Data protection / FOI

Private eye

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

Photo: © istockphoto.com

IN BRIEF

- The largest monetary penalty notice to date has been issued by the Information Commissioner & is set to be appealed. The fine of £325,000 has been imposed following loss by an NHS trust of hard drives containing patient & staff data which subsequently were offered for sale on eBay.
- The new cookies law is now being enforced, following the release of updated guidance from the Information Commissioner's Office (ICO).
- Google's WiFi data collection is back in the spotlight as the ICO reopens its investigation & Google potentially faces a £500,000 fine.

Brighton and Sussex University Hospitals NHS Trust has been handed the largest civil monetary penalty issued so far under the Data Protection Act 1998 (DPA 1998). At £325,000, this substantial fine was issued following the theft of computer hard drives containing confidential information relating to thousands of patients and staff in September 2010. Highly sensitive personal data was found on hard drives sold on eBay two months later. The data included details of patients' medical conditions and treatment, disability living allowance forms and reports on children. It also included documents containing staff details such as National Insurance numbers, home addresses and information referring to criminal convictions and suspected offences.

Source of the information breach

It seems that the source of the breach was an individual engaged by the trust's IT services provider which was supposed to securely destroy approximately 1,000 hard drives held in a secure room at Brighton General Hospital. Four of those hard drives made their way onto eBay and were sold to a data recovery company. Following an initial investigation, the Information Commissioner's Office (ICO) said that the trust had given assurances that no more hard drives were affected, but a university contacted the ICO several months later to say that one of its students had purchased hard drives containing data which belonged to the trust.

It is not clear how the hard drives came to leave the hospital, but they clearly did. The ICO found there to be inadequate data processor arrangements in place between the trust and its IT services provider, and the IT services provider had subcontracted the hard drive destruction work to a third party in circumstances where the trust had not imposed any prohibition on subcontracting imposed by the trust or a requirement on the provider to obtain the trust's consent to sub-contracting. Whatever explanations the trust has given it has clearly not satisfied the ICO, and the deputy commissioner and director of data protection David Smith has made no secret of the fact that the ICO intended to make an example of the trust with the level of this fine, saying that "the trust failed significantly in its duty to its patients, and also to its staff". The trust has committed to provide a secure central store for hard drives and other media, review its process for vetting potential IT suppliers, obtain the services of a fully accredited ISO 27001 IT waste disposal company and make progress towards central network access.

While clearly a significant milestone in data protection enforcement, it would be wrong to say that this is the largest fine ever issued for a data loss—there have been much larger fines issued to the banking sector under their own rules—but this is the largest by far pursuant to the ICO's power under the DPA 1998 to fine without taking the alleged wrongdoer to court.

Significantly, it is clear from quotes which have been published in the press that the trust disagrees with the assessment made by the ICO and views the fine as unduly harsh. It is understood that the trust is going to appeal the fine, which it says it cannot afford, and denies that it was reckless in its actions. It has promised to lodge an appeal against the fine, which will be the first time the ICO's decision in relation to a fine has been challenged. The ICO took some time to finalise the level of the fine, has made strong public statements in support of its decision and has issued a very detailed decision notice, so it will be interesting to see the outcome of the appeal. In the meantime, the case serves as a timely reminder for all data controllers to make sure that they have appropriate written arrangements in place with their data processors and that those arrangements are vetted. This case also neatly illustrates the fact that a data controller remains liable for its data processors' breaches and so appropriate indemnities should be sought in the data processing agreement which will at least reimburse the cost of any fine.

Cookies

Just over a year ago, data protection lawyers across the country had great fun amusing readers with headline-grabbing puns on the word "cookie".

Twelve months later authors are again scraping the bottom of the tin looking for a crumb of novelty to give their articles a catchy headline. Not this author though.

This time around the news is that what we said a year ago would be enforced in a year's time will now be enforced. So while that does not seem at first sight to be particularly newsworthy there are some points to note, namely:

(i) Having allowed for such a long lead-in period, the ICO will not be impressed with anyone operating a website who has not made at least some attempt to identify what cookies their website is using, assess what impact that may have on users' privacy and explain the findings to users.

(ii) The ICO has updated its previous guidance on compliance with the new regime. The crux of the issue is whether or not positive opt-in consent has to be obtained from users prior to planting or reading a cookie. If read literally, the new legislation does require this, but the ICO seems to have relaxed its position on implied consent at least for the most common types of cookies that are not particularly invasive. The updated guidance states that "implied consent has always been a reasonable proposition in the context of data protection law and privacy regulation and it remains so in the context of storage of information or access to information using cookies and similar devices". This is a welcome clarification when compared with the earlier draft of the guidance, but it does still leave the issue of the processing of sensitive personal data where implied consent on its own will not be sufficient. Most importantly, any website operator seeking to rely on implied consent still needs to provide sufficient information to users in a manner that enables them to make an informed decision.

(iii) The ICO's pragmatic approach to the issue of implied consent reflects the reality that the UK is already ahead of much of the rest of Europe in trying to comply with the new legislation, while not disadvantaging UK businesses by making their websites implement awkward and aesthetically displeasing consent-collection tools.

(iv) There is an enforcement mechanism to back up the new legislative requirements along the same lines as for other data protection breaches, although it is hard to imagine many circumstances where failure to comply with the new cookies laws will result in fines being issued unless there is some other serious wrongdoing associated with it.

(v) The new regime does not apply solely to the use of cookies; it applies to all website-tracking technologies. The problem is that more people have heard of a cookie and it is hard to think of a pun for any other type of tracking technology.

> "The problem is that more people have heard of a cookie & it is hard to think of a pun for any other type of tracking technology"

Google back in the spotlight

Google has been at the centre of numerous privacy concerns over recent years. Some will say that this is because the search engine giant does not take privacy seriously, but others would argue that they are pushing at the boundaries of what is possible. Street View was at the leading edge of mapping technology and its use today has become second nature to many of its users. While the early concerns about Street View revolved around being able to identify individuals should the face-blurring technology fail, it later became clear that the cars which roamed the country collecting images of streets also collected information from WiFi networks.

This is not news; it has been known about for some time. Google had perhaps hoped that the controversy had died down, having assured the ICO that any data collection was inadvertent. The ICO surprised many by the relatively low level of formal enforcement action taken against Google once it became clear that Google had been harvesting WiFi data from unsecured WiFi routers. An undertaking was ultimately sought confirming that Google would take steps to make sure similar breaches did not happen again and the company submitted itself to a privacy audit, but no fine was issued.

The ICO has so far stood accused by the media of not investing sufficient resource into identifying what Google actually did with the data or how it came to collect it. In its defence, the ICO has been quoted as saying that it had to take into account the fact that it has limited financial resources and that there was no evidence that Google intended to use the collected data or that any individual was at risk.

Regulators in other countries, including the Federal Communications Commission (FCC) in the US, uncovered much more controversial facts than those found by the ICO. As a result, the ICO announced in the second week of June 2012 that it has reopened its investigation and has published a letter which it sent to Google. It seems that the software used to collect the data was specifically written for that purpose and that the software engineer in question had flagged this with Google. The ICO has now surmised that it seems likely that, contrary to its previous impression, Google collected this information deliberately. Google was required to respond to seven specific questions clearly aimed at flushing out exactly what Google knew about the data collection software, and at what points in time, in order that the ICO can ascertain whether it was misled in its earlier investigation.

In the face of criticism following its earlier investigation, the Information Commissioner Christopher Graham promised that "Google will not be filed and forgotten by the ICO." The ICO is coming under some considerable pressure to come up with the goods this time. It is fair to say that there was a widespread feeling that Google got off lightly the first time around; a different outcome seems more likely on this occasion. NLJ

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