

Information Sharing and Local Government Timothy Pitt-Payne

INFORMATION SHARING IN 2009: AN ABANDONED REFORM PROPOSAL

1. Public authorities collect, analyse and disseminate vast amounts of personal information. In recent years this aspect of their activities has proved increasingly controversial. There are concerns as to whether an excessive amount of information is being collected, to a point where individual privacy is compromised: phrases such as “the database state” and “the surveillance society” are a commonplace of political debate. There has also been controversy about the security of information held by public authorities, thanks to a well-publicised series of data losses beginning with the reported loss of 25 million child benefit records by HMRC in November 2007.
2. At the same time, there has been a perception within Government that the legal framework governing the use of personal information by public authorities is unduly restrictive. There has been much discussion of the desirability of “information sharing” (or “data sharing”, for those of a more technical or legalistic bent). This expression has no precise definition, but in general it covers both the disclosure to one organisation of information held by another, and the use of personal information for a purpose different from that for which it was originally collected.
3. Those who advocate more extensive information sharing within the public sector do so for a variety of reasons. There are considerations of administrative efficiency: for instance, it is said that individuals ought not to be required to give the same basic personal information over and over again to different public bodies. Then it is suggested that, if information held in the public sector is pooled, the delivery of public services can be enhanced. For instance, in a speech in October 2007 the Prime Minister expressed his belief that:

a great prize of the information age is that by sharing information across the public sector – responsibly, transparently but also swiftly – we can now deliver personalised services for millions of people.

Information sharing is also appealed to as an aid to preventing crime, combating terrorism, and protecting children and vulnerable adults from the risk of abuse.

4. In October 2007 the Prime Minister announced that he had asked Richard Thomas (the then Information Commissioner) and Mark Wolpert (of the Wellcome Trust) to review the framework for

the use of personal information. Their review, published in July 2008, focused on the subject of data sharing. It attempted to move beyond what is often a highly polarised debate; the review argued that data sharing involved both benefits and risks, and could not be viewed in unequivocally positive or negative terms. It suggested that in the past Government had tended to focus in a one-sided way on the potential benefits, ignoring risks and costs; and also that there had been a tendency to endorse information sharing before considering carefully whether there was a genuine need for it. The review quoted Rosemary Jay – a leading data protection expert – as having described the Government’s vision of data sharing as being:

rather like wishing to encourage better nutrition among school children by having a “vision” of grating or peeling or some other culinary process, rather than a vision of healthier children.

5. At the same time the Review accepted that in some contexts information sharing was uncontroversial, and clearly beneficial. For instance, following the terrorist attacks on the London Underground on 7th July 2005 there was little concern about the extent of personal data sharing that ensued. To give a less dramatic example, the Review referred to information sharing between motor insurance companies, the MoT certification authority, and the DVLA, allowing vehicle tax discs to be renewed online through the DVLA’s website: this development has received widespread support.
6. The Review concluded that the relevant legal framework was complex and confusing, giving rise to considerable uncertainty. One of its main recommendations was that a new statutory fast-track procedure should be created, to be used where there was a genuine case for removing or modifying an existing legal barrier to data sharing.
7. Following the publication of the Review, in January 2009 the *Coroners and Justice Bill* was introduced in the House of Commons. Clause 152 of the Bill sought to amend the *Data Protection Act 1998* (“the DPA”) so as to facilitate information sharing. The proposal proved to be extremely controversial, with opposition from civil liberties groups, the Bar Council, and the British Medical Association. The Information Commissioner himself stated that the proposals went beyond what had been recommended in the Walport/Thomas review. In March 2009 the relevant clause¹ was withdrawn from the Bill.
8. The proposed amendments to the DPA would have allowed a Minister to make an Information Sharing Order (ISO), enabling any person to share information that consisted of or included

¹ By now it was clause 154, not 152.

personal data. An ISO could be used in order to confer powers, or to remove or modify statutory or common law obstacles to the proposed information sharing. A Minister could make an ISO if satisfied: (i) that the ISO was necessary for a policy objective of that Minister; (ii) that the effect of the ISO was proportionate; and (iii) that the ISO struck a fair balance between the public interest and the interests of any affected person. For this purpose, information sharing was to be defined as including both the disclosure of information, and its use for a purpose other than that for which it was originally obtained.

9. Critics of the proposals suggested that ISOs could be used to set aside fundamental protections for personal privacy, including the provisions of the DPA or of the Human Rights Act 1998. Following the withdrawal of the clause, no similar proposals have been put forward by Government. The fate of clause 152 shows us two things: there is a strong perception within Government that the legal regime about information sharing is unsatisfactory; and there is widespread public scepticism about ambitious proposals involving governmental use of personal information.

THE CURRENT LEGAL FRAMEWORK IN OUTLINE

10. Does the current state of the law deserve the criticisms made in the Thomas/Wolpert review?
11. There is no legislation that specifically addresses “information sharing”; indeed there is no statutory definition of the term (though the provisions of the Coroners and Justice Bill would have introduced one). Instead there is a complex legal regime governing the collection and use of personal information generally; information sharing has to be considered within that general framework.
12. Many of the relevant provisions apply to private sector data controllers as well as to the public sector. Information sharing within the private sector seems at present to be less controversial, though its implications for individuals can be profound; for instance, inaccurate information held by credit reference agencies (perhaps as a result of identity fraud) can make it impossible for individuals to obtain credit or to get a mortgage.
13. Focusing specifically on the position of local authorities, there are number of different forms of information sharing in which authorities may wish to engage. There is an important difference between sharing information between different departments of the same local authority, and sharing information with external individuals or organisations. There is also a difference between

the routine or bulk sharing of information – for instance, in order to populate a customer relations management (CRM) system, or as part of a data-matching exercise in order to detect fraud – and *ad hoc* information sharing (for instance, disclosing information to prospective employers about a suspected child-abuser). However, there are common legal issues that recur across all of these kinds of information sharing.

14. It is suggested that information sharing by local authorities needs to be assessed by reference to the following questions.

- Does the authority have the *vires* for the proposed information sharing? Information sharing proposals are usually made in connection with the performance one or more of a local authority's functions; so one obvious starting-point is to consider the provisions empowering the local authority to perform that function. It may also be necessary to consider the ancillary power in section 111 of the Local Government Act 1972, or the well-being power in section 2 of the Local Government Act 2000. In some cases there may be a specific power to share information: for instance, under section 115 of the *Crime and Disorder Act 1998*. In other cases, wide-ranging statutory powers or duties may be relied upon (e.g. the safeguarding duty under section 11 of the Children Act 2004).
- Is there any specific prohibition on the proposed information sharing? There may be a provision that prohibits local authorities from disclosing particular kinds of information, or from doing so unless specified conditions are satisfied.
- Would the information sharing breach the DPA? The DPA requires data controllers to comply with eight data protection principles in processing personal data. Local authorities will be data controllers in respect of the personal information that they hold. "Processing" includes using information, and disclosing it; so information sharing will involve the processing of personal data, and will need to comply with the data protection principles. The issues arising under the DPA are discussed in more detail below (at §15-18).
- Would the information sharing be consistent with general common law principles? Prior to the coming into force of the Human Rights Act 1998 the courts developed a principle that public authorities should only share information about individuals where there was a "pressing need" for them to do so. For instance, when the information involved suspicions that an individual had committed an offence, then whether there was a pressing need to share the information would depend on both the authority's assessment of its reliability, and the interest that the receiving body had in seeing the information. See generally *R v Chief Constable of North Wales ex parte Thorpe* [1999] QB 396; *R (on the application of Ellis) v Chief Constable of*

Essex Police [2003] EWHC 1321 (Admin). These cases gave practical effect to article 8 of the Convention, as part of English administrative law, even before the Human Rights Act 1998 (HRA 1998) came into force; hence the case-law remains relevant even after HRA 1998.

- Would the information sharing be incompatible with the right to respect for private life under article 8 of the European Convention? If so, then it is prohibited by section 6 of HRA 1998. In considering whether there would be a breach of article 8, it is necessary to consider whether the article 8(1) right to respect for private life is engaged, and if so whether any interference with that right is justified under article 8(2).
- If information is obtained on a confidential basis, then its disclosure may involve a breach of confidence. There is a potential defence, where the disclosure is in the public interest (see *Moseley v News Group Newspapers* [2008] EWHC 1777 for recent unsuccessful attempt to rely on this, in the context of a newspaper story about an individual's private life). The precise scope of the defence is unclear; but what is clear is that there is a public interest that confidences should be maintained, and hence disclosure in breach of confidence will be justified as being only if it serves some more compelling public interest. For instance, the defence might apply where a disclosure that was necessary in order to prevent serious harm to an individual, or to prevent the commission of a criminal offence.

15. Within the legal regime summarised above, the DPA needs to be considered in more detail. In the context of data sharing, it is the first and second principles that are most likely to be relevant.

16. The first principle breaks down into a number of elements.

- Personal data must be processed fairly
 - Data subjects must be given certain specified information (often referred to as "fair processing notices") about who is processing their data and the purposes for which it is being processed. This applies both when the data controller obtains the information directly from the data subject, and when he obtains it from a third party.
 - The processing must also be fair in general terms: this is obviously a very wide concept.
- Personal data must be processed lawfully. So if the processing is *ultra vires*, or in breach of confidence, or in breach of article 8, then it will also be in breach of the DPA. This means

- that the data subject will be able to make use of the remedies under the DPA (e.g. complaining to the Information Commissioner in the hope of prompting enforcement action).
- A Schedule 2 condition must be met.
 - In the case of sensitive personal data, a Schedule 3 condition must also be met. Section 2 of the Act defines what constitutes sensitive personal data.
17. Principle 2 requires that personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with those purpose(s).
18. There are however a number of exceptions to these principles. Personal data that is processed for the purpose of prevention and detection of crime, or for certain related purposes, may be exempt from the first and second data protection principle (see DPA 1998 section 29); as may data that is disclosed pursuant to a legal obligation (see DPA 1998 section 35).
19. Although the above can be made to appear bewilderingly complex, there is a considerable overlap between the different issues referred to above. In particular, questions about whether data sharing is *necessary* and *proportionate* are relevant in relation to article 8; the application of the DPA; and the administrative law principles about information sharing. These questions will lie at the heart of any assessment of legality in this area.
20. It is suggested that the following questions are likely to be of practical assistance, in considering whether any proposed information sharing is necessary and proportionate.
- What is the aim of the information sharing? The object should be defined as clearly as possible. Any potential benefits should be identified, in relation to: (i) the person who is the subject of the information; (ii) third parties; and (iii) the public in general.
 - How will the proposed information sharing contribute to achieving the aim? If the answer is that it will not, information sharing is unlikely to be justifiable.
 - How much information needs to be shared? Could the aim be achieved by sharing a more restricted set of information? In particular, could the aim be achieved without sharing information that discloses individual identities?

- How widely does the information need to be shared? This requires a careful consideration of the roles and functions of the proposed recipients, and the ways in which they could make use of the information.
- Finally, where does the balance lie between the interests of the individual and the objectives that the information sharing is intended to achieve? How serious are the potential consequences for the individual if the information is disclosed? On the other hand, how serious are the potential consequences if the information is withheld?

In considering these issues, the Information Commissioner's framework code of practice for information sharing may be of general assistance².

INFORMATION SHARING BETWEEN LOCAL AUTHORITY DEPARTMENTS

21. A number of local authorities have embarked on projects to share information systematically between their different departments.

- Some authorities have set up Customer Relationship Management (CRM) systems, containing basic information about all local residents (e.g. name and address details). This has the advantage for the local authority, and for residents, that it means that information of this kind only needs to be collected once.
- Sometimes CRM systems are used in a more ambitious way, for instance, in order to help a local authority to identify residents who would potentially benefit from a particular service but who are not currently receiving it.
- Some authorities have tried to set up a "one stop shop" whereby residents can deal with all aspects of their relationship with the authority using a single channel of communication (e.g. online, or via a call centre). For this to be workable, the person dealing with the resident on behalf of the authority needs to have access to all relevant information held by the authority.

22. The ambition behind projects of this kind is that local authorities should operate as single organisations, not as a collection of competing departmental fiefdoms (or "silos").

² http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/pinfo-framework.pdf

23. The Information Commissioner has given guidance about data protection issues regarding the sharing of information between local authority departments. The latest version is dated 30th May 2008 and is available on the Commissioner's website³.
24. The Commissioner's starting-point is that for data protection purposes a local authority is a single organisation. The data controller will be the authority itself rather than a particular department or employee. It follows that when information is passed from one department to another, but the purpose for which the information is used does not change, then the information sharing is unlikely to give rise to difficulties under the DPA: the information will be used by the same data controller, for the same purpose as before.
25. There are however potential difficulties where one department passes information to another department so that it can be used for a different purpose. The Commissioner refers to this as "secondary use" of the information. The guidance discusses the application of the first and second data protection principles to this situation. Its main recommendation is that at the point when information is obtained, fair processing notices should identify the possible secondary uses of the information.
26. One recurring source of difficulty has been the use by local authorities of Council tax records in order to populate a CRM system with basic name and address details. In the past, guidance both from the Information Commissioner's Office ("the ICO") and from central Government has taken a rather restrictive approach to the secondary use of Council Tax information. See the Guidance issued by the Data Protection Commissioner (as the ICO was then known) in May 1999; the ICO's compliance advice issued in May 2001; and the further guidance on the secondary use of Council Tax information issued by the ICO in August 2004. The DCA's Guidance *Public Sector Data Sharing, Guidance on the Law* (issued in November 2003) also takes a restrictive approach in relation to the secondary use of Council Tax information: see in particular paragraphs 3.28-3.30. The common theme of this guidance is that the secondary use of Council Tax data is likely to be *ultra vires* and hence unlawful. None of this guidance has yet been tested in the courts; and a number of practitioners have argued for a less restrictive approach.
27. The ICO has since modified its position. The most recent guidance, dated 17th January 2007, states that the ICO will not use its enforcement powers to prevent the secondary use of Council Tax data unless there is evidence of genuine unfairness or unwarranted detriment to individuals. The ICO states that it cannot provide any assurance about whether secondary use of Council Tax data would involve a local authority acting *ultra vires*; authorities should take their own legal

³ See http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/local_authorities_-_data_sharing.pdf

advice if in doubt. In other words the ICO has moved from an adverse position in relation to *vires* (i.e. that secondary use is likely to be *ultra vires*), to a more neutral position (local authorities should take their own advice). This is however coupled with an indication that the ICO will take a pragmatic approach to enforcement: to summarise, it appears that the ICO is now unlikely to take enforcement action unless it considers that secondary use of Council Tax information is causing genuine harm to individuals. This suggests that the use of Council Tax records simply to populate a CRM, and avoid a need for basic name and address details to be collected repeatedly, is unlikely to be of concern to the ICO.

28. In general the secondary use of Council Tax information gives rise to three issues:

- does a local authority have the *vires* (the legal powers) for the proposed use of the information;
- is there any legal prohibition, express or implied, on the proposed use of Council Tax information; and
- does the proposed use comply with the Data Protection Act 1998 (“DPA 1998”)?

The other recurring issues identified at §14 above are unlikely to arise; for instance, secondary use of Council Tax information in order to populate a CRM system is unlikely to give rise to issues under HRA 1998.

29. As far as *vires* issues are concerned, it is of course trite law that a local authority is a creature of statute and can only act in circumstances where it has a statutory power to do so: *R v Somerset County Council ex parte Fewings and others* [1995] 1 All ER 513, [1995] 1 WLR 1037. If the Council holds information, and uses that information for the purposes of one of its statutory functions, then the necessary *vires* will usually be provided by the statutory provisions conferring that function on the Council; together with, if necessary, the well-known incidental power in section 111 of the Local Government Act 1972 (“the 1972 Act”). Alternatively, section 2 of the Local Government Act 2000 provides a potential legal basis for establishing a CRM system and populating it in this way. In order to rely on this provision the Council would need to consider whether the proposed system would achieve any of the objects specified in section 2(1) of the 2000 Act; and it would need to have regard to the Council’s community strategy prepared under section 4 of the Act. There would need to be clear evidence that the Council had given specific

consideration to these issues: see *R (ota Risk Management Partners) v Brent London Borough Council and others* [2008] EWHC 692 (Admin) at §115-118.

30. The next question is whether there is any express or implied prohibition on the proposed use of Council Tax information. The restrictive guidance referred to at §26 above has treated Schedule 2 to the Local Government and Finance Act 1992 (“the 1992 Act”) as a complete statutory code governing the use (including secondary use) of Council Tax information. On this basis, the guidance has treated Schedule 2 as if it contained an implied prohibition on any use of Council Tax data that is not specifically provided for in Schedule 2. For this reason, the guidance has been that secondary use of Council Tax information is likely to be *ultra vires*.

31. The guidance rests on a questionable reading of Schedule 2. There is nothing in the Schedule that deals in general terms with the secondary use of Council Tax data by the local authority that collected the data. Indeed, the Schedule has very little to say about that subject. The Schedule deals with three main issues about information use, as follows:

- it provides for regulations to be made permitting the use *for Council Tax purposes* of data originally collected *for other purposes* (Schedule 2, paragraph 18);
- it provides for regulations to be made about the disclosure to third parties, for a fee, of anonymised Council Tax data (Schedule 2, paragraph 17); and
- it makes specific provision about the use of Council Tax data in identifying vacant dwellings and bringing them into use (Schedule 2, paragraph 18A).

The Schedule does not deal with the general question of whether there is any power to make secondary use of Council Tax data. Hence it is difficult to argue that the Schedule sets out a complete code for the secondary use of Council Tax information, or that it contains any implied prohibition on such secondary use. Clearly, there is no express prohibition in the Schedule.

32. The next question is whether the proposed secondary use would satisfy the requirements of DPA 1998. This requires consideration of the first and second data protection principles, summarised above.

33. Provided that the processing is *intra vires* and not expressly or impliedly prohibited (as to which see above) it would be *lawful* for the purposes of the first data protection principle.

34. As far as *fairness* is concerned, it is advisable for a suitable fair processing notice (FPN) informing residents of the proposed secondary use should be sent out *before* any new CRM system becomes operational, and for an authority to do everything reasonably possible to inform its residents of any such proposed use of their Council Tax information.
35. The first principle also requires that fairness should be considered in general terms: see e.g. *Johnson v MDU* [2006] EWHC 321 (Ch), § 114 onwards. Provided that the various steps set out above are taken, my view is that the generalised test of fairness is likely to be satisfied.
36. Would any such use of Council Tax information meet any of the conditions in Schedule 2? In my view Schedule 2 paragraph 6 is potentially relevant. The question raised by this provision is whether the processing is necessary for the Council's legitimate interests, and is not unwarranted by reason of prejudice to the data subject's rights, freedoms and legitimate interests. The provision involves a proportionality test, in which the Council's interests are balanced against any adverse effects on the data subjects. It is suggested that the use of Council Tax records to populate a CRM system is likely to satisfy this test.
37. The second DPP requires that personal data shall only be obtained for one or more specified and lawful purposes, shall not be further processed in any manner inconsistent with such purpose(s). Paragraph 5 of Part II of Schedule 1 to DPA 1998 provides that the purposes for which personal data are processed may in particular be specified in a fair processing notice, or in a notification to the Commissioner under Part III of the Act. The possible difficulty here is that, even if residents are *informed* of the proposed secondary use of Council Tax data before it is implemented, the data may well have been *collected* before they were given any such information. Arguably therefore there is a breach of the second principle.
38. However, the second principle causes difficulty only if the proposed use of the data is *incompatible* with the use for which they were originally obtained. *Incompatible* is not synonymous with *different from*: the meaning is closer to something like "incongruous with". The Information Commissioner's guidance interprets the second principle as follows:

unless a relevant exemption applies, that a local authority must not obtain personal information for one set of purposes and then use it for a completely separate and unrelated, i.e. incompatible, set of purposes.

I would suggest for example that selling Council Tax records to a commercial organisation for use in direct marketing would be incompatible with the purposes for which the information was originally collected. But using name and address details from a Council Tax database in order to populate a CRM system is, I would suggest, unlikely to be incompatible in this sense.

SHARING INFORMATION WITH EXTERNAL ORGANISATIONS

39. Sharing of information with external organisations can take a wide variety of forms. There is an important difference between systematic or bulk sharing of particular kinds of information, and *ad hoc* disclosure of information about a single specific individual; however, both are likely to involve consideration of the general issues identified at §14 above.

An example of bulk information sharing: the Audit Commission's National Fraud Initiative

40. The Audit Commission is responsible for ensuring that public money is spent economically, efficiently and effectively in the areas of local government, health, housing, community safety and fire and rescue services. Its statutory basis is the Audit Commission Act 1998, which confers wide powers for it to obtain information necessary for its audit functions.
41. Since 1996 the Audit Commission has run the National Fraud Initiative (NFI), which is a data matching exercise to help participating bodies to identify possible cases of fraud and detect and to correct any consequential under or overpayments.
42. As part of the 2007/08 NFI, the Audit Commission matched Council Tax (CT) data to other datasets, with a view to detecting fraudulent applications for Council Tax Single Persons Discount (CT SPD). As part of this exercise, the Audit Commission sought to collect Council Tax and Electoral Register data from all local authorities. The thinking behind the exercise was that if the Electoral Register showed more than one person registered at an address, but the CT data showed that there is a claim for CT SPD from one of those persons, then this was *prima facie* evidence that the claim is fraudulent. A number of local authorities were concerned about whether it was lawful for them to provide the requested information.
43. The statutory basis for the NFI has now been clarified: the *Serious Crime Act 2007* inserts new Part 2A into the Audit Commission Act 1998, giving the Audit Commission new powers to conduct data matching exercises. The legislation requires the Commission to prepare a code of practice

to govern its data matching exercises. The current Code was laid before Parliament on 21st June 2008⁴.

Ad hoc information sharing about individuals

44. This form of information sharing can give rise to acute difficulty for local authorities. They often involve issues about the disclosure of allegations of child sexual abuse, or convictions for such abuse. See the following cases by way of example.

- *R v a Local Authority in the West Midlands ex parte LM* [2000] 1 FLR 612. There were allegations that an individual had sexually abused his daughter, and another child. A local authority and a police authority disclosed the allegations to a county council with whom he had contracted to provide school transport. The allegations had been made 10 years previously and were unproved. The Court held that the disclosure was unlawful; in the circumstances, there was no “pressing need” for disclosure.
- *R (on the application of J) v West Sussex County Council* [2002] EWHC 1143 (Admin). J applied for judicial review of the local authority's decision to tell her daughter (who had children) that J's partner was a Schedule 1 offender under the Children and Young Persons Act 1933, having been convicted of indecent assault on a child in January 1999. J argued that the decision was perverse, and in breach of her article 8 right to respect for her family life. The Court held that the disclosure was justified, and dismissed the application.
- *R (on the application of C) v Waltham Forest LBC* [2002] EWHC 2007. C was formerly a teacher at a school operated by the Defendant. Allegations were made that he had abused a child of his partner. The Defendant informed another local authority (where C had applied for job) of those allegations. In judicial review proceedings the Court held that the Defendant had failed to carry out a proper balancing exercise and that the decision to disclose was unlawful. After considering various authorities (including *LM*) the Judge summarised what was required as follows (see §54):

It is plain to me that what these authorities require is the following. First, a weighing exercise must be carried out by any party who decides to disclose sensitive confidential information, a fortiori where it relates to matters which are not the subject of conviction or even caution. Second, I find helpful and persuasive the analysis of Dyson J in ex parte LM , where he suggested that at least three matters require to be included in that

⁴ See <http://www.audit-commission.gov.uk/SiteCollectionDocuments/Downloads/CodeDMPFinalJuly08.pdf>

weighing exercise: one, the proposed discloser's own belief as to the truth of the allegation — the greater the conviction that the allegation is true the more pressing the need for disclosure — two, the interest of the third party in obtaining the information — the more intense the legitimacy of the interest in the third party having the information the more pressing the need to disclose is likely to be; and, three, the degree of risk posed by the person if disclosure is not made. That analysis, or at any rate the detail of it, appears to have been doubted as appropriate by Turner J in R(A) v Chief Constable of C , to which I have referred, but I respectfully prefer the approach of Dyson J in that regard. Clearly, those three important questions are not necessarily conclusive or exclusive in the weighing exercise, but the background to all of them is what is emphasised by Lord Woolf in ex parte Thorpe and has been taken up in all the other authorities, namely is there a pressing need for disclosure?

45. Thus cases of this kind require very close and careful consideration of their specific facts. The cogency of any allegations needs to be carefully considered, as does the question of precisely what information needs to be disclosed, and to whom. A blanket decision that disclosure should be made to all of those who are likely to come into contact with a particular individual is unlikely to be upheld by the Courts if challenged.
46. Where findings of fact are made by the Court in child protection proceedings, suggesting that a particular individual poses a risk to children, the Court may be willing to make an order permitting disclosure of those findings to other persons or bodies: see e.g. *D v Buckinghamshire County Council* [2008] EWCA Civ 1372.

INFORMATION SHARING AND EMPLOYMENT

47. There is a complex statutory framework governing employment vetting. Under this framework local authorities may both receive information from third parties and make disclosures to third parties. Two aspects of this framework are discussed below: CRB checks; and the work of the new ISA.

CSA checks

48. The Police Act 1997 is the legal foundation for the Criminal Records Bureau (CRB). It needs to be understood against the background of Rehabilitation of Offenders Act 1974.
49. The 1974 Act governs the extent to which employers can ask for information about criminal convictions. Convictions are divided into two categories: unspent and spent. In general,

convictions become spent at the end of a rehabilitation period, provided that the individual has served any sentence and has not reoffended. The rehabilitation period varies depending on the severity of the sentence and the age of the offender, and will run from the date of sentence. Some convictions are excluded from rehabilitation: e.g. where the individual is sentenced to imprisonment for a term over 30 months, or for life. Any employer is entitled to ask candidates about their unspent convictions. This is so regardless of the nature of the job to which he is recruiting. Employers are free to reject candidates on the ground of unspent convictions; and they are also free to dismiss an employee for misconduct, if they subsequently discover that the employee lied about their unspent convictions when applying for the job. However, in general employers are not entitled to ask about spent convictions. Candidates may answer questions about convictions as if they referred only to unspent convictions. A spent conviction, or failure to disclose such a conviction, is not a proper ground for excluding a candidate from employment.

50. There are complex exceptions to the 1974 Act. A 1975 Order⁵ made under the section 4(4) of the Act allows employers to ask certain candidates about their spent convictions. This applies to certain work in relation to vulnerable adults⁶, and to work in a regulated position⁷.

- A vulnerable adult for this purpose is a person aged 18 or over who has a substantial learning or physical disability; a physical or mental illness or mental disorder, chronic or otherwise, including an addiction to alcohol or drugs; or a significant reduction in physical or mental capacity⁸.
- A regulated position⁹ includes:
 - a position whose normal duties include work in an educational institution, or various other sorts of institution for the care of children;
 - a position whose normal duties include work on day care premises;
 - a position whose normal duties include work on day care premises;
 - a position whose normal duties include caring for, training, supervising or being in sole charge of children; and

⁵ The *Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975 (SI 1975/1023)*, as subsequently amended.

⁶ See Schedule 1, Part II, paragraph 12 of the 1975 Order.

⁷ See Schedule 1, Part II, paragraph 14 of the 1975 Act.

⁸ See definition in Schedule 4 to the 1975 Order.

⁹ See definition in Schedule 4 to the 1975 Order, incorporating definition in section 36 of the *Criminal Justice and Court Services Act 2000*.

- a position whose normal duties involve unsupervised contact with children under arrangements made by a responsible person.

51. The CRB, set up under the Police Act 1997, provides a mechanism for employers to obtain access to conviction information, and also to other information relevant for employment vetting. The 1997 Act provides for the CRB to issue certificates giving three levels of disclosure (only two of which are currently available).

- Basic disclosure certificates. This covers an individual's unspent convictions only. Basic disclosure is not currently available from the CRB, though it is available from the equivalent Scottish body (Disclosure Scotland).
- Standard disclosure certificates. This covers all an individual's convictions, spent and unspent; it is available only to those employers who are entitled to ask questions about spent convictions.
- Enhanced disclosure certificates. This covers the same information as standard disclosure. It also includes additional information, where the chief officer of a relevant police force considers that the information:
 - might be relevant for the purpose for which the disclosure is sought; and
 - ought to be included.

This gives a wide discretion to include non-conviction information (including information that did not lead to a trial, or to criminal charges). Enhanced disclosure is available for those applying to carry out certain specified work with children or vulnerable adults¹⁰.

52. Where relevant, a CRB check will also include information as to whether an individual is on any of the statutory banning lists referred to in the following section of this paper.

53. The most controversial aspect of the CRB system is the provision of non-conviction information (sometimes referred to as "soft intelligence") by way of enhanced disclosure. From the employer's point of view, considering such information and deciding how much weight to give it is a difficult task. The obvious temptation is to exclude any employee for whom an enhanced CRB check

¹⁰ See section 113B of the *Police Act 1997*, as amended by the *Serious Organised Crime and Police Act 2005*, and as further amended by the *Safeguarding Vulnerable Groups Act 2006*; and see regulation 5A of the *Police Act 1997 (Criminal Records) Regulations 2002*.

shows any negative information. The Administrative Court has criticised this approach: see *R (Pinnington) v Chief Constable of Thames Valley* [2008] EWHC 1870 (Admin), at paragraph 59.

54. From the individual's point of view, a negative enhanced CRB check can create a very difficult situation. There is no easy way to challenge the inclusion of the information. There is no statutory right of appeal against the police decision to include the information; contrast the position, discussed below, in relation to the statutory banning lists. The CRB's internal complaints procedure, under section 117 of the 1997 Act, has a limited remit. Where soft intelligence is disclosed, the CRB's duty under section 117 is to consider whether the allegations in the enhanced disclosure were made, not whether they were well-founded: *R (B) v Secretary of State for the Home Department* [2006] EWHC 579 (Admin).
55. Some individuals have brought judicial review claims in order to challenge the police decision to disclose information. In general these have been unsuccessful, and the courts have treated the 1997 Act as conferring a wide discretion on the police.
- The leading case is *X v Chief Constable of the West Midlands Police* [2004] EWCA Civ 1068, [2005] 1 WLR 65. The subject of the disclosure was applying for a job as a social worker. He had previously been charged with indecent exposure, but was acquitted after the prosecution offered no evidence at trial. Details of the allegation were included in an enhanced CRB disclosure. The Court of Appeal dismissed a claim for judicial review of the police decision to disclose the allegation.
 - See also the unsuccessful judicial review claims in: *R (Pinnington) v Chief Constable of Thames Valley* [2008] EWHC 1870 (Admin); *R (L) v Commissioner of Police for the Metropolis*; *R (G) v Chief Constable of Staffordshire* [2006] EWHC 482 (Admin); and *R (L) v Commissioner of Police for the Metropolis* [2007] EWCA Civ 168.
56. On the current state of the authorities, an enhanced disclosure certificate is not confined to information about actual or potential criminal activity, or acts which show a propensity to crime. In one case, an individual applied for work as a casual midday assistant in a school; her enhanced CRB check disclosed that her own child had previously been placed on the Child Protection Register under the category of neglect. Her claim for judicial review failed: *R (L) v Commissioner of Police for the Metropolis*, above.
57. The *L* case went to the House of Lords earlier this year (it was heard in July 2009, and was one of the last cases to be heard before the new Supreme Court came into operation). Their Lordships were invited to consider both: (i) whether the approach in *X v West Midlands* was right,

having regard to article 8 of the Convention; and (ii) whether the information that could be disclosed by way of “soft intelligence” was confined to information about actual or potential criminal activity. A decision is currently awaited.

The work of the ISA

58. Currently there are three statutory banning lists; these prohibit individuals from working in specified employment, and also prohibit employers from engaging them.

- There is a list maintained under section 142 of the Education Act 2002. This covers education in schools, and other education-related work. For historical reasons it is often known as “list 99”.
- There is a separate list under section 1(1) of the Protection of Children Act 1999 (“the POCA list”), covering those considered unsuitable to work with children.
- There is also a list for the protection of vulnerable adults (“the POVA list”), which sets out the names of those considered unsuitable to work with this group. It is maintained under Part 7 of the Care Standards Act 2000.

59. Individuals placed on any of these lists have a statutory right of appeal. Appeals formerly went to the Care Standards Tribunal. The work of this Tribunal has been transferred to the Health, Education and Social Care Chamber of the First-tier Tribunal, with effect from 3rd November 2008, under the *Tribunals, Courts and Enforcement Act 2007*.

60. The House of Lords has recently held that the POVA list contravenes articles 6 of the European Convention on Human Rights, because an individual can be provisionally placed on the list before there has been any opportunity for a hearing. See *R (ota Wright and others) v Secretary of State for Health and another* [2009] UKHL 3.

61. The employment vetting regime is currently undergoing radical reform, as the *Safeguarding Vulnerable Groups Act 2006* comes into force. The 2006 Act is intended to give effect to the recommendations of the Bichard enquiry, following the Soham murders. It creates a new agency, the Independent Barring Board. The Board operates as the Independent Safeguarding Authority (ISA).

62. The scheme created by the 2006 Act, in outline, is this.

- The three existing lists will be replaced by two new lists, one relating to work with children and one relating to work with vulnerable adults.
- A person included on either list will be barred from “regulated activity” relating to the relevant group. It will be an offence for an individual to seek to engage in regulated activity from which he is barred. It will also be an offence for an employer to use a barred person for regulated activity.
- The ISA will maintain the two new barring lists.
- So that the ISA can keep the lists up to date:
 - persons seeking to engage in regulated activity must register for monitoring with the ISA;
 - the ISA must consider information about such persons both when they apply for monitoring, and at intervals thereafter; and
 - there are detailed provisions requiring employers, local authorities and others to refer information to the ISA: sections 35-42 of the Act.

63. The definition of “vulnerable adult” is in section 59 of the 2006 Act. It is very different from the existing definition. Broadly, a person is a vulnerable adult if he is in certain settings or situations or receives certain services.

64. “Regulated activity” is defined in Schedule 4 to the Act: part 1 deals with children, and part 2 with vulnerable adults.

65. There are four possible bases for inclusion on the either barred list¹¹:

- automatic inclusion;
- automatic inclusion, subject to consideration of representations;
- inclusion on grounds of behaviour; and
- inclusion on grounds of risk of harm.

¹¹ See Schedule 3 to the 2006 Act.

66. The Act also makes provision about controlled activity. This is a distinct category of work with children or vulnerable adults, defined in sections 21 and 22 of the 2006 Act. Broadly speaking the difference is that a barred individual may not be employed in regulated activity; such an individual may be employed in controlled activity, but the employer must put appropriate safeguards in place.
67. Where an individual is included in either barring list there is a right of appeal to the Health, Education and Social Care Chamber of the First-tier Tribunal, under section 4 of the 2006 Act. An appeal can be brought on a point of law or an issue of fact; but the decision whether it is appropriate for an individual to be included in a barred list is specifically stated not to be an issue of law or fact (see section 4(4)).
68. The new scheme will operate alongside the CRB disclosure scheme, and does not replace it. Hence employers will be entitled to standard or enhanced CRB checks, as at present, and in addition will be entitled (and obliged) to check whether individuals are on a relevant ISA barring list. The scope of the scheme is very wide indeed; apparently it is anticipated that once it is fully operational some 11 million individuals will be subject to ISA monitoring.
69. The 2006 Act is being brought into force in stages¹².
- From 20th January 2009, the ISA has taken over the task of updating the three existing statutory lists.
 - As from 12th October 2009 these three lists will be replaced by the two new lists introduced by section 2 of the 2006 Act.
 - From July 2010, new entrants to roles working with vulnerable groups, and those switching jobs within the sector, will be able to register with the ISA. Employers will be able to check registration status online.
 - By November 2010 new entrants and those moving jobs will be obliged to register with the ISA, and employers will be obliged to check their status.
 - The intention is to bring the whole of the existing workforce into the scheme by 2015.

September 2009

¹² For information about the progress of implementation, see the ISA's website: e.g. at <http://www.isa.gov.org.uk/Default.aspx?page=372> and at <http://www.isa.gov.org.uk/Default.aspx?page=385>