

After Soham

Marcus Turle of Field Fisher Waterhouse discusses data retention and vetting following the conviction of Ian Huntley for the Soham murders

In the aftermath of Ian Huntley's conviction for the murder of Soham schoolgirls Holly Wells and Jessica Chapman it has become clear there were serious flaws in the vetting and data retention procedures employed by the police in Humberside and Cambridgeshire. The case is a stark and salutary reminder that employers must think carefully about their own data retention and vetting procedures.

Employment vetting is a notoriously tricky business. While there is obvious concern to avoid 'putting the paedophile in charge of the playgroup' so to speak, is it fair to deprive someone of a position merely because of unproven allegations? For that matter, should organisations even bother to keep records of allegations which are never proven, and if they do, can these be included in records used for vetting? Are there any guidelines for this?

As is so often the case in matters of data protection, the short answer is that, except in cases which are blindingly obvious, the law is so vague that it is almost impossible for the lay person to make decisions with confidence. And as the Bichard Inquiry – set up following Huntley's conviction to investigate the vetting and intelligence procedures employed by Humberside and

Cambridgeshire police – has shown, even where guidelines do exist, critical flaws in the system can still be catastrophic.

Systematic failures

We now know that Huntley had targeted young girls in Grimsby from the mid-1990s. Social services looked into four separate complaints of underage sex – in one case with a girl of just 13 – and an allegation of indecent assault on a 10-year-old. No one at social services linked the cases together – they were handled by four different teams of social workers in different parts of Grimsby, and their files focused on victims not perpetrators.

The police were involved in all but one of these cases, and also investigated three separate claims by women who said Huntley had raped them. But in none of the cases was Huntley convicted. Humberside police interviewed him on a number of occasions, but because of their policy of weeding computer records monthly, vital information was thrown away and no one realised he had a string of past allegations against him – except for a lone Humberside constable who warned in a report in July 1999, after he spotted that Huntley had been linked with four separate rape allegations, that he was a 'serial sex attacker'. The report was passed to

'Data protection law is so vague that it is almost impossible for the lay person to make decisions with confidence.'

intelligence officers in the former school caretaker's native north-east, but was later deleted from a computerised local intelligence file. By the time Huntley was vetted for the school caretaker's job in Soham, the officer's report would not have shown up.

The Bichard Inquiry

David Westwood, the chief constable of Humberside Police, claimed in a *Newsnight* interview before the start of the Bichard Inquiry that his force had been obliged to delete the nine sexual allegations made against Huntley because of the requirements of the Data Protection Act 1998 (DPA). He subsequently apologised for this when giving evidence at the Inquiry, admitting, 'I misinterpreted the advice I was given [from Deputy Information Commissioner David Smith] and I got it wrong'.

The Bichard Inquiry is due to report at the end of May, and will reconvene six months after that to review the progress which has been made in implementing its recommendations. The author will himself be reporting on the Inquiry's findings in this journal. In the meantime, what should employers be doing to comply with the law?

Data Protection Act rules

The overriding principle in the DPA is that all 'personal data' (ie data relating to an identifiable living individual) must be processed 'fairly and lawfully'. Data should also only be held and used for limited purposes, and should not be kept for longer than necessary.

Information regarding an individual's criminal record, and information concerning allegations which are not proven, is classified in the DPA as 'sensitive' personal data. A further set of rules apply to this kind of information (in addition to the general principles mentioned above). While

retention of information about unproven allegations must be 'lawful' and 'fair', and not kept for longer than necessary, anyone can hold this kind of data where necessary:

- to protect the vital interests of the data subject or another person;
- in connection with legal proceedings (including prospective legal proceedings); or
- for the exercise of any functions conferred on any person by any enactment.

The Data Protection (Processing of Sensitive Personal Data) Order 2000 also permits the holding and use of this kind of sensitive data where necessary:

- in the public interest;
- for the purposes of prevention or detection of any unlawful act; or
- for the exercise of functions conferred on any person by any rule of law.

The trick is how to interpret and apply these rules in a way which meets the requirements of the law, but also allows you to run your organisation efficiently and effectively from day to day. Humberside Police did still have the records of allegations made against Huntley, but only in paper form. They do not consult their paper records for vetting because to do so would take months for every single enquiry.

On the question of retaining records for employment vetting, there is the general principle on the one hand of not keeping data for longer than necessary, and the specific allowances on the other for disclosing details of convictions or unproven allegations where 'necessary' for the various reasons described above.

The Information Commissioner recently indicated that:

It's for the police to decide what purposes they're holding information for, and as long as they are holding it for legitimate purposes, such as the investigation or prevention of crime, they can hold information in some cases for a very long time indeed.

Clearly there are compelling arguments for holding data relating to allegations of underage sex, rape or indecent assault for an unlimited period of time. Modern forensic techniques and DNA analysis can lead to the arrest of a suspect long after the event. On this basis, Humberside's practice of deleting data every month was clearly erroneous.

The ACPO code of practice

The police's own industry guidelines also contradict the arguments put forward by Humberside's Chief Constable on *Newsnight*. The Association of Chief Police Officers (ACPO) code of practice for data protection – issued with the support of the Information Commissioner in October 2002 – seems clear. While police forces have a duty 'to ensure that personal information is periodically reviewed and information that is no longer required is removed', and 'information should not be retained on the grounds that it may possibly become relevant in the future', the Code does permit retention for five years where a sexual offence is alleged, even if the suspect is acquitted or the case is discontinued because of lack of evidence. This can be extended where the circumstances of the allegation would give cause for concern if the individual applied for employment involving substantial access to vulnerable persons.

However, ACPO has recently been subject to enforcement action by the Information Commissioner for 'over-retention of conviction data', so it seems even their guidelines are not free of controversy.

The employers' code of practice

Employers can look for help in Part 2 of the Employment Practices Data Protection Code, which develops and applies the DPA in the context of employment. In relation to pre-employment vetting, the Code recommends:

- doing it only where there are particular and significant risks to the employer, its clients, customers or others, and where there is no less intrusive and reasonably practicable alternative;
- doing it at an appropriate point in the recruitment process (so, for example,

comprehensive vetting should only be conducted on a successful applicant);

- making it clear early in the recruitment process that vetting will take place and explaining how it will be done;
- using it only to obtain specific confirmation;
- seeking information only from sources where it is likely the information will be revealed;
- allowing the applicant to make representations about information which will affect the employer's final decision whether or not to appoint; and
- where it is necessary to obtain release of documents or information from a third party, getting a signed consent from the candidate.

As the Criminal Records Bureau is now operational employers must also, in appropriate circumstances, check whether a candidate has a criminal record.

In relation to data retention, the DPA does not override statutory requirements to keep records, for example for the purposes of working time, minimum wage, statutory sick pay or PAYE. While the original draft of the Code contained guideline retention times for different categories of data, the final version only provides guidance for employers on developing a practice of standard retention times based on actual rather than theoretical need, leaving employers to make their own decisions. It might be sensible to retain basic employment details, such as names, dates of birth, dates of employment and national insurance numbers, indefinitely. As far as other records are concerned, an employer must balance the risk of a future claim against the cost of the administration involved in retaining records, and the possibility of an enforcement action or a claim for damages under the DPA.

Opinion on these difficult issues is far from settled, and the author looks forward to reporting again once the Richard Enquiry has published its findings.

Marcus Turle is a solicitor in the privacy and information law unit at Field Fisher Waterhouse. He can be contacted at Marcus.Turle@ffw.com.