Data protection / FOI

Private eye

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

Photo: © istockphoto.com

IN BRIEF

- Government ministers failing to keep their own houses in order does nothing to help to encourage businesses to take data security seriously.
- Information commissioner asks for stronger audit powers & for courts' custodial sentencing powers to be activated for certain types of data breaches.
- New junk mail suppression arrangements due to go live next spring.

It is a generally accepted principle in our society that personal information should be treated with care. We did not need to put in place a piece of legislation to tell us that, but we did and it does. So why have two government ministers recently been the subject of press stories highlighting their apparent disregard for information which was in their—or their offices'—possession?

Cabinet office minister Oliver Letwin was caught on camera throwing constituency correspondence and other papers into a waste paper bin in St James's Park and, less than a month later, business secretary Vince Cable was forced to apologise after letters were found in bags placed outside his Richmond and Twickenham office. Granted, their indiscretions would perhaps not have received quite so much attention had they not been government ministers, and both have subsequently issued apologies, but such events do nothing to help encourage businesses, charities and public sector organisations to put their houses in order when the law makers have some tidying up of their own to do.

ICO continues to sharpen its teeth

A common view in the early days of the data protection registrar and later the information commissioner's office (ICO) was that our data protection laws were policed by a seemingly toothless and benign regulator. Until relatively recently the ICO could give you a bit of a bashing in the papers (and indeed has now become quite proficient at it), but as for formal enforcement powers, the worst it could do was issue notices and try to convince the court to fine you up to £5,000. Such a paltry fine was seen as not much more than a business expense, assuming your line of business was selling stolen information for at least 10 times that amount.

Well, times have changed. The ICO has gathered some real momentum following quite a range of activity over recent months. The information commissioner Christopher Graham has been in Parliament asking for an underlying power for the courts to put people in jail for data theft to be activated—the power was put on the statute books several years ago but has laid dormant ever since. Members of Parliament on the House of Commons Justice Select Committee are backing his calls so perhaps we can now expect the power to finally come into force.

The ICO has also been churning out guidance at quite a pace on a range of issues, including the impact that freedom of information has on research studies, and how organisations should handle requests for information held in complaints files. While much of that guidance has arisen out of issues affecting the public sector, the information commissioner has been keen to point out that the private sector needs to take greater care than it has done in recent times.

Compulsory audit powers

Public sector organisations have been at the forefront of most of the recent data protection news stories, but the reality is that we hear more about the public sector because public organisations are more proactive in reporting themselves to the ICO when they breach the Data Protection Act 1998 (DPA 1998), and in some cases they have no legal option but to report themselves.

One way to tackle this would be to open up more organisations to an ICO audit. The ICO has very limited powers to force an audit upon an unwilling auditee and for that reason it is making a case for an extension of its powers of audit. In an attempt to garner support, the information commissioner has been promoting audits as "free health checks". While some will remain sceptical, the ICO has repeated its position that it will not generally impose a fine if a breach of DPA 1998 is discovered during the course of the audit (although the auditee will be expected to remedy that breach quickly and its compliance will be monitored). The ICO is trying hard and is undoubtedly genuine in its wish to be helpful, but it is still a tough sell to try to get an organisation to subject itself to a voluntary audit, unless it is either sure that its procedures are tight enough to bear scrutiny or it is equally confident that something has gone terribly wrong and it is therefore hoping for a bit of leniency in return for cooperation.

Handling complaints files

The public has a general right of access to information held by public authorities, and all individuals have the ability to require a data controller to disclose information held about themselves. In

practice, most people do not exercise those rights because they have better things to do with their time. There are, however, times when the right to access information becomes a powerful tool. It is a sad but inevitable truth that a sizeable proportion of requests under DPA 1998 and the Freedom of Information Act 2000 (FIA 2000) arise in connection with a wider complaint. Where there is a wider complaint there is often a pile of correspondence, internal notes and other documentation surrounding the handling of that complaint or the circumstances associated with the complaint, some of which the holder of the information may prefer is not disclosed.

Recognising the difficulties that data controllers and public authorities face in dealing with such requests, the ICO has released guidance on handling requests for information held in complaints files. The guidance is far from revelationary, and, in places, its reasoning seems a little opaque, given that it does not cover in any depth the various exemptions to disclosure that often apply, but it is a visible and welcome attempt by the regulator to put the application of the law into a practical context.

Disclosure of research information

A second piece of guidance has been produced following recommendations made in the House of Commons Science and Technology Committee report on the disclosure of data about climate change involving the University of East Anglia. It attempts to increase academics' and researchers' understanding of freedom of information legislation and to help public authorities comply with their disclosure obligations. The guidance is of specific relevance to universities and other public sector organisations carrying out research and recognises the complexities associated with the research and peer review process, but many academics will remain nervous as to the impact of FIA 2000 on their work and the detrimental impact that could have on the value of the results of the research.

New public authorities subject to FIA 2000

Three more organisations have recently been named as public authorities to be made subject to the requirements of FIA 2000: the Financial Ombudsman Service, the Association of Chief Police Officers of England, Wales and Northern Ireland and the Universities and Colleges Admissions Service. The change was made pursuant to the Freedom of Information (Designation as Public Authorities) Order 2011 (SI 2011/2598). The government has previously made clear its desire to extend the scope of FIA 2000 to cover more organisations that are in receipt of public funds. It was thought some time ago that housing associations would be among the first to be added to the list. They have escaped direct regulation under FIA 2000 so far, but it seems inevitable that they will at some point be caught by this additional compliance requirement.

Reducing unwanted junk mail

A new initiative is set to be launched next year with the intention of reducing the amount of junk mail received by members of the public. The Department for the Environment, Food and Rural Affairs has entered into an agreement with the Direct Marketing Association (DMA) with the aim of reducing waste and carbon emissions by encouraging organisations to be more environmentally responsible and making it easier for householders to withdraw their consent to receiving unsolicited mail.

Currently there are three different systems that individuals must sign up to if they no longer wish to be sent junk mail. The new arrangements aim to establish a single point of access with a new website expected to be launched in April 2012. Householders will also be sent guidance as to the different types of marketing and how they can manage their exposure to them.

The new procedures will impact on all organisations which send physical direct marketing communications including unaddressed mail and loose inserts in other publications. Untargeted marketing can be costly to the advertiser and downright annoying to an unwilling recipient; by putting in place a more sophisticated and hopefully less bureaucratic system for junk mail suppression, advertisers should be able to get a better return on their investment by only marketing to those who wish to be marketed. Perhaps we can also save a few trees into the bargain.

Plenty of security breaches but no more fines?

In the August edition of this column I included a round-up of enforcement activity that had taken place in the preceding quarter (NLJ, 12 August 2011, p 1134). It has been a similar story over the past three months, with a number of data losses involving USB keys and unencrypted laptops and the health sector remaining a particular cause for concern.

There does appear to have been a slowdown in fining activity following an initial flurry of substantial monetary penalty notices. Instead of issuing fines, we seem to be witnessing a period where the ICO is focusing on providing more practical guidance and publicising organisations' mistakes. The main enforcement mechanism used over the past few months has been for the ICO to issue an undertaking requiring the organisation to do better next time which is then signed by the chief executive of the organisation.

Undertakings commanding the boss to put his or her organisation back on the straight and narrow are surely an effective tool; after all, which data protection officer wants to have to tell the person that may decide his or her future career path that the organisation is being publicly admonished and ask that person to sign the undertaking so that the ICO can get on with issuing its press release? And if the boss's answer is "no" then the poor data protection officer's may then need to be "please can you sign this company cheque for up to £500,000 and is there anything you would like to say in the organisation's press release responding to the publicly issued fine"?

Following a survey which found that businesses say they take data protection seriously but that the general public remains unconvinced, the information commissioner was recently quoted as saying: "Companies need to consider the damage that can be done to a brand's reputation when data is not handled properly. Customers will turn away from brands that let them down." Very few well-meaning businesses would disagree with that statement; the information commissioner is making clear that he will not shy away from using that fact to his office's advantage.

So, a regulator without teeth? Not in my opinion. The ICO is maturing in its approach to enforcement, supporting responsible organisations that just get it wrong despite their best efforts and chastising those who have not taken enough care to try to get it right in the first place. And for those who would steal personal data for their personal gain? I think we can assume that they may soon be facing the threat of a stay in one of Her Majesty's less salubrious hotels. NLJ

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