use is corporate and when it is personal. Employee use of corporate social media resources can create problems when the employee leaves. For example, LinkedIn connections can be valuable. In *Whitmar Publications v Gamage* [2013] EWHC 1881, an employee was ordered to hand over log-in details to LinkedIn accounts after leaving to set up a rival business and using LinkedIn both before and after departure to notify the former employer's customers of the new business. The law on ownership of post-employment social media contacts is uncertain.[29]

3. Educate their staff about social media generally, especially their in house lawyers, given the high level of in house legal teams (20%) unfamiliar with how social media works[30]. In house lawyers should have their own Twitter accounts – after all, it is a great way to follow the Supreme Court of NSW's latest judgment (although no substitute for Jade Barnet).

---

any of the phones or equipment used for hacking to be discovered. In fact, discovery of these phones never appears to have been sought.

[28] See, for example, the 2012 list: http://mashable.com/2012/11/25/social-media-business-disasters-2012/ (my favourite is the grovelling apology KitchenAid had to give President Obama after a personal tweet was mistakenly published on the company's Twitter account).

[29] See Jessica Fisher, "Networking or notworking?" (2014) Internet Law Bulletin Volume 17 No 4, April 2014.

[30] http://reports.kwm.com/themes/social-media/ .

4. Develop a social media policy reflecting the needs not only of the company and its employees, but also contractors, customers and family members (to discourage photos of dad's Christmas party champagne disaster).

5. Loss of confidential client data can also lead to breach of privacy issues. From 12 March 2014, new privacy laws now apply, inter alia, to advertising on social media. The Office of the Australian Information Commissioner (OAIC) has prepared draft guidelines to explain how the OAIC will interpret and apply the Australian Privacy Principles (APPs) introduced under the *Privacy Amendment (Enhancing Privacy Protection) Act* 2012 (Cth), which in turn amended the *Privacy Act* 1988 (Cth). APP 7 states that organisations may not use or disclose personal information for direct marketing purposes in the form of online advertising, which would include social media, such as "promoted" sites on Twitter or Facebook.

6. Keep up to date with information about risks arising from potential loss of information through social media as well as from computer use generally (including interconnectivity issues, such as remote access by employees). There are a number of government initiatives concerning cyber security, the most recent being the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cyber Security.[31] Cyber attacks can lead not only to business disruption but also reputation damage and loss of customers. In November 2013, ASIC chairman Greg Medcraft put cyber crime costs at about $110 billion annually, with attacks on Australian companies at about $2 million.[32]

7. Consider unexpected risk areas, such as potential for legal action if the social media is accessible in countries other than Australia (generally the case for social media), such as EU data protection rules.

8. Finally, having taken these steps, companies should review existing insurance policies to determine whether those policies reflect the social media policy and areas of risk.

[31] Released February 14, 2014: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf .
[32] Reported at http://www.financialobserver.com.au/articles/measures-against-cybercrime-crucial-asic