Data protection

Private eye

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

IN BRIEF

- All mobile devices should be encrypted.
- The ICO's publication of guidance and fining activity continues apace.
- Google just cannot escape that data protection spotlight.

The Information Commissioner's Office (ICO) has again made clear that it is not optional to encrypt personal data held on any portable storage device. Nevertheless, many businesses, charities and public sector organisations are either deliberately or unwittingly allowing the continued use of unencrypted devices. It would be a bit of a pun to say that encryption is key to data security, but it has for some time been clear that it is likely that you will be found to be in breach of principle seven of the Data Protection Act 1998 if you lose an unencrypted device containing personal data. Unfortunately, Greater Manchester Police (GMP) was reminded of that by finding itself on the wrong end of a £150,000 fine.

Based on the reported facts, it was a bit of a slam dunk for the ICO. A drugs squad detective took a memory stick home and kept it safe in his wallet. Sadly, his home was broken into and his wallet—along with the memory stick—was stolen. The memory stick contained details of 1,075 individuals with links to serious crime investigations over an 11-year period. In the words of the ICO's director of data protection, David Smith: "The consequences of this type of breach really do send a shiver down the spine." You know when the ICO says something like that it is going to be accompanied by a large number with a pound sign next to it.

The data was not encrypted, meaning that anyone with a computer would be able to read its contents. There was a very real concern that in the wrong hands the data could cause some individuals serious—and possibly physical—harm. This is not the first such incident for GMP: following a similar security breach in September 2010 it failed to make sure that only encrypted memory sticks were used and did not provide adequate data protection training to employees, although since this latest case, over 1,000 memory sticks were handed in by staff as part of an amnesty exercise.

The ICO has made no secret that it is hoping that the level of the fine will discourage others from making the same mistakes. It is in my view becoming critical for all businesses, charities and public sector organisations to encrypt any portable devices containing personal data—including smart phones, memory sticks, tablets and laptops—to mitigate the risk of a substantial fine should the device be lost. Other questions those charged with data protection law compliance should ask themselves are:

- What information is being copied from central IT systems and does it really need to be taken off premises? If it does, what mechanisms beyond a written policy have you put in place to make sure rules are followed?
- Have you disabled data transmission through computer USB ports and do you have software in place to track unusual movements of data off your network?
- Have you provided your workforce with secure means of accessing data remotely such that the data itself remains safely tucked away in a central location and the portable device merely acts as a portal to let you see what is there, rather than staff carrying the crown jewels around with them?

Remember also that there are other sources of risk—Welcome Financial Services Limited was recently fined £150,000 following the loss of two unencrypted backup tapes. Any data that goes off site should be looked at in the same way and kept encrypted.

Five salutary tales

While the ICO has made clear that it will not issue fines that send any data controller into insolvency, a charity will not escape punishment by virtue of its status. One of the social workers at social care charity, Norwood Ravenswood Limited, left highly sensitive care reports relating to four young children outside the home of the children's prospective adoptive parents. The reports went missing. The social worker had not received data protection training, in contravention of the charity's policy. In issuing a £70,000 fine, the ICO made clear that while it does not want to be fining charities, it has no choice when faced with facts such as these. Many charities by their nature handle particularly sensitive information and are therefore potentially at greater risk if something goes wrong.

Scottish Borders Council engaged an outsourcing company to digitise some records, but did not obtain security warranties. This came back to bite them when some of its former employees' pension records were discovered in an over-filled paper recycling bank in a supermarket car park. That led to the council being fined £250,000. This is a stark reminder that if your organisation engages a third party to process data on its behalf, it is your organisation—not the processor—which is on the hook for a fine. You should make sure that you have a written contract in place setting out how the data is processed, requiring appropriate security measures to be maintained and restricting the ability of the outsourcer to send information abroad. Once the contract is

in force you will then need to monitor the outsourcer's compliance.

St George's Healthcare NHS Trust was fined £60,000 when it sent a vulnerable individual's medical details to a previous home address. A month earlier, Belfast Health and Social Care Trust received a £225,000 fine for leaving medical records, x-rays, scans, lab results and staff records in a disused hospital which was then broken into. Many of the records should have been destroyed years earlier in accordance with the trust's data retention policy. Torbay Care Trust was fined £175,000 after the sensitive details of over 1,000 employees were accidentally published in a spreadsheet on the trust's website. The data covered the equality and diversity responses of 1,373 staff and included names, dates of birth and National Insurance numbers, along with sensitive information about the person's religion and sexuality. Not a good quarter for the health sector.

Surveillance society

It came as a surprise to many when it was reported that Southampton City Council had been ordered to stop the mandatory recording of all conversations in the city's taxis. Not a surprise that it had been ordered to stop, but a surprise that the recording was taking place at all. The taxis also have CCTV systems, but it was the audio recording that was deemed to be particularly intrusive and disproportionate. Echoing the advice in the ICO's CCTV Code of Practice, images should only be recorded where it is clearly justifiable and audio recordings should be a rarity.

ICO releases industry guidance

The ICO's role is to promote good practice as well as to punish. A flurry of guides and offers of help have been issued recently. A data protection "check-up" for charities by way of a one-day advisory visit is on offer. Some may be reluctant to take up an offer from the same regulator that can issue substantial fines, but equally it will not serve any charity well to bury its head in light of recent cases such as Norwood. The consequences of something going wrong can be severe for a charity, but catastrophic for individuals. A report has also been issued following a survey of 400 schools highlighting areas of risk and offering "top tips", as well as an IT security guide for small businesses. There is heavy emphasis on the fact that data protection compliance should be used to gain a competitive advantage—to demonstrate that your organisation is most trustworthy—and not simply be seen as a legislative requirement.

Vexatious FOI request?

In *Pringle v Information Commissioner and Bury Council* (Case No EA/2012/0062), the information tribunal looked at the issue of vexatious requests for information under the Freedom of Information Act 2000 (FIA 2000). The council sought "critical friends" regarding its plans for a neighbourhood, but felt that some of the respondents were going too far. A number of requests for information were submitted and one made by Mr Pringle was refused on the ground that it was vexatious. The ICO agreed but the tribunal took a different view, finding that the council was too hasty to aggregate Pringle's single (albeit lengthy) request with the many requests received from a campaign group. The tribunal felt that the request had been too lightly characterised as vexatious, particularly in light of the original request for criticism. The irony is that it may now make public authorities less inclined to seek open debate now they realise that such a call may make it harder to argue the vexatious exemption.

Correspondence with the future King

The Attorney General (AG) has stepped in to block the release of letters sent by the Prince of Wales to a number of government departments following a request under FIA 2000. The letters formed, according to the AG, part of the prince's "preparations for kingship", enabling him to engage with the government of the day. The courts took a different view, feeling that the public interest lies in transparency, but the AG has used his statutory power of veto in what he describes as an exceptional case given the prince's unique constitutional role. Others argue that if our future King is lobbying the government to take particular courses of action, the public has a right to know.

Google back in the spotlight

Google continues to find itself in the data protection spotlight. France's equivalent to the ICO—the CNIL—has written to Google on behalf of all EU data protection regulators, citing concerns about how the internet search giant handles users' information. In particular, Google is combining data gathered about users from across its platforms such as YouTube and Gmail to help it better target advertising. The regulators feel that Google is providing users with insufficient information about how their data is used. Litigation is threatened if the measures set out in the CNIL's letter—such as obtaining users' explicit consent—are not taken in the next few months. Google's position is that its privacy policy, which was revised in March 2012, complies with the law.

In the previous edition of this column we also looked at the ICO's reopening of its investigation into Google's collection of WiFi data by its StreetView cars. Since then, Google has confirmed that it has erroneously retained some of the data collected. This looks to be in breach of the undertaking it gave in November 2010. The ICO has now required that all such data is handed over for forensic analysis and Google has committed to continue its cooperation with the ICO. Not that it has much choice. NLJ

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