Data protection / FOI

Private eye

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

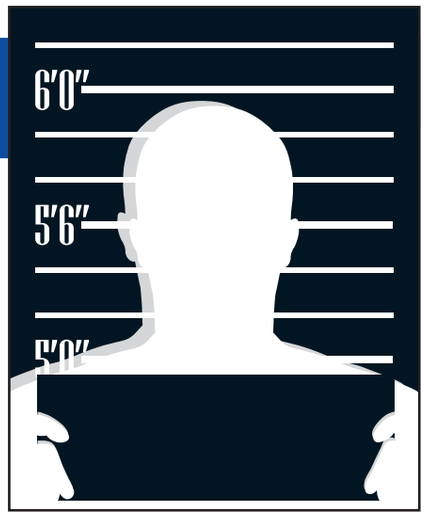

Photo: © istockphoto.com

IN BRIEF

- The revelations surrounding the *News of the World* are not new; they were highlighted by the information commissioner five years ago.
- Is everyone in your organisation handling personal information appropriately?
- Organisations are repeatedly having enforcement action taken against them for inadequate security procedures. Lack of encryption and mis-directed faxes and e-mails are recurrent themes.
- Tweets can be valid FOI requests.

I mentioned in my first column that one of the consequences of a public authority complying with a request for information under the Freedom of Information Act 2000 (FIA 2000) can be that the media acquires some embarrassing information (NLJ, 20 May 2011, p 698). In the months that have followed it has been certain media outlets themselves that have suffered the consequences of disclosure as new revelations concerning inappropriate use of private investigators have come to light. Whilst some of the recent detail is disturbing, the fact of newspapers using private investigators to uncover information is not new. Neither is the fact that some of the methods used by those private investigators have been questionable at best.

Operation Motorman

Following an investigation code-named Operation Motorman the then information commissioner, Richard Thomas, highlighted the issues in his 2006 reports to Parliament *What Price Privacy* and *What Price Privacy Now?*. One of his aims was to expose the illicit trade in personal data that had existed for some time and which he felt had to be stemmed—and it was clear from those reports that the questionable practices were not limited to the *News of the World*. Individuals were profiting from the sale of personal information such as telephone records to feed various newspapers' insatiable appetites for scoops. The information commissioner argued for custodial sentences for the worst cases but was given fining powers instead. This latest set of revelations has prompted the current information commissioner, Christopher Graham, to renew his predecessor's call for the threat of jail for the worst offenders and his files have again been copied to the police to assist in their investigations.

So what does all this mean for those of us who are not private investigators or newspaper publishers looking for the next big story?

First, just as there was an increase in awareness and enforcement activity after HMRC's loss of two discs containing personal data in 2007, the same may well happen again. Individuals will wonder just what information you hold about them, how you obtained it, and what you are doing with it. You have proactive obligations under the Data Protection Act 1998 (DPA 1998) to inform individuals what information you are processing and why, and, if asked the question, you are required to respond within a tight timeframe. Are you sure that you could comply with a request for that information in a prompt and accurate manner?

Second, are you sure that your staff are dealing with third parties appropriately? As has been seen in recent weeks there is little sympathy for heads of organisations (no matter how large) who do not know what their staff are doing or who do not seem to have adequate procedures in place to keep staff in check. Have your staff been properly trained in their data protection obligations recently? Is there a policy in place governing how information should be handled and to whom and for what purposes it may be disclosed? Has that policy been updated and has it been re-communicated to staff with training appropriate to their role? If the answer to any of these questions is no, or if you are not sure, now would be a good time to check and take corrective action rather than wait to see if anything goes wrong.

Freedom of information round-up

In some respects freedom of information (FOI) has taken a bit of a back seat over the past few months while the furore surrounding the *News of the World* and the associated data protection issues have taken centre stage. It would be wrong to think that this means that FOI has slipped down the information commissioner's agenda. There has been a marked increase in complaints this year, with a record number being dealt with.

The information commissioner's office (ICO) continues to monitor a number of public authorities' compliance with FIA 2000 and is persisting in its policy of naming those authorities being actively monitored. Seven out of 33 public authorities monitored in the period up to the end of June 2011 were required to make improvements. In addition to obtaining undertakings from the London Borough of Hammersmith and Fulham, the London Borough of Islington, Westminster City Council, and Wolverhampton City Council, the ICO has also required undertakings from the Cabinet Office, the Ministry of Defence and

Birmingham City Council demanding that they improve their response times to FOI requests. As well as being named and shamed, if any of these authorities fails to comply with the terms of an undertaking the ICO may decide to take formal regulatory action. The message for public authorities from the latest round of announcements is clear: respond to FOI requests within the statutory timeframe or risk enforcement action. The ICO also continues to push for a culture of openness, recently ordering the Cabinet Office to disclose the names of public sector workers who earn more than £150,000 per year.

Wanting to be seen to keep up with modern forms of communication, guidance has been published on the circumstances in which a direct tweet sent to a public authority using Twitter can constitute a valid FOI request. Perhaps more alarmingly the ICO takes the view that "@mentions" can also be valid FOI requests. Given the consequences of non-compliance and the tight timescales involved, this latest guidance highlights the need for all public authorities that use Twitter and similar messaging services to monitor their accounts on a regular basis or put in place appropriate contractual arrangements with their service providers to make sure the accounts are monitored on the authority's behalf.

Data protection round-up

Data security remains one of the most prevalent issues when it comes to data protection compliance:

Sheffield-based charity Asperger's Children and Carers Together and Nottingham-based charity Wheelbase Motor Project were both found to have breached DPA 1998 by failing to encrypt computers containing sensitive information. This follows a string of decisions where it has been repeatedly made clear that encryption, particularly for portable devices, is not optional where those devices store personal data.

Co-operative Life Planning failed to ensure a contractor followed the company's security procedures. One of the reasons the organisation escaped a fine was that it could demonstrate that it had appropriate policies already in place regarding protection of personal information stored on its servers.

North Lanarkshire Council breached DPA 1998 after the theft of a home support worker's bag containing papers which included sensitive personal information. The bag was not locked and contained the worker's visiting schedule for the next two days, including information as to the mental or physical health of six vulnerable adults who were being supported by the council. Is your briefcase locked as you read this?

Surrey County Council received a £120,000 fine after sensitive personal information relating to 241 individuals was e-mailed to the wrong recipients on three separate occasions. The worst disclosure involved accidentally e-mailing an unencrypted file to an incorrect group of external e-mail addresses, highlighting the risks of having e-mail groups that include external e-mail accounts. One of the incidents, however, involved an internal-only group of e-mail addresses but was still considered serious due to the nature of the information disclosed. The ICO has required the council to take action to improve its policies on information security, including the development of an early warning system which alerts staff when sensitive information is being sent to an external e-mail address and implementing improved staff training.

The health sector remains an area of particular concern for the ICO, prompting it to issue a press release highlighting repeated cases of inappropriate use of unencrypted memory sticks and misdirected faxes. Five undertakings have recently been issued in relation to the health sector, all of which relate to a lack of adequate security measures.

Individuals are also being prosecuted: two former T-Mobile employees who were found to have stolen and sold customer data were ordered to pay a total of £73,700 in fines and confiscation costs, and a former personal injury claims company employee has pleaded guilty to offences of illegally obtaining NHS patients' information to generate leads for Direct Assist. He was prosecuted under s 55 of DPA 1998 and ordered to pay a fine plus a sum towards prosecution costs and a victims' surcharge.

Voluntary audits

The ICO has made a plea for businesses to volunteer for data protection audits. Its latest annual report shows that almost a third of reported security breaches originated from the private sector, but less than a fifth of businesses accepted an offer to undergo a free data protection audit compared to over two thirds of public sector organisations. While in principle an audit could reap significant benefits, any organisation thinking about volunteering for an audit would first need to assess the pros and cons of doing so.

Cookies update

The last column went to print just as the new law relating to the use of cookies came into force. At the same time the ICO published a press release outlining its position on enforcement. Some media outlets interpreted this as meaning that there was no need to take any action until next year: to follow that approach would not only be misinterpreting the ICO's enforcement policy but would also put website owners at greater risk of receiving a fine come May 2012. The ICO has made clear that it expects every organisation which has a website to spend the coming months analysing what cookies they have in place, what impact the use of those cookies might have on privacy and what plans are to be put in place to address those privacy issues. If these steps have not been taken and the ICO investigates a website before May 2012 it may issue a warning notice requiring corrective action which will be placed on file. If there is further investigation after May 2012, the existence of a warning notice could fast track the website owner to a fine. The ICO has also published details of the proposed use of its fining powers which effectively mirror its existing powers for other data protection breaches and include the ability to fine up to £500,000.

Data-sharing code

A new statutory code of practice has been published which is designed to help businesses and public sector organisations share individuals' personal information in an appropriate manner. Its aim is to help organisations understand when, whether, and how personal information should be shared and reduce the risks surrounding inappropriate or insecure sharing. While the code is helpful in that it puts data sharing in a real-life context, the general rule remains that if an organisation acts responsibly and is open with individuals about how their information will be handled then there is much less scope for inappropriate sharing to take place with the consequences that may follow. NLJ

Tom Morrison is a partner at Rollits LLP.
E-mail: *tom.morrison@rollits.com*
Website: *www.rollits.com*