Linklaters

Social media and the law: A handbook for UK companies

January 2014

Contents

Introduction

Social media has grown explosively in the past few years, fuelled by a combination of greater internet access, smart mobile devices and advert-funded business models.

Social media is different from traditional forms of media and social interaction in a number of important ways:

> **Spontaneity** – Users can instantaneously Tweet, post or send comments from almost anywhere without any safeguards to vet that communication.

> **Reach** – At the same time, social media provides an instant global audience, potentially reaching thousands if not millions of recipients, depending on the popularity and following of the user.

> **Permanence** – Social media messages can be saved or reposted to create a record that is difficult to withdraw or amend.

This leads to a greater risk of saying something stupid, or at least a greater risk that the stupid things you once shared later at night with a few friends, forgotten the next day, are now read by thousands, never to be lost. This has not prevented the wide-spread adoption of social media, though users have been adapting to these challenges both through greater awareness and new technologies, such as Snapchat which sends self-deleting messages.

Social media is also becoming an important tool from a corporate perspective and a number of organisations are now using it to inform, educate and influence the wider public.

Equally, companies are having to grapple with increased use of social media by employees and the difficulties this raises given the blurring of the distinctions between personal and professional lives.

These developments raise important new legal issues, some of which legislators are wrestling with, such as the "right to be forgotten", and some of which are being left to the Courts. We consider the risks and rewards of using social media in this handbook and the practical implications for employers, particularly in light of the influence of the fundamental rights of privacy and freedom of information.

We hope you find this handbook useful.

Marly Didizian
Partner, TMT Practice

Richard Cumbley
Partner, TMT Practice

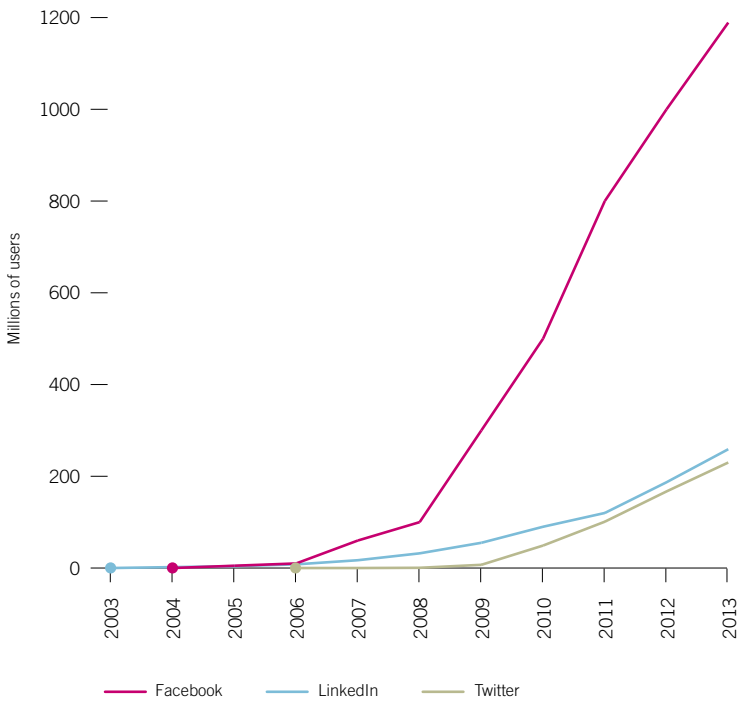
1. The rise and rise of social media

The growth and importance of social media is readily apparent. In the last nine years, Facebook has grown from start-up to a global phenomenon with 1.2 billion users[1], nearly a fifth of the world population.

Other social networks have also had explosive growth. Twitter was only launched in 2006 but has grown to now include 230 million users who create around 500 million Tweets every day[2]. LinkedIn now also has more than 259 million users in over 200 countries and territories[3].

The influence of social media is underlined not only by the number of users, but also by the role it plays in their lives. In the US, Facebook accounts for over 10% of all time spent online[4]. More importantly, a recent study by Pew Research indicated that 30% of Americans use Facebook as a way of obtaining news[5]. Participation in social media is therefore an increasingly important way to inform, educate and influence those users.

Growth of social networks in the last ten years



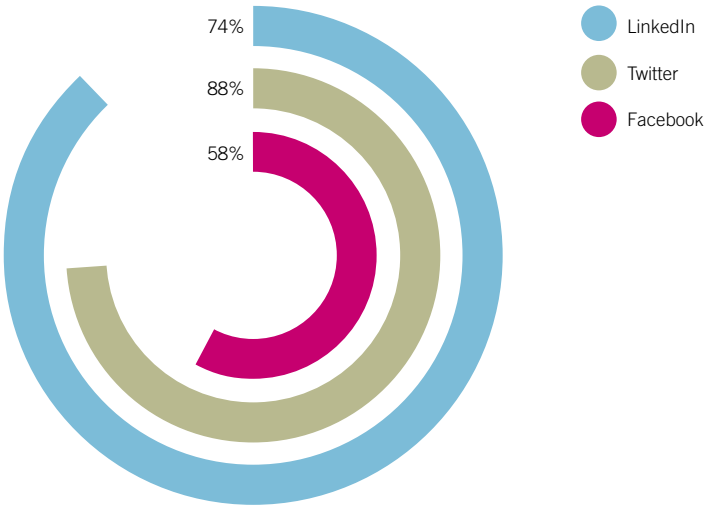
Richard Cumbley
Partner, TMT Practice

"Social media has become phenomenally popular. It is reshaping industries and lives. It also raises new legal issues. Some activities become actionable when conducted via social media; some assets that have been historically protected, cease to be when created via social media."

This growth amongst users is mirrored by increased use by corporates. We recently conducted an online review to determine which FTSE 100 Companies have an official page or account on Facebook, Twitter or LinkedIn[6]. The results are set out opposite and indicate that most are active in this space.

The review was deliberately targeted at pages or accounts that either are, or appear to be, officially sanctioned by those companies. As it is relatively straightforward to set up a page or account, it seems likely that the extent to which these pages are in fact formally approved and supervised by these companies will vary in practice.

FTSE 100 companies with an offical social media page



[1] 1.189 billion Monthly Active Users, Facebook Q3 2013 Earnings Release.

[2] Final Twitter Prospectus, November 2013.

[3] LinkedIn Q32013 Earnings Release.

[4] US Digital Future in Focus 2013, ComScore February 2013.

[5] The Role of News on Facebook, Pew Research Journalism Project, October 2013. Of the 30% that consume news from Facebook, 78% simply consume news as an incidental part of their Facebook usage whereas 22% specifically see Facebook as useful way to get news.

[6] Review conducted in November 2013. The review was aimed solely at identifying pages or accounts in the name of the FTSE 100 Company itself and not pages or accounts operated by its subsidiaries or in the name of its brands.

2. Corporate use

Key points

> Social media is an increasingly important means of communicating and connecting with customers. Even if you do not directly engage with social media, you should consider monitoring activity on social media that relates to your organisation.

> Not all interaction on social media will be positive. You should be prepared for active and sometimes critical debate with social media users. Attempting to suppress it may backfire. Garner support from the social media community and argue your case on the merits.

> Care must be taken over social media postings. They could lead to serious embarrassment or even be actionable. Social media is subject to the same rules as information published by other means.

> If you have paid or otherwise arranged for others to post on your behalf, you should make this clear. Do not try to pass these posts off as genuine user-generated content.

> In some cases, you may become liable for user-generated content. You should consider monitoring user-generated content or, at the very least, putting an effective notice and take down procedure in place.

> If your organisation is listed, you should ensure you comply with relevant disclosure rules for inside information. In most cases, information should be disclosed via a regulatory information service and not just via social media.

> Those using social media to communicate on behalf of your organisation should be given very clear guidelines and training.

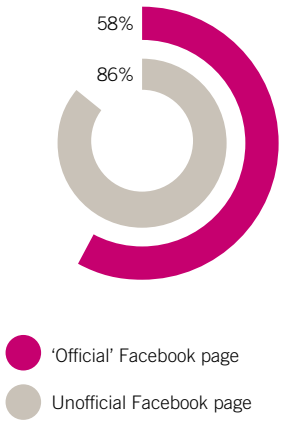
There are both benefits and risks to businesses participating in social media. We consider both below.

2.1 Benefits

Inevitability

For most companies, some engagement with social media is unavoidable. Regardless of whether or not a company has an "official" social media page or account, it is very likely that it is the subject of a number of unofficial pages, its employees are interacting with social media and it is the subject of lively discussion online.

For example, our review of the FTSE 100 Companies' use of social media also looked at unofficial Facebook pages, i.e. pages that do not appear to have been authorised by that company[7]. These have typically been set up by employees, ex-employees, customers or pressure groups and are not always complimentary.



This indicates that around a quarter of the FTSE 100 appear to be unwilling participants on Facebook. By opting out of social media they may put themselves at a disadvantage. They are under discussion but cannot put their side of the story across or influence the debate.

Engagement

A key reason to become involved in social media is engagement. Social media provides a means for that organisation to directly interact with its customers and to obtain feedback from them. Handled properly, this can help to build a brand and create a buzz and awareness to help generate new marketing leads and attract new customers.

Perhaps the most beneficial outcomes from this interaction is social validation – users who start to "organically" advocate your organisation or its aims and ideals. This "electronic word of mouth" can be a very powerful marketing and influencing tool.

Engagement with users might include commenting on topical issues and the organisation using social media to put their side of the story across. One example comes from energy companies who have used their social media presence to comment on rising fuel costs and discuss the link between costs and wholesale energy prices, as well as providing information on related topics such as energy efficiency.

It also allows brands to develop a distinctive tone of voice and style. For example, Tesco recently entered the telecoms market as a mobile virtual network operator. It is pretty challenging to develop distinctiveness in this market but Tesco Mobile has made use of Twitter to try and do so. One user Tweeted

"*Immediate turn off if a girl's mobile network is tesco mobile*" to which Tesco Mobile promptly responded "Are you really in a position to be turning girls away?" before sending him a male grooming kit as a present. It also engaged in an extended debate with the Jaffa Cake Twitter account accusing it of being a biscuit[8].

Social media is also particularly important for corporate communications, not least because Twitter is now heavily used by journalists. Corporate Twitter accounts can allow a company to monitor breaking news, identify PR problems in real time and try to influence the way that news is presented.

Listening
One exercise most organisations will want to do, even if they do not directly engage with social media, is to listen to social media conversations to find out what users are saying about them.

There are a number of off-the-shelf and cloud-based tools that can be used for this purpose. They not only allow monitoring of individual conversations but also monitoring on a macro-level, for example through sentiment analysis. These tools automatically analyse the 500 million tweets sent every day and report on how often a topic is mentioned and whether it is mentioned in a positive or negative context.

The Twitter trends for 2013 in the UK[9] reveal that the top five UK news stories were the death of Iain Banks, the storm in October, the NHS, the death of Seamus Heaney and the prosecution of the actor who plays Ken Barlow in Coronation Street.

The entertainment industry is a heavy user of this technology, both in the television industry where Twitter sentiment has assumed equal importance to traditional rating information and in the film industry where it is a valuable means to predict future blockbusters.

Advertising
Finally, social media is an increasingly important tool for advertising. Some social media platforms are able to build detailed profiles about their users including their sex, age, location, marital status and connections. This allows advertising to be targeted precisely.

2.2 Risks

Too much engagement
One risk of social media is too much engagement. Some users are more than happy to share their views in very uncompromising terms. A thick skin is vital. For example, energy companies using social media accounts to comment on rising fuel costs have received direct and frank feedback from their customers. The same is true in financial services and many other industry sectors.

Attempting to suppress critical comment may backfire. Instead you need to engage with customers and argue your case on the merits. This means your social media team need to be properly resourced. They will also need to update your social media presence to ensure it remains fresh and manages to respond to user comments. This engagement with users is a vital part of any social media strategy, either to build a distinctive brand (as is the case with Tesco Mobile) or to mollify users' concerns (as is the case with energy companies).

Stupid posts
Another problem is embarrassing or ill-judged posts. There are numerous topical examples. For example, Ian Katz, the editor of Newsnight, sent a Tweet in September referring to *"boring snoring rachel reeves"* (Shadow Chief Secretary to the Treasury) following her appearance on the programme. He had intended to send a private message to a friend. The circumstances in which the Tweet was sent are not clear but there have certainly been other cases in which late night rants on Twitter have caused significant embarrassment[10].

[7] Review conducted in November 2013. An "unofficial" Facebook page is one that was about an FTSE 100 Company but, because of its nature or content, did not appear to be officially sanctioned by the company.

[8] Jaffa Cakes are in fact cakes and are therefore zero-rated for VAT purposes, see http://www.hmrc.gov.uk/manuals/vfoodmanual/vfood6260.htm.

[9] See 2013: The Year on Twitter.

[10] Notable examples of Twitter rants by celebrities include Alec Baldwin who quit Twitter after an online row with a Daily Mail reporter in June 2013 and Kanye West who issued a series of Twitter insults to late night host, Jimmy Kimmel, in September 2013.

The informality of Twitter, coupled with its reach and permanence, make this a real risk. You need to train employees to think twice before posting and have a process for dealing with embarrassing posts, normally deleting them and making a suitable apology.

Actionable posts

Some postings may not just be stupid but also actionable. One example is the notorious Tweet by Sally Bercow: "*Why is Lord McAlpine trending? *innocent face**". That Tweet was made when there was significant speculation about the identity of a senior unnamed politician who had been engaged in child abuse.

The Tweet was false and found to be seriously defamatory[11]. It highlights a number of risks with social media. Firstly, the repetition rule applies such that those repeating a defamatory allegation made by someone else are treated as if they had made it themselves. This is relevant when retweeting or reposting content. Secondly, while the courts provide some leeway for the casual nature of social media and the fact that those who participate "*expect a certain amount of repartee or give and take*"[12], that protection only extends so far.

Civil and criminal liability for social media postings can also arise in a number of other ways. Paul Chambers was initially convicted for sending a "menacing" message[13] after Tweeting: "*Crap! Robin Hood airport is closed. You've got a week and a bit to get your shit together, otherwise I'm blowing the airport sky high!!*". He was fined £385 and ordered to pay £600 costs. However, this prosecution was overturned on appeal[14].

Prosecutions were also brought against two Facebook and Twitter users for contempt of court after they posted photographs of Jon Venables and Robert Thompson (the killers of Jamie Bulger)[15]. Both were sentenced to nine months' imprisonment, suspended for 15 months.

Finally, liability could also arise for negligence. It will be relatively rare for a duty of care to arise in respect of a social media posting, not least because most claims will relate to pure economic loss, but such a duty is not inconceivable. It would certainly seem wise to use appropriate disclaimers, though they will be more difficult to include in many social media postings.

Unfair trading

As with more traditional formats, sales and marketing use of social media must be decent, honest and truthful.

Most of the specific social media issues arise out of social validation, i.e. users who "organically" advocate that organisation or its aims and ideals. As this is such a powerful tool there is a real risk of it being misused.

For example, in January 2012 the well known media personality, Katie Price, sent a series of out-of-character Tweets – such as "*Large scale quantitative easing in 2012 could distort liquidity of govt. bond market. #justsayin*" – before a final Tweet "*You're not you when you're hungry @snickersUk #hungry #spon*". The Advertising Standards Authority rejected a complaint about this campaign. The #spon hashtag made it clear that this was advertising and not an unprompted personal recommendation. Whilst the earlier Tweets did not have this hashtag, they were sufficiently closely associated for consumers to understand that they were part of a wider marketing communication[16].

Similarly, "astro-turfing", the generation of artificial grass root support, is very problematic. The Consumer Protection from Unfair Trading Regulations 2008 prohibits the use of editorial content in the media to promote a product if the trader has paid for the promotion and has not clearly identified that this is the case[17]. In conventional media, most readers will be familiar with seeing "Advertorial" features reflecting this requirement. The risk of abuse is fairly clear, for example, by improperly influencing consumers' purchasing behaviour by posting fake reviews for products.

The Office of Fair Trading has already taken enforcement action against an operator of a commercial blogging network, Handpicked Media, requiring them to clearly identify when promotional comments have been paid for. This included publication on website blogs and microblogs, such as Twitter[18].

It is also important to comply with any sales and promotions rules for the particular platform being used for that promotion. In the case of Facebook, this includes prohibitions of promotions appearing on personal timelines, a complete release for Facebook by each entrant and an acknowledgement that it is not associated with Facebook[19]. Failure to comply can result in ejection from the platform.

---

[11] *McAlpine v Bercow* [2013] EWHC 1342.

[12] *Smith v ADVFN* [2008] 1797. In that case Eady J suggested that social media postings are more akin to slander than libel. It is more difficult to obtain damages for the former action.

[13] See 127(1)(a) and (3) of the Communications Act 2003.

[14] *Chambers v DPP* [2012] EWHC 2157.

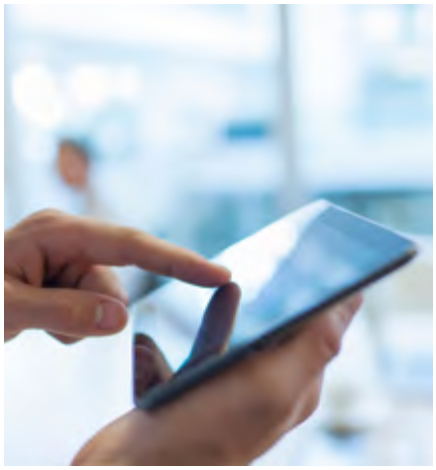
[15] *HM Attorney General v Harkins* [2013] EWHC 1455. See also the *Guidelines on prosecuting cases involving communications sent by social media* issued by the Crown Prosecution Service.

[16] ASA Adjudication on Mars Chocolate UK Ltd, 7 March 2012.

[17] Schedule 1, para 11. Note that this is also likely to be a misleading omission under regulation 3(4)(b).

[18] *Investigation into inadequate disclosures in respect of commercial blogging activity*, Case Reference: CRE-E-25932.

[19] Facebook Pages Terms, August 27, 2013.



Vanessa Havard-Williams
Partner,
Environment Practice

"NGOs and other campaigning groups use social media with great intelligence to launch campaigns, mobilise support and disseminate advocacy pieces. Corporates have been slower to appreciate the importance of tracking activism through social media and of developing contacts and supporters on social platforms. Investing ahead of time in understanding the dynamics of social media campaigns, and building it into your stakeholder engagement and crisis planning is valuable when you need to communicate your point of view quickly and effectively, in a crisis or following NGO criticism."

User-generated content

Liability can arise not only from content posted by an organisation itself, but that posted by its users. The sales and promotion rules will automatically include any content "adopted" by that organisation. What adoption means will vary depending on the circumstances, but a drinks company adopted the content of a third party website by linking to it[20] and Amazon adopted a book description by including it as part of a product description[21]. However, organisations will not generally adopt organic-user generated reviews by simply allowing them on their sites[22].

An organisation might also become a data controller in respect of its personal data posted on its social media page[23] or may become a publisher of that material for defamation purposes, particularly once the organisation has been notified that the material is defamatory[24]. Organisations should therefore consider if they wish to actively moderate content on their social media pages and, at the very least, should ensure that they have an effective notice and take down process to benefit from the various defences this affords[25].

Regulatory disclosures and inside information

Entities listed in the UK should be mindful of the requirements of the Disclosure and Transparency Rules. Amongst other things, these require an organisation to disclose inside information via a Regulatory Information Service prior to, or simultaneously with, disclosure on its internet site[26]. This means inside information must be released in a controlled way. The good news about a new deal or improved financial performance should not be inadvertently posted or Tweeted before an appropriate regulatory announcement is made.

If the good news is to be Tweeted or posted, the content of that post or Tweet should be reviewed carefully by the legal or compliance team to ensure that it fairly and properly discloses the underlying information. Typically, this means the relevant Tweet or post should include a link to the full regulatory disclosure.

The Disclosure and Transparency Rules also require the disclosure of inside information in response to press speculation or market rumour in some circumstances[27]. Listed companies working on sensitive transactions should monitor social media for speculation or rumour as part of their obligation under the Listing Rules to have adequate systems in place to promptly identify disclosable information[28]. Whilst isolated postings or Tweets might not trigger a disclosure, they may provide an early warning that rumour or speculation is building up and a disclosure may need to be made shortly.

[20] ASA Adjudication on Hi Spirits Ltd, 17 July 2013.

[21] The ASA rejected Amazon's argument that it had not adopted the description and instead just automatically sourced from a third party website. See ASA Adjudication on Amazon EU Sarl, 10 July 2013.

[22] ASA Adjudication on N5 Ltd, 4 September 2013.

[23] *Social networking and online forums – when does the DPA apply?*, Information Commissioner, May 2013.

[24] *Tamiz v Google Inc* [2013] EWCA Civ 68.

[25] Such as the hosting defence under Regulation 19 of the Electronic Commerce (EC Directive) Regulations 2002, the defence under section 1 of the Defamation Act 1996 and the proposed defence for operators of websites under section 5 of the Defamation Act 2013.

[26] DRT 2.3.

[27] DTR 2.7.

[28] LR 7.2.

3. Employees and social media

Key points

- There is no specific regulation of social media, so existing employment and data protection laws apply.
- Tell applicants if you intend to use social media for any pre-employment vetting. That use should be proportionate, avoid decision-making on discriminatory grounds and steps should be taken to confirm the accuracy of any findings.
- There is considerable freedom for employers to dictate what constitutes acceptable use by employees through the use of an internal social media policy. It may be difficult to enforce appropriate use without such a policy.
- Social media policies should clearly state that they continue to apply to the use of social media in the employee's personal capacity, using their own computer equipment and outside of normal working hours.
- Tell employees if you intend to actively monitor their social media postings or usage. This should be included in your social media policy.
- The social media policy should be consistent with other policies and disciplinary rules.
- If any disciplinary action is taken in response to social media usage, it should follow approved procedures and be proportionate, recognising the individual's freedom of expression.

The growth of social media has inevitably raised a number of employment law issues. There is no specific regulation on the use of social media by employees and employers in the UK, so the existing employment law and data protection principles apply.

These give employers considerable freedom to regulate the use and content of social media by employees through the use of internal policies. Absent clear policies on what levels and types of usage by the employee are acceptable, an employer may face serious difficulties in enforcing appropriate usage by employees.

The employment issues fall broadly into two camps: social media vetting as part of the recruitment process and disciplinary action for inappropriate use of social media.

3.1 Recruitment

Market practice and employee expectations
It is increasingly common for employers to review candidates' social media footprints as part of the recruitment process. An ACAS Research Paper in 2013[29] found that 61% of employers did so and 15% planned to start doing so in the future.

There are a number of reasons why an employer would want to do this, especially for public-facing roles. A good example of this is the appointment of the 17-year old Paris Brown as Britain's first youth police and crime commissioner. After her appointment she was found to have sent a number of offensive, and potentially racist, Tweets. The subsequent media firestorm resulted in both her resignation and criticism of the Kent Police and Crime Commissioner for failing to adequately vet her appointment.

However, applicants are not necessarily aware these checks are carried out and do not appear to agree with them. A 2011 ACAS Research Paper[30] found that 58% of applicants surveyed would be angry, very angry or outraged if an employer refused them a job on the basis of social media research.

Risks of social media vetting
Social media vetting also raises a range of risks for employers. Perhaps the key risk is that the employer obtains information about protected characteristics[31] and an applicant subsequently claims the decision not to hire them was based on those characteristics and thus discriminatory.

[29] See *The use of social media in the recruitment process*.

[30] See *Workplaces and Social Networking The Implications for Employment Relations*.

[31] Namely information on age, being or becoming a transsexual person, being married or in a civil partnership, being pregnant or having a child, disability, race including colour, nationality, ethnic or national origin, religion, belief or lack of religion/belief, sex and sexual orientation.

Nicola Rabson
Partner, Employment & Incentives Practice

> In the absence of specific legal regulation on the use of social media by employees and employers the importance of internal policies cannot be overstated.

Privacy is also important. The Information Commissioner Employment Practices Code contains a range of general requirements for vetting of employees that are equally relevant to social media vetting. These include:

- informing applicants that social media vetting will take place. As much as anything this may encourage the applicant to clean up their social media accounts or alter their privacy settings to ensure their information is not publicly available;
- giving candidates the opportunity to comment on the accuracy of any findings. This is to mitigate the risk that some information about that individual may be inaccurate or may be about someone else with the same name;
- the search should be proportionate. Clearly, those in a prominent, public-facing role will demand more scrutiny than those in less important roles; and
- the search should be undertaken as late in the process as possible. For example, only at the point that the applicant is short-listed, or even conditionally appointed.

Whilst not included in the Code, the Information Commissioner has also warned against gaining access to an applicant's social media profile by deception (for example, trying to be become a "friend" using a fake identity) or asking applicants for their username and password to conduct a full review of their social media account. There is anecdotal evidence of this sort of forced access in the US, and several States have legislated against it. Whilst there is no specific legislation in the UK, it is bad practice and is likely to be a breach of the Data Protection Act 1998.

3.2 Inappropriate use by employees

Reputation
Most issues have arisen where there has been damage to reputation. A typical example is *Weeks v Everything Everywhere*[32] where Mr Weeks made several postings to his wall describing his place of work as "Dante's inferno". Everything Everywhere had a social media policy that expressly applied to postings in the employee's own time and included a requirement not to criticise Everything Everywhere. Mr Weeks was dismissed for gross misconduct, a decision subsequently upheld by the Employment Tribunal.

However, disciplinary action against employees must be in accordance with established disciplinary policies and procedures. The employer must act fairly and the response must be one which a reasonable employer could have made. One implication of this is that the employer must consider actual impact on business rather than assumed or feared impact.

This brings a number of specific social media factors into play, such as:

- the seriousness of the damage to the employer's reputation. In contrast to the Weeks case, an employee posted the following comment on Facebook after a difficult day at work: "*I think I work in a nursery and I do not mean working with plants*". Her subsequent dismissal for damaging her employer's reputation was found to be unfair. The comment was directed at her colleagues and was relatively mild. There was no evidence of any harm to the employer's reputation, not least because the client

[32] ET2503016/2012.

was not identified in the posting nor had it raised any concerns about the posting[33]; and

> whether the employee is contrite and withdraws the posting. For example, an employee set up a Facebook page "*Halfords workers against working 3 out of 4 weekends*" after a workplace reorganisation, but removed the page two days later when he found out it was in breach of his employer's social media policy. His dismissal was unfair given his prompt removal of the page and previously clear disciplinary record[34].

These cases also indicate that the exact details of how the posting is made are generally less important. For example, there is limited focus on whether it is made in or out of normal working hours or using the employer's computer system. Instead it is important to focus on whether there is a clear connection to work (for example, because of the nature of the posting or naming of the employer) and the impact on the employer in practice.

Bullying and harassment

Social media also provides a medium for online bullying and harassment. This could take a number of forms, including the posting of offensive photos or comments as well as the risk of social exclusion. This could lead to claims for claims for discrimination or constructive or unfair dismissal as employers are vicariously liable for the acts of one employee to another in the course of their employment.

Again, it is important that social media and bullying policies are updated to clearly set out what sort of behaviour is acceptable and extend their scope to cover cyber-bullying outside of the workplace. However, any subsequent action against the employee must reflect the seriousness of the alleged behaviour. For example:

> it was not reasonable to dismiss an employee who "liked" a comment on Facebook that his manager was "*as much use as a chocolate teapot*", commented that it had been the worst year at the company and she was glad her colleague had escaped. This was not serious enough to constitute bullying or harassment[35]; but

> in contrast, where an employee made vulgar comments about the sexual promiscuity of a colleague, refused to remove them and instead posted further comments, that was harassment and his dismissal was fair.[36]

Loss of productivity

Excessive usage of social media by employees can lead to a loss of productivity and overburden the employer's computer systems. So this is one area in which the fact postings are made during normal working hours, or using the employer's computer systems, is relevant.

Some employers have responded to this issue by blocking access to social media sites at work though this may be unpopular and does not prevent employees from using social media on their smartphones. Alternatively, employers might want to monitor their employee's use of social media, though that will need to comply with data protection laws as with any other employee monitoring (see below) and employees should be given clear guidance about what constitutes excessive use.

Privacy and "friends"

These issues are potentially complicated by the overlap with human rights law including the right to privacy and freedom of speech, protected in the European Union by both the European Convention of Human Rights and the Charter of Fundamental Rights of the European Union.

These rights might be relied upon by employees to claim that their social media postings are private and therefore should not be subject to their employer's disciplinary policy. Many social media accounts can be set up so that posting and other information are only available to that person's "friends" and, indeed, in many cases, the employer only becomes aware of the offending posting when the "friend" reports it to them. However, these arguments have fairly limited success. In particular:

> postings can be forwarded and copied. This is highlighted by an English case in which an employee, Mr Gosden, used his personal email account to forward a sexist and racist email to another employee's personal email account. The email contained an express encouragement "IT IS YOUR DUTY TO PASS THIS ON". Accordingly, the other employee sent it to a third employee's work email address. The employer detected the email on its system, saw that it had been initially sent by Mr Gosden and dismissed him. The dismissal was justified as the express encouragement to pass the email on meant it was not a purely personal communication[37];

[33] *Witham v Club 24*, ET1810462/2010.

[34] *Stephens v Halfords plc* ET/1700796/10.

[35] *Young v Argos Ltd* (unreported).

[36] *Teggart v TeleTech* [2012] NIIT 00704_11IT.

[37] *Gosden v Lifeline Project* ET/2802731/2009. See also *Martin v Gabriele Giambrone* [2013] NIQB 48.

- the posting may, in any event, be widely available. Some people also have a lot of "friends". In one case, a pub manager made a number of derogatory comments about her customers after they had abused her. Her argument that they were private communications only available to her "friends" was undermined by the fact that there were 646 of them[38]; and
- there are limits to an individual's right to privacy which may be overridden by other factors. For example, the European Court of Human Rights had to consider an appeal from a probation worker who was involved in the treatment of sex offenders. He was dismissed after his employer discovered pictures of him on the internet involved in bondage, domination and sadomasochism. The Court decided that even if his dismissal was a potential infringement of his privacy, it could have been justified because it conflicted with his role in working with sex offenders[39].

Equally, whilst most cases seem to arise from "friends" notifying the employer of offending content, if an employer wants to actively monitor its employees' social media postings it should respect their right to privacy and comply with data protection laws. Whilst there is no direct guidance from the Information Commissioner, this is likely to be subject to Part 3 of his Employment Practices Guide: Monitoring at work. This suggests, amongst other things, notifying employees through an appropriate policy and carrying out a privacy impact assessment.

Freedom of expression

Finally, an employee might also argue that restrictions on his use of social media infringe his right to freedom of expression. This right was considered in *Smith v Trafford House Trust* [2012] EWHC 3221. Mr Smith was disciplined for setting out his negative views on the proposal to introduce gay marriage in the UK via his Facebook account. His comments, which were clear, reasoned and unaggressive in nature, caused upset to a fellow employee who was also a "friend" on Facebook.

When the "friend" drew the employer's attention to Mr Smith's comments on gay marriage the employer took disciplinary action against him on the basis that the employer was a housing trust which included gay people among its clients. It therefore considered that his statements were inappropriate and that disciplinary action was justified as they breached its Code of Conduct that stated that employees should not "*promote their political or religious views*".

However, the policy did not expressly extend to personal communications and, in light of Mr Smith's right to freedom of expression and freedom of speech, the High Court interpreted it as only applying to work-related communications. Moreover, frank but lawful expression of private views on social media, as on any other platform may cause upset to those of opposing views, but that this was consistent with the concept of freedom of speech and was the necessary price for such a freedom. Accordingly, the action against him was unlawful.

This is one of the only social media cases to be heard in the High Court, as opposed to the Employment Tribunal, and it is possible that the right to freedom of expression and freedom of speech will become increasingly significant in future cases.

[38] *Preece v JD Wetherspoons* ET/2104806/10.

[39] *Pay v UK* [2009] IRLR 139.

4. Ownership of social media accounts

The ownership of social media accounts is an area that has attracted considerable interest. However, the analysis is often confused by conflating corporate profiles and the profiles of individual employees.

Corporate social media accounts
Ownership of corporate social media accounts is relatively straightforward. The starting point is to identify what accounts your organisation currently owns and what accounts you want to own.

Acquiring new accounts for more popular social media sites may give rise to "name-squatting" problems, similar to those that arise in relation to domain names. Whilst most social media sites have express squatting policies[40], that does not help where there is genuine conflicting use.

Certainly, if you are one of the many people to congratulate John Lewis on its recent #bareandhare Christmas adverts and you sent your Tweet to the handle @johnlewis, you might be surprised to get a response from the computer science professor, John Lewis of Blacksburg, Virginia, USA.

It's also sensible to control passwords to those accounts and ensure they are not held by one person alone. This will help to manage the risk of an employee leaving with control of that corporate account or deliberately sending unauthorised messages. For example, this could have avoided mild embarrassment at the insolvent retailer HMV after its social media planner used its Twitter account to provide real-time updates on the dismissal of its staff.

The Courts are also likely to be sympathetic to claims that a corporate account has been misused or misappropriated. For example, a company successfully obtained an injunction preventing its ex-employees from using a corporate LinkedIn group in a competing business[41].

Personal social media accounts
Employee social media accounts are more difficult to deal with. The idea that a company "owns" its employees' social media accounts is conceptually difficult, as its contents, connections and interactions are normally personal to that employee.

By way of example, the television journalist Laura Kuenssberg moved from the BBC to ITV in July 2011. Her Twitter account had around 60,000 followers and, on moving, she changed her handle from @BBCLauraK to @ITVLauraK. The BBC did not take any action over her move and in many ways it is hard to see what action they could have taken. The account could hardly have been reassigned. Laura's 60,000 followers chose to follow her not some other person nominated by the BBC. In any event, things may have worked out well for the BBC following the announcement in November 2013 that Laura will re-join as chief correspondent and presenter for Newsnight.

Quite apart from this conceptual difficulty of corporate ownership of personal social media accounts, there are also difficulties in identifying what legal rights exist in those accounts and therefore in protecting them in a meaningful way. An analysis of one professional social network (overleaf), LinkedIn, illustrates these difficulties.

Key points

> Ownership of corporate social media accounts is relatively straightforward. Ensure you know which accounts your organisation is using, who has control of those accounts and that control is not limited to one employee.

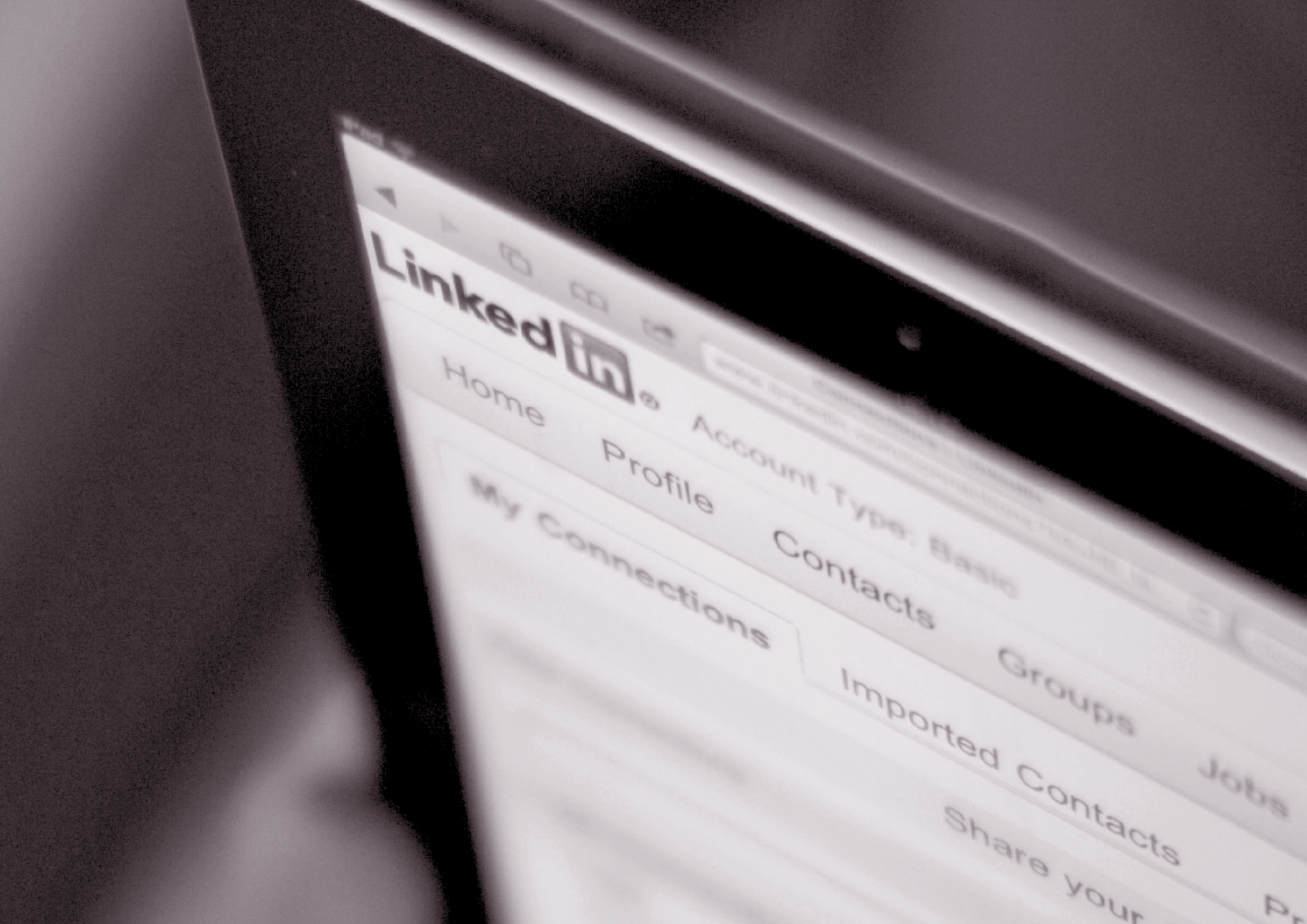
> Corporate ownership of personal social media accounts is complex, not least because they are often inherently personal to the relevant employees.

> Banning the use of social media by employees will be difficult, given most have smartphones and internet access at home. Enforcing such a ban may be not practical.

> Consider how existing provisions in employment contracts, for example restrictive covenants, will apply to social media accounts.

[40] Such as the Twitter Username squatting policy (https://support.twitter.com/articles/18370) or Facebook which has specific measures to block fake pages.

[41] Whitmar Publications Ltd v Earth Island [2013] EWHC 1881.


LinkedIn
Home
Profile
Contacts
Groups
Jobs
My Connections
Imported Contacts
Account Type: Basic

Ownership of LinkedIn Contacts

What is LinkedIn?
LinkedIn is a social networking website for use by professionals in a business context. It is run by a California company, LinkedIn Corporation. It is necessary to register to use the social network and agree to the LinkedIn User Agreement. That creates a personal contract which, amongst other things, obliges users not to provide their password to any other person nor to allow anyone else to use their account.

Personal Profiles and Groups
Each user of LinkedIn creates their own profile. This typically includes a short description of that user's educational and employment history and a short description of their current role.

The user can then make "connections" with other LinkedIn users to build up a network of contacts. Those connections may be with persons the user knows as a result of their current employment, but equally they may arise from a user's previous employment, educational history, family relations or friendships.

Connections may be made by the user, or other users may ask to make a connection. Further connections are suggested by LinkedIn based on these connections and any shared educational or employment history. Finally, it is also possible for a user to carry out a bulk upload of contacts from Outlook and certain other email systems. The average user reportedly has 150 connections.

The default settings on LinkedIn allow a user to view their connection's connections and therefore also try and connect to those persons. However, it is possible to amend the default setting so that only shared connections are displayed.

Users can also set up groups on LinkedIn. These are typically set up to manage a professional community based on common interest, experience, affiliation and goals. LinkedIn users can be invited, or can ask, to join a group. Each group will have one or more managers and it is possible to transfer management responsibility from one user to another or to have multiple managers of a group.

What rights exist in a LinkedIn Profile?
The area of most interest is normally the user's connections. However, it is not immediately obvious what proprietary rights exist in those connections[42].

For example, traditional "offline" customer lists are often protected by the *sui generis* database right. However, for those rights to arise, there must be a substantial investment in obtaining, verifying and presenting the contents of the database. Given a large number of connections may have been instigated by other users or automatically suggested by LinkedIn, it is not clear that there is such an investment. Equally, employers are only entitled to database rights created by their employees "in the course of their employment", so pre-existing connections or those that arise from a user's educational or personal relationships are unlikely to result in a proprietary right for the user's employer.

Traditional "offline" customer lists are also often protected by the laws of confidentiality, but if a LinkedIn user has not changed the default settings for their account, the list of their connections will be visible to all their connections. If the user has 150 connections (being the approximate average) this means that 150 other people have access to this information – the vast majority of which will not be subject to any duty of confidentiality or other obligation (beyond those owed to the individual user in the LinkedIn User Agreement) that could restrict their use of the information. No such duties will be owed to the employer.

When have the Courts asserted control over LinkedIn profiles?
Despite these difficulties, there have been cases in which the Courts have intervened. Confidentiality may be relevant when a user uploads a list of "offline" connections or uses an employer's proprietary database to create a list of connections for their LinkedIn account. This is likely to be a breach of confidence; see *Hay v Ions* [2008] EWHC 745.

The Court is also more likely to recognise rights in a corporate account or a LinkedIn Group set up for a corporate. The Court provided interim relief in *Whitmar Publications v Earth Island* [2013] EWHC 1881 to prevent ex-employees from continuing to use a LinkedIn Group. The Group was originally set up by those employees to promote Whitmar but was used by them after they had left to promote a competing business.

Nemone Franks
Partner, Intellectual Property Practice

"The idea that a company owns its employees' social media accounts is conceptually difficult - those accounts are often inherently personal to the employee."

What can you do in practice?
There are some steps an employer can take to assert "ownership" over, or control use of, their employees' LinkedIn accounts. Whether they are all appropriate will vary depending on the business in question. However, for all but the most connection-heavy businesses, such as recruitment consultants, the following are likely to be problematic:

> **Banning use of LinkedIn:** This could be partly achieved by blocking access to LinkedIn at work. However, given most employees have their own smartphones and home computers, this prohibition would be difficult to enforce in practice. It would also deny the employee access to this popular networking tool;

> **Requiring employees to delete their LinkedIn profile and connections at the end of their employment:** This presents a number of issues. Firstly, the employee may have used LinkedIn prior to joining the employer and a number of his connections may be personal or otherwise created outside of the course of his employment. This may mean the employee will see a request to delete this information as unfair. A compromise would be to just remove connections made during the employee's employment but it may raise difficult evidentiary issues. Secondly, the employer will be dependent on the employee deleting the profile and/or connections himself (as the LinkedIn User Agreement prevents the employee from giving his username and password to his employer) so there may be difficulties in enforcing this right. Thirdly, given the quasi-public nature of those connections, it may be relatively easy for the employee to copy those connections and then recreate them under a new profile; and

> **Requiring the employee to hand over the connections when their employment ends:** It is difficult to see how this could be done. The user is prevented from transferring their LinkedIn account to anyone else. The employer could require the employee to provide a complete list of connections with a view to another of its employees seeking to recreate those connections, but there is no assurance that all such connection requests would be accepted. Also, this is likely to breach the LinkedIn User Agreement which only allows a user to connect to another user they know.

In light of these difficulties, employers might want to explore other options such as:

> **Copy information to your organisation's internal contacts database:** Oblige employees to also add all of their contacts to your own contact database, and to keep this information up to date. This will ensure you can retain that information if the employee leaves;

> **Restrictive covenants:** Review restrictive covenants and related provisions to see if they would apply to post-termination contact with connections formed by that employee during their employment. One difficulty is that when you change details of your employer on LinkedIn, that change will be automatically notified to your connections. It is not clear if this automatic notification constitutes a solicitation and therefore is a breach of any restrictive covenants with that employee;

> **Technical changes:** Configure email servers to prevent bulk uploads of email contacts to LinkedIn. This will help to prevent a confidential and proprietary customer list becoming part of the public domain; and

> **Profile settings:** Recommend that employees change the default settings on their profiles to hide their list of connections. This may prevent others from benefitting from your employees' connections and could help with the argument that those connections are confidential.

[42] For completeness, some commentators have suggested there is a data protection argument that the connections are "owned" by an employer. In essence, if the employee "owns" the connections it must also be a data controller in respect of the underlying personal data. The employee is therefore responsible for complying with the Data Protection Act 1998, including notifying the Information Commissioner of the relevant processing if he is making use of contacts outside of his personal family and household affairs (s.36). Most personal connections probably fall into this exemption but to the extent not, failure to make such a notification is a criminal offence. As almost all employees will not have made that notification they are faced with a choice of agreeing that the connections are really "owned" by their employer or admitting they have committed a criminal offence. However, this argument breaks down as the employee may be exempt from notification under the Data Protection (Notification and Notification Fees) Regulations 2000 or alternatively could just make a new notification to cure the earlier breach.


HD VIDEO

5. Privacy issues

The use of social networks will inevitably involve the processing of personal data and thus engage privacy and data protection laws.

Is social media compatible with privacy?
New technology has challenged traditional concepts of privacy for well over a century. Samuel Warren and Louis Brandeis' seminal 1890 paper on "*The Right to Privacy*" grappled with the prospect of "*numerous mechanical devices*" and "*instantaneous photographs*" creating a world in which "*what is whispered in the closet shall be proclaimed from the house-tops*". Social media, smartphones and other wearable technology, such as Google Glass, has brought this threat to life.

In the intervening hundred years, the law has evolved to provide generalised rights to privacy or specific data protection laws or both.

New technologies are also redefining social attitudes to privacy. Many users disclose significant amounts of personal information about themselves on social media. Indeed, for many, the very purpose of social media is to provide an endless stream of information about themselves from the trivial, to the intimate to the tragic. However, and perhaps counter-intuitively, users remain very concerned about their privacy and want to keep tight control of their information[43].

Ground rules for compliance
Operating in this fluid environment with both changing technology and changing privacy expectations is challenging, not least because the legal framework in the European Union was adopted in 1995. This predates social networking as we now know it and even the widespread use of the internet.

However, the purpose of these laws is to protect an individual's privacy and put them in control of their information. With this principle in mind, you should consider the following guidelines:

> **Don't be sneaky**: Individuals have a right to know what you are doing with their information. The normal way to provide this information is through a privacy policy but these can be problematic, not because they say too little but because they say too much[44]. Think about other ways to get your message across.

> **Don't be creepy:** Make sure you are using an individual's data for a proper purpose. Data protection laws typically only permit use of personal information for certain statutory purposes, such as with consent. They also impose general requirements not to process that information in a disproportionate manner. Often this comes down to a question of the reasonable expectations of the individual, which in turn depends on what you have told them you will do with their information.

> **Put users in control**: Wherever possible, give individuals the opportunity to make informed choices about how their data will be used. Informed consent that will normally ensure use of the individual's information complies with privacy and data protection laws. This is important for marketing activities, which often specifically require user consent.

Key points

> Trust is important. Individual expectations are an important part of privacy laws so don't be sneaky or creepy.

> Be open and transparent with individuals about how you are using their information.

> Do not just rely on privacy policies. Think about other ways to get your message across.

> Wherever possible, give individuals choices about how you will use their information.

> Make information security a priority.

> Use anonymised information wherever possible.

[43] The *Information Commissioner's Annual Track 2013*, which measures the awareness of the Data Protection Act amongst the general public reveals that protecting personal information is the second most important social issue. Its survey reveals 88% of the public consider it of social importance, very slightly behind unemployment (89%) but in front of preventing crime (87%) and education (84%).

[44] For example, see The Cost of Reading Privacy Policies, Aleecia M. McDonald & Lorrie Faith Cranor, I/S: A Journal of Law and Policy for the Information Society Volume 4, Issue 3 which estimated that it would take an individual around 244 hours a year to read all of the privacy policies of the sites they visit during that year, slightly more than half the time actually spent online

[45] Article 29 Working Party *Opinion 03/2013 on purpose limitation*, Working Paper 203, April 2013

> **Think about security:** One of your key duties under data protection legislation is to keep personal information secure. Cyber attacks against organisations are increasingly common, not least because personal information is a valuable asset for criminals for use in identity fraud. This has risen up many regulators' enforcement agenda with a number of high-profile casualties. For example, Sony's PlayStation Network was hacked in 2011 leaking around 77 million customers' details. Current estimates suggest the breach has cost Sony $1.25 billion from lost business, various compensation costs and new investments.

> **Watch out for sensitive personal information:** Additional controls apply to the use of information relating to an individual's racial or ethnic origin, religious beliefs, political opinions, trade union membership, health, sex life or criminal record. The general rule is that this sort of information should only be processed with the individual's explicit consent.

Big Data

Social media generates huge volumes of information. Facebook alone generates 500 terabytes of data a day, including 2.7 billion new likes and 300 million new photos. This is fertile ground for Big Data analysis.

To the extent that this involves personal information, it will be subject to privacy and data protection legislation, a question European privacy regulators grappled with earlier this year in its Opinion on purpose limitation[45]. For the regulators the key distinction is whether the analysis is just intended to detect general trends and correlations (for example, sentiment analysis) or is intended to support measures in respect of an individual.

Unsurprisingly, the former is unlikely to be objectionable so long as there are proper safeguards in place. The regulators stress the need for "functional separation" such that the output of this analysis cannot be linked back to an individual.

In contrast, if the analysis could be used to support measures in respect of an individual, then greater care will be needed. The regulators have an antipathy for profiling, e.g. direct marketing, behavioural advertisement, data-brokering, location-based advertising or tracking-based digital market research, and suggest it would "almost always" require specific, informed and unambiguous consent. The legitimacy of other uses will depend on the circumstances but, to a large degree, will depend on whether the new Big Data analysis is compatible with the purpose of the original social media posting.

Future of data protection regulation

The European Union intends to deal with many of the challenges raised by social media through its proposed General Data Protection Regulation. A draft of the regulation was issued by the European Commission in January 2012 and is now being debated by the European Parliament and European Council, with the European Parliament voting through its draft of the regulation in October 2013.

The regulation contains a number of provisions that are relevant to social media. For example, it contains restrictions on "profiling" that are likely to require consent for many types of profiling, mirroring the position already advocated by many European regulators.

It also contains a "right to be forgotten". This provides enhanced rights to ask that personal data be deleted. It is intended to deal with the problem that the internet may reveal information about individuals that is unfair, out of date or just plain wrong.

However, this right is nuanced and is subject to a number of carve outs, such as where it would conflict with another person's freedom of expression. This will make it difficult to apply in practice. For example, while it should be easier for an individual to remove material they have posted about themselves, forcing someone else to remove information they have posted about the individual will involve a harder tussle between competing fundamental rights.

Marly Didizian
Partner, TMT Practice

> "The privacy issues are challenging because new technology and changing privacy expectations create a very fluid environment."

These issues have already surfaced in other jurisdictions, such as Germany, where two men who killed an actor in 1990 have successfully prevented further publication of their names in Germany. In contrast, they have been less successful in suppressing publication elsewhere and failed to remove their details from Wikipedia. As much as anything, this demonstrates the difficulties in implementing a "right to be forgotten" on the internet where many of the large internet companies are based in the United States and protected by the right to freedom of speech and freedom of the press in the United States Constitution.

Privacy rights

The right to privacy is often seen as a fundamental right, protected in the European Union under article 8 of the European Convention on Human Rights and article 7 of the Charter of Fundamental Rights. However, because of its wide application, it is subject to a range of derogations that allow interference where necessary in the interests of wider society.

In the UK, the law has developed to provide privacy rights against both the state and private persons through the tort of misuse of confidential information[46]. This means privacy rights are potentially applicable to almost any form of social media activity such as the posting of photographs[47], even when the underlying information is effectively commercial in nature[48].

Data protection

Data protection laws are also very relevant to social media; introduced from the 1970s onwards in response to the growing power of computers, they are now widespread with nearly 100 countries adopting such laws, often as part of an international framework[49]. They typically supplement generalised privacy rights with a set of more defined principles coupled with enhanced rights for individuals and the establishment of a regulator. The relevant legislation in the UK is the Data Protection Act 1998.

Posting information about individuals on social media can breach data protection laws. Nearly ten years ago, a Swedish church worker was fined for posting information about other church members on the internet without their consent, including the fact that one had injured her foot. Despite the trivial and commonplace nature of the disclosure the fact this was a breach of data protection laws was confirmed by the European Court of Justice[50].

[46] *Campbell v MGN* [2004] UKHL 22.

[47] *Edward RocknRoll v News Group Newspapers* [2013] EWHC 24.

[48] *OBG v Allan* [2007] UKHL 21.

[49] Such as the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data adopted in 1980 and, more recently, the APEC Privacy Framework which was issued in 2005.

[50] *Lindqvist (Approximation of laws)* [2003] EUECJ C-101/01.

UK Contacts

Marly Didizian
Partner, TMT Practice
Tel: (+44) 207 456 3258
marly.didizian@linklaters.com

Richard Cumbley
Partner, TMT Practice
Tel: (+44) 207 456 4681
richard.cumbley@linklaters.com

Nicola Rabson
Partner, Employment & Incentives Practice
Tel: (+44) 207 456 5284
nicola.rabson@linklaters.com

Vanessa Havard-Williams
Partner, Environment Practice
Tel: (+44) 207 456 4280
vanessa.havard-williams@linklaters.com

Nemone Franks
Partner, Intellectual Property Practice
Tel: (+44) 207 456 5813
nemone.franks@linklaters.com

Simon Kerr-Davies
Managing Associate, Employment & Incentives Practice
Tel: (+44) 207 456 5411
simon.kerr-davies@linklaters.com

linklaters.com

General Editors: Peter Church and Gemma Parker

6727_F/01.14