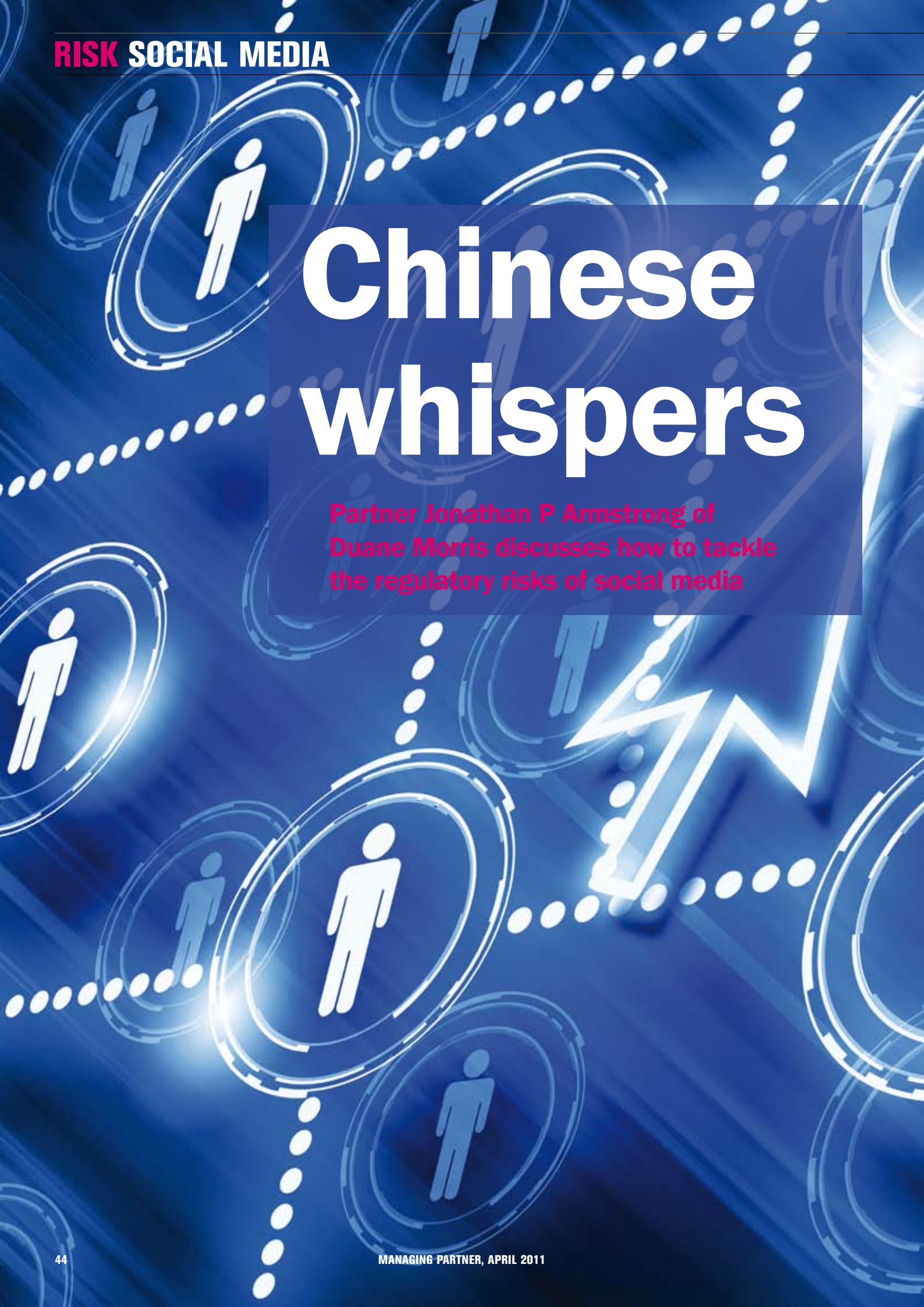

Chinese whispers

Partner Jonathan P Armstrong of Duane Morris discusses how to tackle the regulatory risks of social media

Government bodies around the world are getting increasingly involved in regulating how social media is used.

On 1 March 2011, the UK Code of Non-Broadcast Advertising (known as the CAP Code) was extended to the online environment. The CAP Code rules apply to any firm's marketing communications on its own website. The rules had already covered paid internet ads but now extend to non-paid marketing space, including on social media applications like Facebook and Twitter. This means that any comment by a firm must not mislead, harm or offend.

In addition, the Office of Fair Trading (OFT) in the UK has the power to regulate social media by virtue of the Consumer Protection from Unfair Trading Regulations 2008 (CPRs). In the limited space available in Twitter messages or Facebook or LinkedIn status updates, it is relatively easy to fall foul.

As an example, OFT used the CPRs to take enforcement action against PR agency Handpicked Media in December 2010. Handpicked operated a network of bloggers and niche websites across a variety of sectors.

OFT was concerned that some of those engaged by Handpicked were publishing online content which promoted the activities of Handpicked's clients without sufficient disclosures in place to make it clearly identifiable to consumers that the promotions were being paid for.

Handpicked agreed to sign undertakings prohibiting any future promotion that does not clearly identify that the promotion has been paid for "in a manner prominently displayed with the editorial content such that it would be unavoidable to the average consumer".

OFT also announced in December that it is joining forces with 11 other EU member states to improve the investigation and enforcement of online regulation.

Rumours have been circulating that a number of celebrities are also being investigated for tweeting repeatedly about skincare products, jewellery and cars, for which they have received value.

Good lawyers sometimes promote their clients' goods and services. It will be important to make sure that improper promotions are not made. In some circumstances, this might necessitate the client's permission before publishing the blog, in order to properly disclose the relationship.

Regulating blogging

Parallel rules exist in the United States. In December 2009, the Federal Trade Commission (FTC) brought in specific guidance to regulate blogging. The rules require bloggers to disclose any payments (or free products) they receive in exchange for reviewing products online.

Violating the rules could cost up to US$11,000 for each violation. Bloggers or advertisers also could face injunctions and could be ordered to reimburse consumers for financial losses stemming from inappropriate reviews.

"The training process should include educating staff about the risks of social media and what is required to reduce those risks"

The FTC followed its announcement by starting its first public investigation against Ann Taylor LOFT, a clothing chain.

In January 2010, LOFT launched a preview of its summer collection and announced the event to bloggers. It told bloggers that anyone who attended would receive a special gift, and those who posted coverage from the event would be entered into a prize draw to win up to US$500 to spend at LOFT.

Press coverage after the event was apparently overwhelmingly positive. After complaints were made that there was a potential breach of the FTC's blogging rules, LOFT's president defended the event. He explained that there was no incentive to write a positive review and bloggers were free to write whatever they wanted about the event.

Some of the bloggers disclosed the gift card promotion, others did not.

The FTC learned of the event and started an investigation into the potential violation of its guidelines. The FTC took no action against LOFT as it understood it to be the company's first event, that only a small number of bloggers had posted content and an even smaller number had failed to disclose the promotion.

The FTC heard evidence that LOFT had put a sign at the event telling bloggers that they should disclose the gifts if they posted comments about the event. In addition, it heard of LOFT's remedial action after the event, which included a written policy explaining that bloggers would have to disclose any gifts given in their blogs. The FTC had also been given to understand that LOFT would monitor bloggers' compliance with the policy.

Data protection legislation

In Europe, data protection legislation mandates that a business keeps personal data secure. In other countries, including the US, specific legislation exists to the same effect. In the olden days, stealing a firm's secrets required time and resources but now, for the technically astute, it can be the work of an instant.

Take the example of solicitor Andrew Crossley of ACS:Law. Crossley was already unpopular with the online community after he took action against alleged filesharers. His firm collected details of those accused of unlawfully sharing pornography, music and video games. Groups which opposed ACS:Law's actions retaliated with a denial of service attack to take ACS:Law's website down.

Internet news site The Register phoned Crossley on his mobile and reported him as giving a possibly ill-advised off-the-cuff reaction: "It was only down for a few hours. I have far more concern over the fact of my train turning up 10 minutes late or having to queue for a coffee than them wasting my time with this sort of rubbish".

The groups redoubled their attack. Records were seized from ACS:Law's servers, which are likely to increase the pressure Crossley is under from the

Solicitors Regulation Authority and to lead to an investigation by the information commissioner.

ACS:Law ceased trading in February. The SRA has said that it has received over 400 official complaints from members of the public. Crossley closed his firm saying that he had received death threats.

Ongoing litigation

The dangers of commenting on ongoing litigation were highlighted in September 2009 with the settlement of the Patent Troll Tracker blog case. The Patent Troll Tracker blog was set up by Cisco's director of intellectual property, Rick Frenkel.

"The best time to plan for action is before an incident happens, not when one takes place"

Frenkel's blog was anonymous, but in the blog he commented on IP litigators who were representing the other party in litigation where Cisco was a defendant. Other Cisco employees circulated links to the blog without revealing that the author was a Cisco employee.

After Frenkel revealed his identity, the two lawyers concerned sued him and Cisco for defamation. The case was settled, but Cisco decided to very publicly acknowledge the risks and its responsibility for Frenkel's actions.

Mitigating risk

The first step in any response strategy has to be education. This should include educating:

- those at the top of the organisation about the risks of social media and the need to take them seriously;
- the information security team about the full range of legal risks; and
- employees and partners at all levels about the need for them to act responsibly.

For most firms, the training process should include educating staff about the risks of social media and what is required to reduce those risks (see box: Creating a social media policy).

CREATING A SOCIAL MEDIA POLICY

No two policies should be the same. A firm which has an open culture, few secrets and operates heavily in social media will have a different risk profile than a more old-school firm with a financial services client base and which shares sensitive information on its clients. As their risk profiles are different, so should their policies be. If your firm is international, your policy should be international too.

There is no magic language. Consultation is generally a good idea. Given the demographical issues, make sure the policy is not just drawn up with the input of senior managers. More junior workers are often those using social media the most, so listen to their views. A policy will need to be reasonable if it is to be observable and enforceable.

Be aware of the possible adverse publicity of a too-restrictive policy. You should expect your policy to find its way into the public domain and be prepared to justify it in the court of public opinion. Make sure that there are sound business reasons behind what you propose to do.

In addition to staff, think through who else should be bound by your policy. You might want sub-contractors or anyone who has access to your firm's information or your clients to be bound by your policy. This could include, for example, counsel or expert witnesses in long-running litigation.

State explicitly what you plan to do. If you intend to monitor the policy by, for example, monitoring an employee's internet and email traffic, there is often a legal obligation to make this explicit.

Include general wording to protect your reputation. Ensure that employees understand that this is not limited to materials which mention the firm by name. Employees need to exercise caution when disclosing anything which could be associated with the firm or its clients, for example, photographs on your premises or with other identifying marks such as a firm's umbrella or sports kit.

They also need to know that some social media applications will track IP addresses, so 'anonymous' comments can be traced.

Alert employees to the particular risks of blogging late at night, especially on weekends, as they might be tired and emotional.

Keep the policy flexible enough to allow it to be changed – the best policies develop after an incident or new risk comes to light. Be aware that the best policies in this area for most businesses permit as well as prohibit. You will need to have a dialogue and see if there are good business reasons for the use of any application before you ban it.

Responding to an incident

Even in the best run organisations, incidents will still happen. Plans need to be put in place to enable a quick response. The best time to plan for action is before an incident happens, not when one takes place.

When an incident occurs, you must plan to act. It is often the case that incidents start small – for example an isolated and relatively uncontroversial blog posting. Often employees do this to test the water – if there is no response, worse can follow.

Responding to incidents will need a multi-disciplinary team, possibly involving people in HR, marketing, IT and compliance. To be effective, the plan will also need to be rehearsed. Plan rehearsals are an increasing feature of data regulators' guidance and are a wise precaution – in the heat of the storm there is often little time to assign roles and responsibilities. mp

JPARMSTRONG@DUANEMORRIS.COM