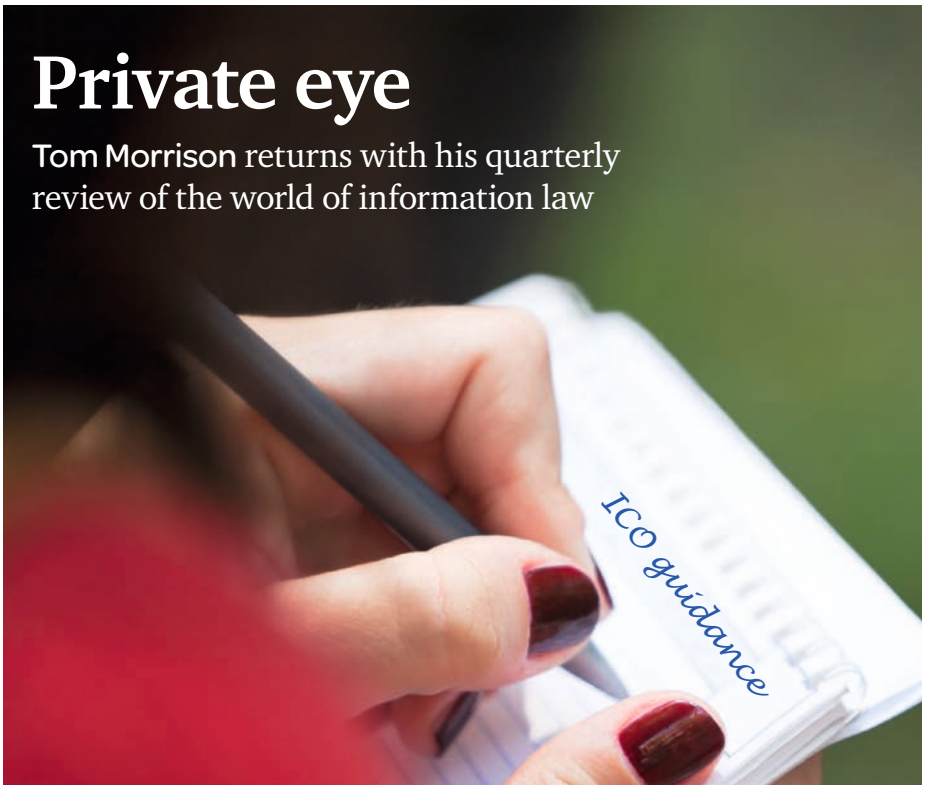
Private eye

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



© iStock/webphotographeer

IN BRIEF

- ICO publishes guidance for the media.
- MoJ at the wrong end of enforcement action.
- Lawyers warned to take extra care.
- DPA 1998 in an electronic world.

The summer can be a slow season for news, but somehow information law seems to keep finding a way of getting itself in the headlines. This season the sun has shone its light on democracy. I am not referring to the energetic and heartfelt campaigns fought in support of both sides of the debate on Scotland's place in the Union. I am referring to those who report on such campaigns, to those who support the legal system upon which our democracy was built and those who enforce the rule of law.

The press: democracy in action?

Just as the schools were going back, the Information Commissioner's Office (ICO) published guidance for the attention of all of those who work in the media, together with advice for individuals who feel that their information has not been dealt with properly. The guidance was produced in response to one of Lord Leveson's recommendations and was heavily consulted upon within the industry and the public at large. The ICO's response to those consultations was published at the same time.

The aim is to give journalists and others working for news organisations a tool to help them understand what the Data Protection Act 1998 (DPA1998) requires of them. The ICO, and more accurately the Information Commissioner within whom the Office's power sits and who used to be a journalist himself, is not out to annihilate freedom of the press. The ICO is after all the enforcer of the public's right to know as a result of its freedom of information remit. At the same time there is an expectation that the media will play by the rules our society has set on the protection of individuals.

Striking a balance between freedom of expression, the public's right to know, and the individual's right to privacy is never going to be a simple task. The ICO acknowledged immediately on publication that the guidance will not be universally supported as there are those that feel that the current law on data protection is too generous in the protection it affords some individuals who might not deserve it, while others argue that the press can already lawfully intrude too far into people's private lives. Given that broad spectrum of opinion, the guidance was never going to be capable of being popular, but that is not what it should be. What it should be is an attempt to explain the practical impact of the law upon the media industry and upon those affected by the work of the media so that they have a better chance of striking what our society considers to be the right balance as determined by its legislators.

Speaking of the legislators...

Moving from those that strengthen our democracy through their reporting to those that guard it by virtue of their role in our system of justice, it is no doubt with a degree of schadenfreude that some will have read that the Ministry of Justice (MoJ) was recently on the wrong end of enforcement action from a public body for which it is the sponsoring government department. The ICO demonstrated its independence when it slapped the MoJ with a £180,000 fine as a result of what it described as serious failings in the way prisons in England and Wales had been handling prisoners' information. Two portable computer hard drives have gone missing in the past three years, containing details of nearly 20,000 prisoners. Neither was encrypted.

The particularly galling aspect of this story is that, after the first loss, the prison service provided its prisons with new hard drives capable of encryption but the prison responsible for the second loss had not appreciated that it needed to turn on the encryption function for it to work. The ICO was highly critical of the MoJ for not properly training those using the hard drives in their safe use. Unsurprisingly, the MoJ has now made sure that all of the hard drives being used by prisons are securely encrypted. Nobody can argue that the government department charged with protecting the public must be held to the highest standards and so this case reminds us that nobody is beyond reach—and that all portable hard drives containing personal information should be encrypted.

Data protection matters for lawyers too

It was a sad day for my own profession when a paralegal who had previously worked at a law firm was prosecuted under s 55 of the DPA1998 for illegally taking the sensitive information of some of its clients before leaving to join a rival firm. He had sent the information in a number of e-mails with the intention of using it in his new role.

He will be far from the only person moving to a new job—lawyer or otherwise—who has taken some of the tools he might think are his to take, with the intention that it will he will use them in his new role. New employees who are keen to impress might be afraid of failing, but this case is a stark reminder that taking information about people is a crime. Such is the seriousness of the issues that the ICO used this case to remind the public that it remains dissatisfied with the fact that such crimes are not punishable with custodial sentences.

Equally, taking other non-personal information could still be a serious matter of breach of confidence which can have serious professional ramifications for solicitors for example. Theft of client contacts and copying of materials in which the former employer owns copyright are also all too common and often but erroneously seen as fair game.

Wider data protection risks for the legal profession

Fifteen data protection incidents involving members of the legal profession were reported to the ICO over a three-month period during the summer. While this might not seem like a huge number it is worrying. If a solicitor or a barrister is in possession of someone's information then by necessity it will be for a reason. The chances must be higher than for other data controllers that the nature of the damage resulting from any accidental disclosure, loss or destruction of information held by them will make a fine more likely. When you add to that the fact that lawyers often require access to large amounts of information when advising their clients, the risks just keep climbing.

In order to try to help members of the legal profession reduce the risk of a potentially career-ending (and as a minimum reputation-damaging) blunder, the ICO has published some tips on how to keep information secure. They sound basic, but for any lawyers reading this ask yourself if you or a colleague has ever done any of the following:

- Left files in a car?
- Taken home more papers than needed "just in case"?
- Sent work to a home e-mail address—and without being encrypted?
- Left information on a home computer or in a drawer after a matter has been dealt with?
- Disposed of an old computer without being certain that any information on the hard drive has been permanently erased (if you have just hit delete then you fall into this category)?

Now is the time for every lawyer to revisit his or her own ways of working and to ensure that the firm is taking these issues seriously.

And in other news...

While all of the above involve some pretty big and serious themes, there has been a lot going on in the summer months at a more detailed level. Much of this has involved better educating the public on how an Act of Parliament drafted in 1998 has direct relevance to the electronic world we live in over 15 years later.

The wonderfully named "Internet of Things" describes the fact that an increasing number of gadgets are connected over the Internet. That I might be able to use my smart phone to turn up my heating to ensure a warmer welcome when I get home does not strike me immediately as a data protection issue but when you start to aggregate that with the many different ways we consume and interact with content from smart TVs and tablets, and you understand that your water meter is being read from a different continent and your living room lamp can flash blue when your football team scores a goal, then it starts to get interesting.

Linked to this is a survey of over 1,200 mobile apps by privacy regulators from across the globe, showing that a large number make use of our personal information without clearly telling us that this is the case. The Global Privacy Enforcement Network, which undertook the survey, found that 85% of the apps surveyed failed to clearly explain how they were collecting, using and disclosing personal information. It was not all bad news, though. The best apps contained basic notices with the key points on how information is used, with links to delve deeper.

Many apps make good use of technology by issuing instant notifications at the moment the app is about to collect or use information. There has to be a balance though. While knowledge is power, I really do not want my satnav asking me if I am happy for it to know where it is when I ask it to show me the way home. **NLJ**

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