

## Unscrubbed Hard Drives Report

### **Background**

In December 2010, the ICO engaged an independent computer forensics company (NCC Group) to purchase and analyse approximately 200 hard disk drives, 20 memory sticks and 10 mobile telephones. These were bought from a variety of sources with most coming from online auction sites.

NCC first examined the drives using no additional software to see what information was immediately evident. The drives were then studied using forensic tools which were freely available on the internet. This was carried out to replicate the attempts which more knowledgeable individuals may make to try and recover data for improper usage.

Following completion of this exercise, NCC provided the ICO with a final report detailing its findings, along with a brief summary of what, if anything, was found on each drive. Copies of the 'imaged' drives were also provided to the ICO so that further investigations could be carried out.

### **NCC Findings**

Negligible personal data was found on the memory sticks and mobile telephones. In the case of hard drives:

- 38% of the devices had been wiped of data
- 14% were damaged/ unreadable
- 37% contained non-personal data
- 11% contained personal data

In total, some 34,000 files were found containing personal or corporate information. NCC was pleasantly surprised to find that in the case of bulk purchases, most vendors had taken steps to securely erase the data. However, there were concerns about the amount of data found on many of the individually purchased drives. Although some action had been taken in a number of cases (such as deleting drive partitions) this was not enough to ensure that the personal data was unrecoverable.

Upon further ICO examination, it became clear that at least six of the drives contained significant amounts of personal data. These drives are

likely to have originated from desktop machines and can be split into two main categories:

- i) Devices containing comprehensive personal data relating to the owner/ main user of the drive (2 drives);
- ii) Devices containing comprehensive personal data relating to employees or clients of organisations (4 drives). These drives were either personally or corporately owned, and in some cases, it transpired that unauthorised home working had been taking place.

In the first category, the documents included information about business ventures, copy passports/ birth certificates, bank statements, scans of bills/ invoices, payslips, CVs, job application forms, details of motoring offences/ convictions, some medical details, personal relationship information, family photos, tax information and job performance reviews. There is likely to have been more than enough information on both the identified drives to enable a third party to carry out an identity theft.

In the second category, personal and sensitive personal data featured in detailed reports, photographs, spreadsheets, job application forms, references, copy passports/ birth certificates/ driving licences, CVs, tax forms, enhanced disclosure forms, and residence permits. Health information and full bank details were also found. In this category, all four identified organisations were contacted by the ICO for an explanation of how the situation occurred and what measures had been put in place to ensure something similar could not happen again.

## **Conclusions**

The ICO has now been assured by the organisations contacted as a result of this exercise, that they have since put sufficient remedial measures in place to prevent a similar situation recurring. However, an Undertaking has been obtained from a private company committing it to improve the security of its drive decommissioning process moving forward.

Despite the commitments made by these four data controllers, there is still an ongoing concern that other organisations and individuals may be disposing of redundant IT equipment in an insecure manner. In many cases, this will be due to a general lack of technical awareness, on which the ICO will continue to provide guidance.