Data protection / FOI

Private eye

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

Photo: © gettyimages.co.uk

IN BRIEF

- Significant increases in the information commissioner's use of fining powers over the past few months have been accompanied by renewed calls for prison sentences for "blagging" offences.
- Proposals are being considered to update data protection legislation across Europe with the fear that it will increase the legislative burden on all organisations which hold information about individuals.
- Anyone working for a public authority should not assume that just because they are using private e-mail accounts the contents of their e-mails fall outside the FOI regime.
- Don't forget about the new cookies laws which will be enforced from May 2012.

The previous edition of this column highlighted the fact that, while there had been a great deal of enforcement activity in the preceding quarter, the information commissioner's office (ICO) had seemed to have eased off using its fining powers following a pattern of fairly consistent use over the previous year (161 NLJ 7490, p 1586). The focus had very much switched to highlighting what had gone wrong and securing compliance going forward through a series of undertakings to do better. Well things have moved on since then.

So what has been happening?

Councils in particular have been in the firing line; here are a few examples:

(i) Worcestershire County Council and North Somerset County Council were fined £80,000 and £60,000 respectively at the end of November 2011. In the Worcestershire case a member of staff e-mailed highly sensitive personal data about a large number of vulnerable people to 23 unintended recipients. The error was caused by the sender clicking on the wrong e-mail distribution list. In the North Somerset case an employee sent five e-mails to the wrong NHS employee, two of which contained highly sensitive and confidential information. The sender was told each time by the recipient that the error had taken place but the same error kept getting repeated. That was never going to go down well with the ICO.

(ii) Powys County Council was fined £130,000 in December 2011 for allowing the details of a child protection case to be sent to the wrong recipient. A similar but less serious incident was reported by the same council a year and a half earlier. The breach basically arose out of a mixing of papers on a shared printer. Easily done, but what seems to have particularly angered the ICO is that the council did not implement the recommendations made by the ICO following the first breach.

(iii) The biggest fine to date came not long into the New Year. Midlothian Council had disclosed sensitive personal data relating to children and their carers to the wrong recipients on five separate occasions for which it was fined £140,000. The ICO judged all of the breaches to have been both serious and avoidable, had adequate procedures and training been put in place. Some occurred after investigations into the earlier breaches had already started so the risks were known. Given that the breaches specifically involved inadvertent addressing, the council has implemented new procedures to make sure that any letter containing sensitive or confidential information is now checked by a second member of staff before being sent. A good rule of thumb: expect to be fined, or to be fined more, if you don't learn from your mistakes.

(iv) Cheshire East Council was ordered to pay a fine of £80,000 after an employee sent an e-mail to a local voluntary sector co-ordinator's personal e-mail account detailing some concerns that the police held about an individual. The e-mail was not sent using the council's secure system and was ultimately forwarded through a chain to 180 unintended recipients. The ICO highlighted that the council had insufficiently robust systems and had not provided adequate training to the employee who initiated the communications.

The ease with which some of these organisations found themselves on the wrong side of a fine is frightening, but not because they are particularly unusual. Quite the opposite; it will not take much for any organisation from the public, private or third sector to find itself in a similar situation if it does not maintain effective procedures, train its staff in a meaningful way, monitor compliance, actively look for exceptions and learn from any mistakes made.

The demand for prison sentences

Our enforcement mechanism is found lacking when it comes to the punishment of individuals who unlawfully obtain or access personal data, ie "blaggers". In December 2011, a court heard that a receptionist unlawfully obtained her sister-in-law's medical records in order to find out about the medication she was taking. She was only given a two-year conditional discharge and ordered to pay £614 prosecution costs. In January 2012, a former healthcare assistant at a hospital pleaded guilty to unlawfully obtaining patient information by accessing the medical records of members of her ex-husband's family in order to obtain their new telephone numbers. She was fined just £500 and paid a £15 victim's surcharge and £1,000 towards prosecution costs.

By contrast, at end of February 2012, information commissioner Christopher Graham commented on a successful prosecution under the Fraud Act 2006 by the Serious Organised Crime Agency (SOCA), involving a private investigator and his three accomplices. Graham made clear his frustration at the continued delay in activating a power for the courts to hand down prison sentences solely under the Data Protection Act 1998 (DPA 1998), saying "If SOCA had been restricted to pursuing this case solely using their powers under DPA 1998 then these individuals would have been faced with a small fine and would have been able to continue their activities the very next day. This is not good enough. Unscrupulous individuals will continue to try and obtain peoples' information through deception until there are strong punishments to fit the crime".

It does seem a little absurd that an organisation which makes a mistake can be fined up to £500,000 but individuals who go about their business by unlawfully gaining access to personal information face a fine which is likely to be smaller than the financial gain made from committing the act. The Leveson Inquiry is clearly relevant to the debate, as much of the discussion around press standards relates to the use of private investigators. Maybe the time has come for the government to bite the bullet and activate the power for the courts to impose prison sentences under DPA 1998, without forcing prosecutors to find alternative legislation to reach the same end.

Legislative change in the pipeline

The European Commission has recently proposed making Europe-wide changes to data protection law. The consensus so far seems to be that there is potential for the proposed changes to increase the compliance burden on all organisations that process personal information (which means pretty much every organisation in the private, public and third sectors). A "right to be forgotten" is being muted, and has largely arisen out of the wish of many citizens to be able to erase their social media history, while a proactive obligation to notify data breaches seems popular but if not handled correctly could lead to individuals and the ICO being swamped with notifications for relatively innocuous breaches.

> "The phraseology in DPA 1998 is often counterintuitive & the language can be frustratingly vague"

There is a valid fear that by being more prescriptive the law may lose some of its flexibility. Our law is far from perfect, but it does on the whole work. The phraseology in DPA 1998 is often counterintuitive and the language can be frustratingly vague, but I am not hearing a broad-based ringing endorsement of the European Commission's proposals. Watch this space.

Remember to check cookies compliance

As reported in previous editions of this column, the law on cookies changed last May. A period of grace was granted by the ICO to give organisations time to secure compliance. That period comes to an end in May 2012. The ICO has indicated that it feels that some organisations have not been moving fast enough to get themselves ready for the new regime and has issued an updated version of its guidance. So if you are not looking at it yet, now is the time to be pushing cookie compliance towards the top of the to-do list.

Not so private e-mails

Why is the secretary of state for education currently considering appealing against a decision of the ICO to require that certain e-mails are disclosed pursuant to a request for information under the Freedom of Information Act 2000 (FIA 2000)? Because the e-mails went through his personal e-mail account rather than his official work e-mail account.

There have been various reports regarding the content of the e-mails, but in basic terms the ICO has found that the e-mails were about departmental business, and therefore disclosable under FIA 2000. The lesson for all public authorities is not to forget that information held on behalf of (as well as by) a public authority is caught by FIA 2000. So if, for example, a piece of work is e-mailed to and from a home account by a public authority employee the information contained within those e-mails is potentially disclosable (subject to the usual exemptions) because the employee is holding that information on behalf of the public authority.

It would have been ludicrous if the ICO had found that only work e-mail accounts were covered by our freedom of information regime. If that had been the case, then anything which a public authority wanted to shield from disclosure could have been taken out of scope, merely by using a different e-mail account. That surely cannot have been what was intended by the legislators. If we assume that the general public believes that it is on the whole a good thing to be able to have access to information held by authorities which are basically bankrolled by the taxpayer, then a perverse outcome has been averted.

The department for education can, if it wishes, appeal or issue a refusal notice, giving reasons for its refusal to comply with the ICO's decision. Either way, all public authorities should remind their employees that they may be expected to search their home e-mail accounts pursuant to a request for information and that if they choose to delete or conceal information (which might include hiding information in a home e-mail account), with the intention of preventing its disclosure following receipt of a request, they could be committing a criminal offence under s 77 of FIA 2000. And that is before you even get on to looking at the security implications and associated data protection issues of allowing employees to use home e-mail accounts for work purposes. NLJ

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