Private eye

Tom Morrison returns with his quarterly review of the world of information law

IN BRIEF

- Data protection issues abound with the growth in social networking.
- Does BYOD = Bring Your Own Downfall?
- Will two recent FOI cases make it harder for regulators to secure cooperation?
- The ICO wants to get less embroiled in wider disputes.

Christmas 2013 may have become a distant memory, but any work-related party of note will have left its indelible mark somewhere on a social network. Party-goers up and down the land will have made sure that those special moments from their work dos were captured in prose on Twitter, through grainy fake Polaroids on Instagram or with amusing clips posted on YouTube. There can be few workplaces where an employee has not done something like tweeting a picture of a photocopied body part with the hashtag #mybossisanidiot or posted a video of themselves drinking vodka via their eye sockets.

The anecdote becomes somewhat less amusing for the employee if, once the alcohol-induced haze has cleared, his or her employer decides that the employee may have brought the business into disrepute because the company's social media account was used, or the star of the video was in company uniform at the time. There is an employment law minefield to navigate, not only in relation to how that employee is dealt with, but also in terms of how to handle situations that can develop between employees.

Thankfully, it is beyond the scope of an information law column to get into this in too much more detail, but it does help to illustrate that, whereas in the past what happened at the party might have stayed at the party, it is now much harder for businesses to keep control of their corporate images and the images of their employees in the social media age. It is crucial for all employers to make clear the standards that are expected of their employees. This is relevant not only to the use of corporate social media accounts, but also employees' own accounts. These might include business oriented social media channels such as LinkedIn, but will go further to include other informal media used more widely such as SnapChat or Tumblr.

Alongside employment law issues, there are Human Rights Act considerations; but the basic position will always be that employers should communicate in a clear and unambiguous fashion the standard of behaviour required from their employees. Depending on the extent of use within a given workplace, it might be appropriate for employers to consider giving relevant employees training in how not to find themselves on the wrong end of a social media-induced harassment or defamation claim.

ICO social networking guidance

Social media as a legal topic is not only trendy, but huge. The range of issues from a data protection perspective alone can be significant, to the extent that the Information Commissioner's Office has published guidance to assist both those who use social media and those who run platforms, such as discussion forums. Key questions addressed by the guidance include:

- When does the Data Protection Act 1998 (DPA 1998) apply to social networking?
- When does the domestic purposes exemption apply?
- To what extent are operators of social media platforms data controllers?
- When will the ICO get involved in complaints?

There is also recognition in the guidance that there is a world beyond DPA 1998. Other relevant legislation includes the Protection from Harassment Act 1997, the Communications Act 2003, the Malicious Communications Act 1998 and the newly enacted Defamation Act 2013.

> *"There can be few workplaces where an employee has not done something like tweeting a picture of a photocopied body part with the hashtag #mybossisanidiot"*

Ignore BYOD & Bring Your Own Downfall?

There has been much written in the legal and popular press about the prevalence of Bring Your Own Device (BYOD) in the workplace. Enabling staff to use their own devices for work may make them happier to make themselves available, outside of their normal working hours, for the benefit of their employers and customers; employees use kit they really like and the employer can shave a few pounds off the IT budget if staff are, in effect, paying for devices being used in the workplace.

Many organisations have embraced BYOD, but a sizeable proportion have deliberately restrictive policies. In practice, can many employers really say that no employees are using their own devices for the storage or use of work-related information? Is an employer,

which has highly restrictive policies, really doing more to protect business information and personal data than an employer which has a properly thought out and responsive process to enable controlled use of personal devices? Or are they just deluding themselves and, in the process, leaving a gaping hole in their information handling and security procedures? Surely it must be better to understand why employees are wanting to use their own devices and either satisfy that need by improving what is supplied at the employer's expense, or putting in place ground rules for the use of personal devices.

The Royal Veterinary College breached DPA 1998 when a member of staff lost their own camera, which included a memory card containing the passport images of six job applicants. The ICO found that the organisation had no guidance in place explaining how personal information stored for work should be looked after on personal devices. The college was required to give an undertaking to put training in place training and secure devices going forwards.

The ICO has issued BYOD guidance reminding employers to be clear with staff about the extent to which personal data may be processed on personal devices; require the use of strong passwords and encryption; ensure that the device is locked or wiped if an incorrect password is input too many times; be cautious about using public cloud-based sharing and backup services; and ensure devices can be remotely located and wiped in the event of a loss or theft. Additional points to bear in mind are that:

- private and work data should be kept separate;
- data needs to be transferred off devices in a secure manner and not on open Wi-Fi networks;
- work data must be removed securely from devices when employees dispose of them or change employment; and
- passwords should be changed and access rights to facilities, such as work e-mail, must be revoked when an employee leaves.

Freedom of information leading to secrecy?

The recent cases of *Kennedy v Charity Commission* [2012] EWCA Civ 317, [2012] All ER (D) 143 (Mar) and *Sugar v British Broadcasting Corporation and another* [2012] UKSC 4, [2012] 2 All ER 509, might make organisations look more carefully at what information they are sharing with public authorities caught by the Freedom of Information Act 2000 (FIA 2000).

In *Kennedy*, a journalist for *The Times* newspaper submitted a request for information under FIA 2000 to the Charity Commission relating to three inquiries it carried out into the "Mariam Appeal". The Mariam Appeal was launched in 1998 by MP George Galloway, following the imposition by the UN of sanctions against Iraq. In 2003, allegations were made that improper donations had become funds of the appeal which prompted the Charity Commission to carry out three inquiries. The Charity Commission found that improper donations of £230,000 had been made by a major fundraiser and chairman of the appeal. The Charity Commission further held that the appeal's trustees had not made sufficient enquiries as to the source of the funds and that Galloway may have known of the fund's origin.

> *"Something has got to give. The ICO cannot afford to be used as a pawn in a complainant's game if the real gripe is nothing to do with data protection"*

The Charity Commission refused to release the requested information to Kennedy on the basis that it was obtained during a statutory inquiry and so the legal exemption under s 32 of FIA 2000 applied. The case was unsuccessfully appealed by Kennedy to the Information Commissioner, the Information Tribunal and the High Court. On appeal to the Court of Appeal, Kennedy raised a new argument that his right to freedom of expression under Art 10 of the European Convention on Human Rights (ECHR) had been breached and that the exemption should not apply to inquiries once they are concluded. The Court of Appeal upheld the decision of the Charity Commission and held that the exemption under s 32 lasts for 30 years, following the completion of the inquiry.

Shortly before *Kennedy* was heard by the Court of Appeal, the case of *Sugar v British Broadcasting Corporation and another* came before the Supreme Court which concerned the extent to which FIA 2000 applied to the BBC and the interaction with the ECHR. The Court of Appeal granted Kennedy permission to appeal the decision to the Supreme Court to "consider the precise boundaries of Art 10(1), particularly in a case where the applicant is taking the journalistic role of a social watchdog".

Kennedy has now been heard in the Supreme Court and is currently awaiting judgment. If the appeal is successful, then the information relating to the three Mariam Appeal inquiries may be released, with potential implications for inquiries by the same and other regulators in relation to unrelated cases. Although some regulators have the power to demand disclosure of information when conducting enquiries, and although in some situations the strategic or moral imperative lies in full cooperation, the interaction between these two cases reminds lawyers of the need to advise their clients that any information they give to public authorities, including in relation to inquiries, may potentially be made public.

ICO consultation on complaints handling

The ICO has conducted a consultation and determined that it will change its approach to dealing with complaints under DPA 1998. There has been an argument for some time that it is getting drawn into complaints which have a data protection element but which, in truth, are about a much wider substantive issue.

While the ICO has not been shy in showing its teeth in recent years, if the principal role of the regulator is ultimately (using the ICO's own words) to improve the wider information rights practice of organisations and to tackle systemic problems, then something has got to give. The ICO cannot afford to be used as a pawn in a complainant's game if the real gripe is nothing to do with data protection. Equally, where there are failings in an organisation's compliance, but no intent or serious harm, is it necessarily appropriate to bring the full weight of the law down on that particular organisation just because they are the ones to have tripped up? Or should that element of the taxpayers' resources which are made available to the ICO for data protection matters be focussed on helping those who have suffered substantial loss and trying to tackle the most serious and widespread issues? I know where I want my money to be spent. **NLJ**

Tom Morrison, partner, Rollits LLP (*tom.morrison@rollits.com; www.rollits.com*)