Social media — challenges in the control of information

Olivia Whitcroft, Principal of OBEP, examines the data protection compliance challenges arising from social media use, and proposes a social media 'strategy' for overcoming these challenges

In the online world, it is easy to share information but difficult to control it. We have seen an explosion in the use of social media, as individuals and organisations reap the benefits of networking, blogging and a wealth of information sources. On the other hand, they are seeking to protect their interests in how information is used by other parties. In the last year, employees have been fired over Facebook comments; Twitter users and Google have faced defamation claims; and several prominent social media providers have tackled security breaches and disputes over privacy settings and policies.

This article examines some of the challenges presented by the social media environment, focussing on data protection and related information laws.

What is meant by social media?

Social media describes online forums which enable people to share information, including blogging platforms, social networking sites and other interactive websites or applications. Whilst a lot of recent stories hitting the press have involved prominent names such as Twitter, Facebook, LinkedIn and Google, social media is not just about the big players. Organisations frequently have websites which allow people to post comments on articles or issues, intranets allowing staff to share ideas, or networking sites for members and other interested parties.

Notwithstanding the word 'social', use of such media has, of course, been rapidly expanding beyond pure social use. There is widespread adoption by businesses, charities, public sector and societies to market their activities, and share information and opinions. The blurring of the distinction between use of social media for personal reasons and use for professional, business or other organisational purposes has made it trickier to identify which laws apply, how they apply and who is responsible for unlawful content or use. If someone blogs about me without my permission, do I blame the account holder, their employer or the social media provider? Do I have a right to complain at all?

Application of data protection law

EU data protection law applies when there is processing of personal data relating to living individuals. Social media services involve substantial processing of the personal data of account holders and their friends and acquaintances, including biographical and contact information, opinions, stories, photos and videos. However, the law does not apply to the processing of personal data by an individual for 'a purely personal or household activity' (implemented into UK data protection law as data processed for purposes of 'personal, family or household affairs'); this is known as the 'domestic purposes' exemption. The distinction between 'domestic' and other use has become unclear, which in turn provides uncertainty on when data protection laws will apply.

In May 2013, the Information Commissioner's Office ('ICO') published guidance on when data protection laws apply to social media and online forums (copy available at www.pdpjournals.com/docs/88110). The guidance examines the application of the domestic purposes exemption. It compares the situation where an individual blogs in solely their personal capacity (when the exemption is likely to apply) with the situation where an individual blogs on behalf of an organisation, even if expressing personal views (when data protection laws would apply).

The ICO also highlights that a formal group can have a function independently of its members. If members of the club or society share information via social media, this may constitute processing of personal data for the purposes of the group, and data protection law will apply. This can be compared with friends sharing holiday photos, which could fall within the domestic purposes exemption. Data protection law therefore frequently applies to current uses of social media.

(Continued on page 8)

(Continued from page 7)

Responsibility for compliance

Responsibility for compliance with data protection laws lies with the data controller, who determines the purposes for which, and the manner in which, personal data are processed. In relation to social media, there may be several data controllers relating to any particular account or content:

- the social media provider (to the extent that it controls or uses content of sites, or uses information on account holders for providing services, or conducting marketing or analysis);
- an organisation in relation to which an individual uses an account, even if the account holder is the individual rather than the organisation (for example where an individual blogs or networks on behalf of an organisation);
- the individual blogger or account holder (if the domestic purposes exemption does not apply); and
- any other party who makes use of information which is posted (such as a recruiter searching for new staff, or an employer monitoring staff use of social media).

Compliance obligations

All the principles of data protection must be applied to the social media environment. This includes:

- identifying a lawful purpose for sharing or using data and opinions about individuals, satisfying a 'fair processing condition' and making individuals aware of what is being done;
- ensuring data are adequate, relevant and not excessive in relation to the relevant purposes, that data are accurate and kept up to date and not kept for longer than needed;
- respecting the rights of individuals, including providing a copy of data upon request and ceasing to use information which is causing unwarranted damage or distress;
- keeping data secure from misuse, and keeping control of service providers; and
- not transferring data outside the European Economic Area without adequate protection.

In addition to the domestic purposes exemption discussed above, organisations may be able to rely on alternative exemptions. Of particular note is data processing for the purposes of journalism, literature or art, which seeks to protect the public interest in freedom of expression. However, this exemption will only apply to the extent that compliance would be incompatible with the relevant purpose (and does not overcome all aspects of compliance).

Examples of data protection challenges

Using data for new purposes: Social media account information and content which may originally have been shared or created for one reason may be sought after for wider uses such as recruitment, marketing or behavioural analysis. A common misconception is that material found online can automatically be used freely (and not only is this untrue for personal data, it is also untrue for content protected by other laws, such as copyright). If personal data have been posted in a public forum and an organisation wishes to use that data, a lawful purpose must be identified, a fair processing condition satisfied, and individuals must be made aware (unless an exemption applies).

One example is where employers use information about individuals posted on social media as part of the recruitment process, or to monitor their staff's use of such forums. Any such monitoring must be justified by, and be proportionate to, legitimate organisational reasons. For example, checks on whether staff are posting anything adverse to the employer's interests (including in breach of data protection laws!) may be more easily justified than making business decisions about staff based on information posted for purely social purposes.

Organisations should also be careful in relying on information found online where there may be limited guarantees as to its accuracy. The ICO's Employment Practices Code (copy available at www.pdpjournals.com/docs/88111) contains further guidance on monitoring of employees, which can be applied to the social media context.

Even if an organisation has lawfully collected personal data via social media (for example, to set up an online account), if it wishes to use that data for other activities, the 'fair and lawful' requirements must once more be met. This is one of the reasons that Google has faced criticism of its complex privacy policy which purports to allow it to share data between its various services and therefore use data for several purposes.

The ICO's 'Personal Information Online' Code of Practice contains guidance on giving online privacy choices to individuals.

Unauthorised or unexpected use of data: On the flip side of an organisation using data shared by other people, third parties will be looking to exploit data shared by that organisation. Even if such parties are based within the EU and have similar compliance obligations, the reality is that re-use of social media data is very hard to control in practice. If you are sharing information online, there is a risk that other parties will re-use it without your knowledge or approval.

As has been demonstrated by the recent stories on the US Prism surveillance programme (where regulatory authorities may have had access to UK data stored on social media websites), the scope of parties that have access to data may not be obvious.

Security breaches are also common, whether this is as a result of passwords being compromised or networks and servers being hacked. Facebook, Twitter and LinkedIn have all reported unauthorised access to user details or passwords within the last year. Last week, I was surprised to see my husband tweeting about weight loss programmes (as a software engineer, this is not a topic which he generally discusses with the

world). He was in good company; Jamie Oliver's Twitter feed was also packed with weight loss tips that day, which he later indicated was the result of hacking (as were my husband's tweets).

Sharing data via social media also presents the challenge of addressing restrictions on transferring data outside the European Economic Area, and therefore use of data by parties who are not subject to EU compliance obligations. By their nature, social media may be global; as is succinctly stated at the beginning of Twitter's current privacy policy: 'What you say on Twitter may be viewed all around the world instantly'.

Liability for employees' actions: Employers can be held responsible for the actions of their employees. In the context of data protection, this may include misuse of their colleagues' data by sharing personal details via social media. Even if such posts are personal views made from a personal account, the employer can still be liable if they are deemed to be acting on behalf of, or in the course of, their activities for the organisation (as discussed above in relation to the domestic purposes exemption).

There are many other potential liabilities and risks to consider on this theme (discussed further below), including defamation, employment claims, and misuse of intellectual property or confidential information (of the employer or third parties).

Use of excessive data: The requirement for personal data to be adequate, relevant and not excessive means that the amount of information collected, used or viewed by other users must be limited to that which is required for the specified purposes, and it calls for anonymisation of data where appropriate. Recent research by the Chartered Instituted of Marketing ('CIM') highlights that there is currently a concerning lack of a meaningful purpose where businesses collect data from social media, which indicates they are likely to be collecting more data than is really needed. The requirement also creates challenges for online profiling which relies on gathering as much data as possible about an individual's behaviours and activities.

"An organisation should consider the effects of their social media setup when staff leave. Taking into account potential limits of enforceability, it may wish to require employees to hand over details of business accounts, contacts and content, and impose post-employment restrictions on re-using them."

The initial draft of the proposed EU Data Protection Regulation enhanced these obligations with the principle of 'data minimisation'. However, this has been removed from the most recent draft (published by the Council of the European Union on 31st May 2013), and the future of this principle is as yet unclear.

Checking the accuracy of data posted online: The ICO social media guidance referred to above highlights that those who run a social media website must take 'reasonable steps' to ensure the accuracy of personal data and to note where the data subject disputes accuracy. As an example, it looks at the case of *The Law Society and Others v Rick Kordowski* (Solicitors from Hell) ([2011] EWHC 3185 (QB)). In 2011, the Law Society took legal action against the operator of a website which invited users to name and shame solicitors. The operator had decided which posts were published, and had not taken appropriate action once he was notified of disputes as to accuracy. It was held that the operator was a data controller and the requirement for accuracy had not been met. However, the ICO acknowledges that this may not be the case for a site which has large volumes of third party posts with limited moderation, and where the operator relies on user policies and reporting of problems. The cross-over between the data protection requirement of accuracy and defamation claims is discussed below.

Deletion and transfer of data: The requirement not to retain personal data for longer than necessary is already an onerous requirement for social media providers, who may be collecting extensive amounts of information about huge numbers of individuals. The draft EU Data Protection Regulation creates additional challenges — the proposed 'right to be forgotten' and 'right of portability' mean that individuals can request that all data about them on a social network be deleted or transferred over to a new supplier. Some providers may already be going some way to addressing these new rights, for example Google's 'Takeout' feature and facilities allowing accounts and information to be deleted.

Comparison with related information laws

Defamation: Defamation law provides a remedy for an individual (or business) where a false statement is made about him which causes harm to his reputation. Defamation is often claimed in relation to statements made via social media and websites, including the recent case of *Tamiz v Google* ([2012]EWHC 449 (QB)) and the claims of defamation made last year by Lord McAlpine against individual Twitter users.

The question of whether a website operator or other internet service provider ('ISP') can be liable (as well as or instead of the author who posts the statement) has been debated for many years. Case law (including the ground-breaking case of its time — *Godfrey v Demon Internet* ([1999] EWHC QB 244) and more recently *Tamiz v Google*) has held that the ISP can be liable for defamation as a publisher, and needs to take steps

(Continued on page 10)

(Continued from page 9)

to remove defamatory posts once it has notice of them. Defamation law in the UK will soon be updated by the Defamation Act 2013 (which received Royal Assent in April 2013 but is not yet in force). This provides a new defence for operators of websites in some circumstances, where they are not the party who posted the statement.

There is also once more the question of whether an organisation is responsible for statements made by its employees; this is again complicated by difficulties in distinguishing personal and business use of social media.

There is an overlap between defamation and data protection law, as a defamatory comment about an individual will also be inaccurate personal data. The ICO has previously given a view that defamation may be a more appropriate cause of action where the matter is nothing to do with informational privacy or records management, but is rather a slur on a person's character.

Electronic Commerce Directive: The Electronic Commerce Directive 2000 (implemented in the UK by the Electronic Commerce Regulations 2002) provides defences against civil and criminal liability (for example, defamation or copyright infringement) for certain providers of online services. Providers who merely host a website or run an email service can rely on these defences, provided certain conditions are satisfied (which, in the case of hosting, includes actual knowledge of unlawful information). However, one area of law that is explicitly excluded from the scope of the Directive is data protection.

Employment laws: There have been several recent employment tribunal cases considering whether employees have been fairly dismissed (or disciplined) as a result of comments made on social media about colleagues or the employer. Decisions have gone both ways; for example: in *Weeks v Everything Everywhere* (2012), the tribunal held that it was reasonable to dismiss an employee on the basis of threatening and derogatory comments being made about a fellow employee and the employer. By contrast, in *Trasler v B&Q* (2012) it was held that an employee was unfairly dismissed for making complaints about his employer over Facebook (although in breach of the company's policies).

Employment tribunal cases have also emphasised that employers can be responsible for their employees' actions on social media. For example, in the case of *Otomewo v Carphone Warehouse* (2012), the employer was found liable for harassment as a result of its staff making comments on Facebook about the sexual orientation of colleague.

Intellectual Property and confidential information: Organisations may also face liability for misuse of third party confidential information or intellectual property by its employees over social media (such as revealing client or financial details, or sharing materials or software). There are also challenges in preventing staff from misusing the organisation's own confidential information and intellectual property. It is all too easy to blog about what one is up to at work.

Another important consideration is the extent to which an organisation can maintain control of contacts and content created by its staff. Social media has become an important part of marketing strategies. Relationships with connections, followers and friends are formed and developed by staff members whilst working for an organisation and information shared amongst them.

With traditional marketing materials and customer lists, organisations would claim ownership of copyright and database rights. However, it is less clear whether social media contacts and records 'belong to' the individual account holder, the organisation or the social media provider. In addition, organisations frequently place restrictions on employees maintaining relationships with business contacts when they leave employment through confidentiality obligations and restrictive covenants. However, social media contact lists are often publicly available (and therefore not confidential) and there may be limits on the enforceability of restricting employees from maintaining individual business networks (which have become commonplace in forums such as LinkedIn).

There are therefore risks that a former employee or a competitor may legitimately re-use contacts and materials. Even if not legitimate, the nature of accounts being set up in individual names makes it difficult to prevent. This was demonstrated in the US case of *Phonedog v Kravitz* last year. An employee left an organisation and continued to use a Twitter account with a significant number of followers which had originally been set up to tweet on behalf of the company. The employer argued this was a misuse of its trade secrets. The case was ultimately settled, but it is understood that the employee retained the Twitter account.

Looking at the data protection angle, for the same reasons it is not clear whether contacts have intended to follow or befriend the individual rather than the organisation. Therefore, even if the organisation can take control of an employee's contact lists, it will need to assess whether continued use is fair and lawful.

Other information laws: Many other aspects of information law need to be considered in the social media environment. The UK Human Rights Act 1998 (including Article 8 — right to a private life, and Article 10 — right to freedom of expression) and the law of confidence have become particularly prominent in recent years in relation to media intrusion into private lives. The UK Computer Misuse Act 1990 makes it a criminal offence to gain unlawful access to information stored on computers and should be considered in relation to security breaches. The UK Regulation of Investigatory Powers Act 2000 governs interception of communications and surveillance activities — relevant for situations such as the US Prism surveillance programme referred to above. This is by no means an exhaustive list.

Social media strategy

It is important for all organisations to consider carefully their strategy for making use of social media. Bene-

fits and risks need to be assessed, as a social media user, an employer or a provider of social media services, including legal obligations and potential liabilities. The following considerations may assist in addressing the challenges discussed above and maintaining control of information.

Defining the purposes: The purposes for which social media are used should be clearly defined. These may form part of marketing, publicity, recruitment, networking, staff monitoring or other objectives.

Deciding on appropriate forums: As well as looking at how specific social media can meet strategic goals, an organisation should consider how account information and content may be used and protected in a particular forum. If relying on a third party provider's services, factors may include the reputation and location of the provider, the security and other guarantees provided, and terms of use (including rights which the provider may have to data or content).

In addition to publicly available social media services (such as Twitter or Facebook), an organisation may wish to implement bespoke forums, operated internally or by a third party (for example on a company website or intranet). In this case, it will need to consider its additional responsibilities as a social media provider.

Roles of staff and third parties: The intended involvement and roles of different staff members and third parties (including service providers or agents) needs to be clarified. Will blogging be undertaken by trained marketing personnel only, or will other staff members be permitted (and encouraged) to use social media on behalf of, or in the course of activities for, the organisation? Will there be a defined approval process? The organisation should also decide whether accounts will be held in the name of individual staff members, or whether to set up a corporate account (if permitted by the social media provider) which the staff can use whilst they work for the organisation.

Setting the boundaries of social media use: Boundaries should be set around the defined purposes. For example, if social media are to be used to market and publish a consistent corporate message, limitations should be set on posting personal opinions and wider networking or monitoring activities. The amount of personal data collected over social media should also be proportionate to the stated purposes.

In order to avoid legal liabilities and negative impacts on reputation, organisations may also wish to set controls around how staff use social media in their personal capacity, including restricting the extent to which staff can refer to their professional life and requiring personal views to be clearly distinguished from business views (potentially by holding separate accounts). The practical and legal difficulties in enforcing such restrictions need to be taken into consideration. If an organisation is running its own social media platform, it should clearly define the boundaries of intended use by staff, customers, members or the public (and terms of use are discussed below).

Managing and monitoring use: Organisations should appoint responsibilities for managing social media use and consider how they will retain oversight and control over the activities of staff, customers and the public. For example, will content be checked prior to being posted to third party or internally-run sites, how and when will content be reviewed (and, if necessary, removed) and how can misuse be reported and investigated?

Some level of monitoring will be needed in order to enforce compliance with policies and terms (see below), and to avoid liabilities (as an account holder, employer and/or social media provider). However, data protection and related legal limitations on monitoring will need to be addressed. An organisation should consider the effects of their social media setup when staff leave. Taking into account potential limits of enforceability, it may wish to require employees to hand over details of business accounts, contacts and content, and impose post-employment restrictions on re-using them.

Policies, terms and training: The CIM research identified that whilst businesses have generally acknowledged the risks of social media, less than 50% of organisations have defined social media guidelines and policies. Staff and users of social media must be made aware of their roles and responsibilities. Decisions made on the issues highlighted above need to be documented and communicated, and training provided where appropriate. A social media policy can set out the purposes and boundaries of use, staff responsibilities during and post-employment, and any monitoring of use (all as described above). The risks and consequences in use of social media, for employees, the organisation and other users, can also be communicated.

Terms of use and privacy notices for an organisation's own social media platforms on websites or intranets should be prepared. As well as describing the rules in sharing information (for example, ensuring comments are not defamatory or in breach of privacy laws), these should describe how information may be used and monitored by the provider, the choices which the individual has on data use, and related risks for the user (for example, location and security of data).

Evolving law and reviewing strategy: The law continues to develop with new legislation (including the proposed EU Data Protection Regulation), case law and regulatory guidance seeking to address challenges in protecting rights and applying obligations in the social media environment. These changes are also creating new challenges of their own in practical implementation and enforcement. As well as legal developments, organisations need to keep an eye on the rapidly evolving culture and technology of social media. Strategy and policies need to be regularly reviewed as benefits, trends and risk profiles of social media change, in order for organisations to maintain appropriate control over communication and use of information.

Olivia Whitcroft
OBEP
olivia.whitcroft@obep.co.uk