

After Bichard

Marcus Turle of Field Fisher Waterhouse reports on the consequences of the Home Office inquiry into the Ian Huntley case

The last article in this series looked at the vague yet complex legal framework regulating the retention of information about someone's criminal record, and information relating to allegations which are never proven. It concluded that, while there is little guidance on how the law applies in particular cases, the Data Protection Act (DPA) appears to give employers considerable leeway when making decisions about data retention, albeit within the parameters set out in the legislation.

That article was written just as the Bichard Inquiry completed its evidence-gathering. Set up by David Blunkett last December to examine the intelligence-based record keeping of Humberside and Cambridgeshire police following Ian Huntley's murder convictions, the Inquiry has now published its report. Issues relating to information handling, data retention and employment vetting lie at the heart of its findings, and the Report makes some specific recommendations which, although focused on the police and social services, have application across the whole public sector.

Findings and recommendations

Sir Michael Bichard's key findings are as follows:

- No one identified Huntley's behaviour pattern, despite nine contacts with the police involving allegations of sexual offences between August 1995 and July 1999. The main reasons for this were case management systems which conducted cases in isolation, and poor sharing of information, both between police forces and the police and social services. Indeed, social services failed to share any information with the police (taking no action and raising no concerns at all) about three allegations that Huntley had had sex with 15-year-old girls.
- Humberside's Chief Constable admitted in his evidence to the Inquiry that there were 'systematic and corporate' failures in the way Humberside Police managed their intelligence systems. As a result, Huntley's history did not come to light when he applied for the Soham job.
- No integrated IT system exists for recording and sharing intelligence across the 43 police forces in England and Wales. Indeed, Sir Michael states in his findings that 'the importance everyone concerned professes to give intelligence was not borne out in reality'.
- The DPA was not to blame for information about Huntley's past not being available to officers in December 2001. Nevertheless, officers were not comfortable working with the legislation and too little was done to educate and reassure them about its impact.
- Soham Village College did not adequately check Huntley's employment history and should not have accepted the five (unreliable) open references he provided. The College used an outside company to verify Huntley's particulars, but the company did not check them all.

The Report makes 31 recommendations, of which two are particularly interesting:

- The need for a national code of practice to cover record creation, review, retention, deletion and information-sharing by the police, which is easily understood and uniformly applied across local forces.
- Better procedures for vetting those applying for posts involving work with children and vulnerable adults, and a compulsory registration scheme for those who wish to work with vulnerable people.

Code of Practice for Information Handling

The Bichard Report makes clear what those of us who specialise in privacy and information law have known all along – the DPA was not to blame for information handling errors within the police. It does, however, acknowledge the point made in the previous article – that the law is so difficult to work with that it is almost impossible for non-specialists to make decisions about data protection with confidence.

Bichard recognises a critical absence of clear guidance and training about what information the police should retain, in what format, for what purposes and for how long. This finding could equally apply to many other areas of the public sector. If blame for this falls anywhere, it falls on those whose job it is to make sure the law works – principally the Information Commissioner, the UK's data protection watchdog. The Report recommends guidance on the collection, retention, deletion, use and sharing of information 'so that police officers, social workers and other professionals can feel more confident using information properly'.

The Information Commissioner is now due to meet with the Home Office and various other bodies responsible for regulating the police to come up with

workable guidelines for information handling. A number of points made in evidence to the Inquiry provide useful indicators of the Commissioner's views on what he thinks we should all be doing and how he intends to fulfil his own remit:

- He confirmed the author's view that there is considerable latitude about organisations' policies on the retention and disclosure of records (provided, obviously, that policies are based on the data protection principles and, if appropriate, secondary legislation such as the Data Protection (Processing of Sensitive Personal Data) Order 2000 which permits processing of sensitive personal data to protect a person's vital interests, in connection with legal proceedings or prospective legal proceedings, in the public interest, or for preventing or detecting crime).
- Generally, questions about the retention of data will be less controversial than questions about disclosure – policies on retention will therefore usually be less susceptible to challenge.
- In relation to the police (and presumably, by extension, other specialist sectors) the people on the ground are the first judge of their operational needs and should therefore be the primary decision-makers – the Commissioner's role is to review and supervise, but his staff 'cannot and should not substitute [their] judgment for that of experienced practitioners'.
- Ultimately, if a reasonable and rational basis exists for a decision about the retention or disclosure of personal data, 'that should be the end of the story'.

Of course, for the police, there are particularly complex issues underlying retention of intelligence items. Historically, 'intelligence' (eg allegations or complaints which are not proven) has been treated differently from conviction data. Bichard suggests that this distinction needs to be re-examined for certain kinds of intelligence, principally allegations relating to sexual

offences. Huntley's history shows that information needs to be kept where there is reason to believe that it indicates a pattern of behaviour (because separate allegations are made about the same person), and by implication this means that the 'first' piece of intelligence needs to be kept for long enough to enable a pattern to emerge.

There is a substantial human rights issue in the retention of non-conviction related intelligence which is used to make employment decisions. A person suspected but never given the opportunity to defend themselves in court and never convicted of relevant crimes will effectively be denied the right to work in their chosen field. Bichard makes it clear that this needs to be balanced against the potential dangers of failing to record and share such

'Bichard makes it clear that the DPA was not to blame for information handling errors within the police.'

intelligence. The fact is, given the consequences of Huntley's employment, the balance is likely to be firmly in favour of recording and sharing the intelligence.

Vetting procedures and registration scheme

The Report makes a number of specific recommendations for the vetting of applicants for posts which involve working with children and vulnerable adults:

- all applications should be subject to the Criminal Records Bureau's enhanced disclosure regime;
- those conducting interviews with applicants should receive adequate training; and
- there should be a register introduced, perhaps supported by a card or licence, which would reassure employers that nothing is known about an applicant by the relevant agencies which would disqualify them.

The intention is that selection and recruitment should be far more robust. This can be achieved partly through CRB checks and a registration scheme, but Bichard is concerned to ensure that employers do not become over-reliant on these. Some abusers are not known to the authorities, so no amount of official checks will be fail-safe. It is therefore essential that those responsible for interviewing and appointing staff should be trained properly.

In conclusion, Bichard makes some eminently sensible recommendations. But nagging doubts remain about how these will be addressed in practice. Sir Michael intends to reconvene the Inquiry later this year to check on progress, and it will be interesting to see just how much has been

done. One suspects not a great deal. The drafting of a workable code of practice for intelligence handling which meets the requirements of the DPA and Human Rights Act, but which is also user-friendly, represents a very considerable challenge. Similarly, there is no immediate prospect of a national IT system for intelligence sharing. This has been mooted before, but it will only work if the body responsible for implementing national IT systems – PITO – is given the power (currently absent) to impose a system across 43 diverse police authorities. It is to be hoped that at least the enhanced vetting controls suggested by Bichard can be implemented effectively, although of course this will require the long-suffering CRB to get its act together. One way or the other, the potential consequences of failing to address Bichard's Report are too great to contemplate anything but effective action.

Marcus Turle is a solicitor in the Privacy and Information Law Unit at Field Fisher Waterhouse.