

INFORMATION SHARING & EMPLOYMENT VETTING

Anya Proops

A. INFORMATION SHARING AND LOCAL GOVERNMENT

INTRODUCTION

1. The fact that public authorities collect, analyse and disseminate vast quantities of personal data has given rise to substantial controversies in recent years. Questions which are now regularly being posed by members of the public, campaigners and politicians include whether public authorities:
 - (1) are doing too much with the data they hold (e.g. by effecting gratuitous disclosures);
 - (2) are alternatively doing too little with the data (e.g. by failing to ensure that there is adequate inter-agency data-sharing in cases of potential child abuse) or
 - (3) are just generally going about things the wrong way (e.g. by failing effectively to secure the data which they held – see further HMRC’s loss of 25 million child benefit records in 2007).
2. Over time, the urgency of these questions has become ever more acute as fears that we are ‘sleepwalking into a surveillance society’ and creating a Big Brother-style ‘database state’ jockey for position with fears that our public authorities are not doing enough to deploy data-sharing activities to safeguard society against threats of terrorism, child abuse and other forms of serious criminal behaviour.
3. In January 2009, the Government sought to address the latter fears by introducing new and potentially extremely wide-ranging data-sharing powers under the auspices of the Coroners and Justice Bill. The new powers, contained in clause 152 (and then later clause 154) of the Bill, sought to amend the Data Protection Act 1998 (“DPA”) so as to facilitate information sharing. In essence, the new powers would have enabled a Minister to make an ‘Information Sharing Order’ (ISO) enabling any person to share information that consisted of personal data provided that the Minister was satisfied: (a) that the ISO was necessary for a policy objective; (ii) the effect of the ISO was proportionate; and (iii) the ISO struck a fair balance between the public interest and the interests of any affected

person. However, in March 2009, the clause was abandoned in the face of wide-spread objection that introduction of the powers would result in extensive undermining of personal privacy. The furore over the proposed ISO powers perfectly illustrates the profound difficulties attendant on seeking to achieve an overarching regime for information-sharing which properly balances: (a) the State's need to share data to achieve its legitimate aims with (b) the individual's Article 8 and common law right to privacy.¹

4. A key practical issue for local authorities is how they should seek to strike this particular balance in respect of the vast quantity of personal data which they hold. Resolving this issue requires an understanding of the rather complex legal framework which governs the management of personal data by public authorities.

THE GENERAL LEGAL FRAMEWORK

5. In any case, where the local authority is contemplating a form of data-sharing (whether internally between different departments or with external third parties), the authority should have in mind the questions set out below.
 - (1) Does the authority have the *vires* to effect the proposed data-sharing?
 - (2) Are there any statutory provisions which specifically prohibit the proposed data-sharing?
 - (3) Would the data-sharing be in accordance with the requirements of the DPA?
 - (4) Are there any reasons to suppose that, even if the sharing was permissible under the DPA, it may yet be prohibited as a matter of general public law or alternatively under Article 8 ECHR?
 - (5) Is the data confidential at common law or in equity such that sharing of the data may give rise to a claim for damages for breach of confidence?

Vires

6. On the first of these questions, it is trite law that local authorities are creatures of statute and, as such, may only do those things which are expressly or impliedly authorised to do under statute (*R v Somerset County Council, ex p Fewings & Ors* [1995] 1 All ER 513).

¹ Notably, the proposed powers in the Bill went far beyond what had been recommended in Mark Walport and Richard Thomas' *Data-sharing Review* (July 2008) – see <http://www.justice.gov.uk/reviews/datasharing-intro.htm>.

Accordingly, in every case where data-sharing is being contemplated, the authority must ask itself whether there is implied or express statutory authority for the data-sharing in question. If the authority is sharing the information because this is necessary for the discharge of its statutory functions, then the *vires* will usually be implicit within the statutory provisions which confer the function. Or it may be seen as incidental to the discharge of the authority's functions so as to fall within s. 111 of the Local Government Act 1972.

7. In the alternative, it may be that the power to share the data can be derived from the authority's well-being powers under s. 2(1) of the Local Government Act 2000 ("LGA 2000"). Thus, for example, it may be that the authority could rely on s. 2(1) LGA 2000 as the basis for devising a customer relations management (CRM) system which is populated with data relating to individual tax-payers and is a resource which is shared across the local authority. However, reliance on s. 2(1) is likely to be rendered unsafe if the authority has not considered whether the proposed system would achieve a s. 2(1) objective and/or it has not had regard to the community strategy prepared under s. 4 LGA 2000. If it wishes to avoid legal challenge, the authority should be in a position to adduce clear evidence that it gave specific consideration to these issues (see *R(Risk Management Partners) v Brent LBC & Ors* [2008] EWHC 692 (Admin) where the High Court identified what requirements would have to be met in order to establish that powers under s. 2 LGA had been engaged, §115-118).²
8. In the context of information relating to crime and disorder, it may be that the particular proposed data-sharing would in any event be permitted under s. 115 of the Crime and Disorder Act 1998. In relation to children, it may be that the data-sharing would be authorised under s. 11 of the Children Act 2004 (the safeguarding duty).

Prohibitions

9. Certain legislation governing local authority functions may expressly or impliedly prohibit particular uses of personal data. In some cases, this will be obvious on the face of the legislation. In others, there may be arguments about whether the particular legislation in fact has the relevant prohibiting effect. Thus, for example, It has previously been suggested that schedule 2 to the Local Government and Finance Act 1992 ("LGFA 1992") constitutes a complete statutory code governing the use of Council Tax information and that uses of such information which may differ from the uses approved in the schedule would be unlawful. Certainly, this was the position suggested in guidance

² . The High Court's judgment on the application of s. 2 was upheld on appeal to the Court of Appeal [2009] EWCA Civ 490, see §§114-122.

issued both by the Information Commissioner's Office (ICO) and central government: see the guidance issued by the Data Protection Commissioner in May 1999; the ICO's compliance advice issued in May 2001; guidance issued by the ICO in August 2004 and the DCA's *Public Sector Data-sharing Guidance on the Law*, which was issued in 2003. However, some practitioners have argued for a less restrictive approach and more recent guidance issued by the ICO on 17 January 2007 suggests that the ICO has somewhat relaxed its position on this issue.

10. The arguments surrounding the application of schedule 2 are important, not least because of the administrative advantages for a local authority which is able to use council tax information to achieve its functional objectives. The fact that the legal implications of schedule 2 remain uncertain is therefore clearly unsatisfactory. However, it can be inferred from the ICO's 17 January 2007 guidance that the ICO will not be inclined to take enforcement action if council tax information is used for purposes which, though they fall outside the ambit of the LGFA 1992, do not cause any real harm to individuals. Thus for example, use of Council Tax records simply to populate a CRM is unlikely to attract the attention of the ICO.

Processing under the DPA

11. In common with data controllers in the private sector, local authorities are subject to a general duty under the DPA to comply with the data protection principles (DPPs) contained in schedule 1 to the DPA in respect of the personal data which they hold (see s. 4(4) DPA). That general duty can potentially be circumscribed where one of the exemptions provided for in Part IV DPA applies - see further, for example, the exemption in respect of the prevention and detection of crime (s. 29) and the exemption where data is disclosed pursuant to a legal exemption (s. 28). However, as a general rule, when contemplating whether a particular proposed data-sharing is lawful under the DPA, consideration will need to be given to the question of whether what is proposed would be contrary to one or more of the DPPs.³ If the sharing would contravene one or more of the DPPs then, unless an exemption applies under Part IV, the local authority would be exposing itself to claims for compensation under s. 13 DPA and, further, would risk inviting enforcement action by the ICO.
12. In terms of the DPPs themselves, they number eight in total. In summary, they are aimed at ensuring that personal data are:

- (1) handled fairly and lawfully (DPP1);

³ Data-sharing will amount to 'processing' for the purposes of s. 1 DPA.

- (2) obtained only for specified and lawful purposes and not processed in a manner incompatible with those purposes (DPP2);
 - (3) adequate, relevant and not excessive in relation to the purpose for which they are processed (DPP3);
 - (4) accurate and, where necessary, kept up to date (DPP4);
 - (5) not kept for longer than is necessary (DPP5);
 - (6) processed in accordance with the data subjects rights under the DPA (DPP6);
 - (7) safeguarded by appropriate technical and organisational measures which avoid unlawful processing and accidental loss, destruction or damage (DPP7); and
 - (8) only transferred to another country or territory outside the European Economic Area if that country or territory ensures adequate levels of protection (DPP8).
13. All of these principles are important and, possibly with the exception of DPP8, they should each be considered whenever a local authority is considering a new data processing measure, such as a new data-sharing arrangement. Indeed, at a recent conference on '*Surveillance and the Information Society*', the new Information Commissioner, Christopher Graham, made clear that the eight principles should always be used as a checklist to assess the impact of a proposed arrangement prior to its implementation, rather than as something which comes into play only as a post-implementation afterthought.⁴ In light of such statements, it is clear that a local authority which can adduce evidence that it carefully considered each of the principles in respect of a proposed data-sharing arrangement is going to be far better placed to defend itself against enforcement action than an authority which either ignored the principles or treated them with casual disdain.
14. Thus, for example, in respect of the particular proposed data-sharing arrangement, the authority should be in a position to demonstrate that it has carefully considered and reached rational conclusions on the questions of:
- (1) whether the data which it is proposing to share is accurate (DPP4);
 - (2) whether it is sufficiently up to date (DPP4);

⁴ Conference held at Clifford Chance on 11 March 2010.

- (3) whether it is the right kind of information to enable the particular objectives which underpin the data-sharing arrangements to be met (DPP 3);
 - (4) whether the information sharing arrangements are administratively secure so as to avoid data being unlawfully intercepted and/or gratuitously accessed by third parties (DPP7).
15. In addition to considering these essentially logistical questions, the local authority will also need to address the more difficult questions posed by the DPPs including in particular:
 - (1) whether the arrangements would meet the requirements of the fair and lawful processing principle (DPP1); and
 - (2) whether the arrangements meet the compatibility principle (DPP2).

DPP1

16. DPP1 provides that:

'personal data must be processed fairly and lawfully and, in particular, shall not be processed unless: (a) at least one of the conditions in schedule 2 is met and; (b) in the case of sensitive personal data, at least one of the conditions in schedule 3 is also met'.

17. As is apparent from the wording of DPP1, the question of how DPP1 applies depends on whether the data in issue is or is not 'sensitive personal data' (as defined in s. 2 DPA).
18. 'Sensitive personal data' includes data as to: the data subject's racial or ethnic origin; his political opinions; his religious beliefs or other beliefs of a similar nature; whether he is a trade union member; his physical or mental health or condition; his sexual life; the commission or alleged commission by him of any offence; and any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings. Evidently, this definition would embrace, for example, data as to whether an individual has a tendency towards child abuse.
19. In essence, if the data amounts to sensitive personal data, processing will only be lawful in circumstances where:

- (1) the processing meets one of the conditions provided for in schedule 2 to the DPA; and
 - (2) the processing meets one of the conditions provided for in schedule 3 to the DPA; and
 - (3) the processing is otherwise fair and lawful.
20. The processing of non-sensitive personal data will be in accordance with DPP1 if it merely meets a schedule 2 requirement and is otherwise fair and lawful.
21. Schedule 2 contains a number of conditions which may or may not be met on the facts of the particular case. However, the condition which most typically tends to be invoked is that contained in paragraph 6 of schedule 2. That condition will be met where:
- 'the processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party to whom the data are disclosed except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject' (emphasis added)*
22. In essence, where the authority is proposing to process personal data by sharing it either internally or with third parties, paragraph 6 requires the authority to ask itself four questions.
- (1) Does the proposed recipient of the data have a legitimate interest in receiving the data? (Mere curiosity would be unlikely to qualify as a legitimate interest).
 - (2) If so, is the sharing of the particular data necessary to serve those interests? (In this context, the authority should ask itself whether the interests may be served through the disclosure of some other information – for example anonymised data).
 - (3) Would the sharing of the data prejudice the rights, freedoms or legitimate interests of the data subject (e.g. by interfering with his/her right to privacy or exposing him/her to serious mental distress)?
 - (4) If the data-sharing would have a prejudicial effect on the data subject, is the interest in avoiding that prejudice nonetheless positively outweighed by the legitimate interest in sharing the data?

(See further *Camden LBC v Information Commissioner* on the application of these principles to a case where a person was seeking disclosure under the Freedom of Information Act 2000 of ASBO data held by a local authority (EA/2007/21)).

23. In addition to meeting a schedule 2 condition, where it is proposed to share sensitive personal data, the authority must also show that a schedule 3 condition is met. The schedule 3 conditions are generally much more stringent than the schedule 2 conditions.
24. If the data subject has consented to the particular data-sharing arrangements, then conditions in schedule 2 and schedule 3 would both have been met (see paragraph 1 of schedule 2 and paragraph 1 of schedule 3). It follows that a local authority which obtains the consent of the relevant data subjects prior to engaging in a form of data-sharing will be a long way down the road towards establishing that the particular data-sharing arrangements meet the requirements of DPP1. However, seeking or obtaining such consent may of course not be practicable in a particular case. In general, the authority should always consider whether consent is a realistic option and, if it is not, whether some other relevant condition may yet be met on the facts of the case.
25. As far as 'fairness' is concerned, it was held in *Johnson v Medical Defence Union* [2006] EWHC 321 that fairness should be considered in general terms, although consideration should also be given to the specific interpretation principles set out in Part II of schedule 1. Relevant to the question of fairness will be whether the particular data subjects would have known or ought reasonably to have known that their data would be used in this particular way (see further the *Camden* case cited supra and see also the MPs expenses litigation). If there is any doubt on this question, the authority may seek to protect its position by sending out a fair processing notice informing data subjects of the proposed use.
26. Even if a proposed data-sharing arrangement is not unfair per se, the processing will still contravene DPP1 if it is unlawful. Thus, for example, if the processing would result in an unjustified breach of the data subject's right to privacy it will contravene DPP1.

DPP2

27. DPP2 provides 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 that purpose or those purposes'

28. Importantly, this principle has limited application in practice. This is because a processing of personal data will not contravene DPP2 simply because it is for a purpose which is different from the one for which the data was obtained. Instead, DPP2 will only be contravened if the processing is positively incompatible with the latter purpose.
29. More generally, when considering the application of the DPA to particular data-sharing arrangements, local authorities will wish to consider the ICO's *Framework Code of Practice for Sharing Personal Data*⁵ and also his 30 May 2008 Good Practice Note on the sharing of information between local authority departments.⁶ Notably, the Good Practice Note highlights that, when information is passed from one department to another but the purpose for which it is used does not change, the arrangement is unlikely to give rise to difficulties under the DPA. However, it also makes clear that where information passes from one department to another and the latter department uses the information for different purposes than the former department (a so-called 'secondary use' case), this may give rise to difficulties. In determining whether such arrangements would fall foul of the DPA, the Note invites a focus particularly on the application of DPP1 and DPP2. The principal recommendation emerging from the Note is that, at the point when the information is obtained, fair processing notices should identify the possible secondary uses of the information.

Public Law and Article 8

30. In most cases where the local authority is able to establish that the particular data-sharing would be lawful under the DPA, there is likely to be little scope for arguing that the data-sharing is nonetheless unlawful having regard to general public law principles and/or the requirements of Article 8 ECHR. This is because the tests imposed under the DPA are relatively stringent and, if the authority succeeds on these tests, it may well be that any public law arguments or Article 8 arguments will fall away. However, the authority ought still to have the relevant principles in mind when it is assessing the legality of a proposed data-sharing arrangement.
31. Thus, for example, in terms of public law principles:
- (1) it will want to consider whether the proposed arrangement can be justified as being *Wednesbury* reasonable;

⁵http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/pinfo-framework.pdf.

⁶http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/local_authorities_-_data_sharing001.pdf.

- (2) it will want to ensure that the arrangement is being proposed for a proper (as opposed to an improper) purpose;
 - (3) it will want to ensure that all relevant considerations have been taken into account and all irrelevant considerations disregarded;
 - (4) it will want to consider whether the data subject may have legitimate expectations that the data will not be shared and, if so, whether there is yet a lawful basis for not meeting that expectation (see *R(Nadarajah) v Secretary of State for the Home Department* [2005] EWCA Civ 1363); and
 - (5) it will otherwise want to ensure that there is a genuine 'pressing need' for the arrangement (see further *R v Chief Constable of North Wales, ex p Thorpe* [1999] QB 396 and *R(Ellis) v Chief Constable of Essex Police* [2003] EWHC 1321 (Admin)).
32. In the context of the application of Article 8, a number of considerations will arise including:
- (1) Does the proposed data-sharing infringe the individual's right to privacy under Article 8(1)?
 - (2) If it does, what is the nature and extent of any infringement in the individual's right to privacy?
 - (3) Further, is the infringement necessary to serve a pressing social need and does it otherwise fall within the ambit of the justification provision contained in Article 8(2) ECHR?
33. On the latter question, the recent judgment of the Supreme Court in *R(L) v Commissioner of Police of the Metropolis* [2009] 3 WLR 1056 is instructive. L was employed as an assistant at a midday secondary school, supervising children in the lunchtime break. An enhanced criminal records certificate was supplied to her employer by the police under s. 115 of the Police Act 1997. The certificate showed that she had no criminal convictions, but had included under the heading "other relevant information disclosed at the chief police officer's discretion" the information that her son had been placed on the child protection register under the category of neglect, she being alleged to have failed to exercise the requisite degree of care and supervision (this type of non-conviction information is often called 'soft intelligence'). As a result of the supply of the certificate, L lost her job. She applied for judicial review of the Commissioner's decision to disclose the

soft intelligence. The nub of L's case was that the guidance given in *R(X) v Chief Constable of the West Midlands* [2004] EWCA Civ 1068, [2005] 1 W.L.R. 65 as to the correct approach to disclosure gave insufficient weight to the interests of the applicant. In the *X* case, the Court of Appeal held that a chief police officer was under a duty to disclose under s. 115 if the information might be relevant, unless there was some good reason for not making such disclosure,

34. L's claim was refused by the Administrative Court and her appeal was refused by the Court of Appeal. L appealed to the Supreme Court. The Supreme Court dismissed L's appeal, although it did accept her argument that the guidance in *X* should not be followed. In essence, the Supreme Court held that the disclosed information was plainly relevant for the purpose for which the certificate was required, that is was true and that it bore directly on the question of whether she was a person who could safely be entrusted with supervising children in a school canteen or playground. The risk to children outweighed the prejudicial effects of the disclosure on the facts of the case. In reaching these conclusions, the Supreme Court explored the question of how the Commissioner should decide whether to share soft intelligence in an enhanced criminal records certificate. It held that in deciding such a question, the Commissioner should ask himself:

- (1) whether the information might be true;
- (2) the degree of connection between the information and the purpose for which the certificate was sought;
- (3) whether the information "ought" to be included for the purposes of s. 115; and
- (4) whether the disclosure was otherwise in accordance with the Article 8 right to privacy. Thus, he had to consider in every case whether there was likely to be an interference with the applicant's private life, and if so whether that interference could be justified. On the facts of the case before it, the Supreme Court held that the issue was essentially one of proportionality. On the one hand there was a pressing social need that children and vulnerable adults should be protected against the risk of harm; on the other there was L's right to respect for her private life.

35. As for the guidance given in *X*, the Supreme Court held that the guidance should not be followed as it had tilted the balance too far against the subject of the certificate, encouraging the idea that priority had to be given to the protection of the vulnerable as against the subject's Article 8 right. It held that the words 'ought to be included' in section

115(7) had to be given much greater attention and had to be read and given effect in a way that was compatible with the applicant's Article 8 right, together with that of any third party who might be affected by the disclosure. The correct approach was that neither consideration took precedence over the other and it should no longer be assumed that the presumption was for disclosure unless there was a good reason for not disclosing. In cases of doubt, especially where it was unclear whether the position for which the applicant was applying really did require the disclosure of sensitive information; where there was room for doubt as to whether an allegation of a sensitive kind could be substantiated; or where the information indicated a state of affairs that might be out of date or no longer true; chief constables should offer the applicant an opportunity of making representations before disclosing the information.

36. Needless to say, local authorities are not themselves subject to the requirements of s. 115 of the Police Act 1997. However, it is to be inferred that a similar approach should be adopted whenever a local authority is considering data-sharing arrangements which potentially give rise to an interference with Article 8 rights, particularly where the arrangements countenance the disclosure of sensitive information. What this means is that where local authorities are contemplating sharing sensitive personal data, and particularly where disclosure of the data carries with it the risk that the individual may be harmed, the authority should consider the following issues:

- (1) the reliability of the information – the extent to which it might be true and, further, the extent to which it continues to be current;
- (2) the extent to which the sharing of the information would actually serve a legitimate aim;
- (3) the importance of the legitimate aim to be served;
- (4) the extent to which the sharing would interfere with the data subject's right to privacy and otherwise the potential damage which the data subject may suffer if the information is shared;
- (5) whether it is in all the circumstances proportionate to engaging in the particular information sharing activity; and
- (6) whether, in cases of doubt, it would be appropriate to invite the data subject to set out his/her views on what is proposed.

37. The following constitute examples of how the courts have previously approached the difficult question of whether a local authority was acting lawfully when it disclosed ad hoc information about an individual for child protection purposes. Whilst all of these cases were decided prior to the *L* case, they all essentially embody the spirit of the principles approved by the Supreme Court in *L*.

- *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 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 emphasized 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?’

38. What is clear is that 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. Notably, 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.

Confidentiality

39. A further consideration to be borne in mind whenever a local authority is contemplating a particular data-sharing arrangement is whether sharing the data may constitute a breach of confidence either at common law (i.e. under a relevant contract) or in equity. In cases where there is a risk of breach, the local authority will want to consider very carefully whether it wishes to enter into the arrangements, not least because by doing so the local authority may be exposing itself to costly litigation.
40. However, even where the data-sharing arrangement would give rise to a clear breach of confidence, that does not per se mean that the local authority is automatically precluded from entering into the particular arrangement. This is because on the facts of the case it may yet be that the breach would be warranted on public interest grounds, such that no cause of action will lie against the public authority (see further the examination of the public interest defence in *Moseley v News Group Newspapers* [2008] EWHC 1777). The

precise scope of the defence remains unclear. However, what is clear is that there is a public interest in protecting confidences and, accordingly, to avoid a finding of unlawful breach of confidence, the local authority will need to be able to show that there is a stronger counter-veiling public interest in the disclosure. The public interest defence may be available, for example, where the authority could show that the sharing of the information was necessary to prevent serious harm to an individual or prevent a criminal offence taking place.

B. EMPLOYMENT VETTING

41. In today's multi-media world, employers may seek to obtain information about potential recruits from a number of different sources, including not least social networking sites such as facebook and myspace. The question of whether the use of such sites to vet potential candidates is lawful is an interesting one. Certainly, there are important issues about whether such activities constitute an unlawful interference with the candidate's right to privacy. These are issues which will doubtless achieve increasing prominence as employers become more alive to the advantages of using social networking sites to profile a potential candidate. However, whilst the use of such informal vetting methods is still in its infancy, the use of more traditional statutory methods, including in particular the use of CRB checks is well established. Below I consider the statutory regime which governs CRB checks. I also briefly discuss the work of the new Independent Safeguarding Authority.

CRB Checks

42. The legislative regime governing the CRB system is embodied in the Police Act 1997. The 1997 Act needs however to be considered against the background of the Rehabilitation of Offenders Act 1974 ("ROA 1974"). It is the latter act which governs the extent to which employers can ask for information about criminal convictions.
43. Under ROA 1974, criminal convictions are divided into two categories: spent and unspent. 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 length of the rehabilitation period will vary 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 a life sentence is imposed). An employer is entitled to ask candidates about their unspent convictions irrespective of the nature of the job to which he is recruiting. Employers are free to object candidates on grounds 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.

44. There are complex exceptions to ROA 1974. A 1975 Order⁷ made under the section 4(4) of ROA 1974 allows employers to ask certain candidates about their spent convictions. This applies to certain work in relation to vulnerable adults,⁸ and to work in a regulated position.⁹ 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 capacity.¹⁰ A *regulated position*¹¹ 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 a position whose normal duties involve unsupervised contact with children under arrangements made by a responsible person.
45. 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). First, there are *basic disclosure certificates*. These cover 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). Second, there are *standard disclosure certificates*. These cover all an individual's convictions, spent and unspent; it is available only to those employers who are entitled to ask questions about spent convictions. Third, there are *enhanced disclosure certificates*. These cover the same information as standard disclosure certificates but also includes additional information, where the chief officer of a relevant police force considers that the information: (a) might be relevant for the purpose for which the disclosure is sought; and (b) ought to be included (see further

⁷ The *Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975 (SI 1975/1023)*, as subsequently amended.

⁸ See Schedule 1, Part II, paragraph 12 of the 1975 Order.

⁹ See Schedule 1, Part II, paragraph 14 of the 1975 Act.

¹⁰ See definition in Schedule 4 to the 1975 Order.

¹¹ See definition in Schedule 4 to the 1975 Order, incorporating definition in section 36 of the *Criminal Justice and Court Services Act 2000*.

the *L* case referred to above). Enhanced disclosure is available for those applying to carry out certain specified work with children or vulnerable adults.¹² Where relevant, a CRB check will also include information as to whether an individual is on any of the statutory banning lists referred to below.

46. The most controversial aspect of the CRB system is the provision of non-conviction information (or “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 shows any negative information. However, the Administrative Court has criticised this approach: see *R (Pinnington) v Chief Constable of Thames Valley* [2008] EWHC 1870 (Admin), at paragraph 59. It was precisely this sort of information which was considered in *L* (cited supra). The *L* case is important because of what it says about how chief officers should approach the question of what information to include in an enhanced CRB certificate. However, it is also important because of the way in which it highlights just how difficult it is for an individual to challenge an enhanced CRB certificate. See further on this point the earlier cases of *X v Chief Constable of the West Midlands Police* [2004] EWCA Civ 1068, [2005] 1 WLR 65; *R (Pinnington) v Chief Constable of Thames Valley* [2008] EWHC 1870 (Admin); *R (G) v Chief Constable of Staffordshire* [2006] EWHC 482 (Admin). In each of these cases, the individual’s attempt to judicially review the certificate was unsuccessful.

The Work of the ISA

47. Up until October 2009, there were three statutory banning lists. These lists prohibited individuals from working in specified employment, and also prohibited employers from engaging them.
- There was 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 was often known as “list 99”.
 - There was 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.

¹² 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*.

- There was 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 was maintained under Part 7 of the Care Standards Act 2000.
48. Individuals placed on any of these lists had 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*. The House of Lords has recently held that the POVA list contravened 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 (Wright and others) v Secretary of State for Health and another* [2009] UKHL 3).
49. 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).
50. The scheme created by the 2006 Act, in outline, is this.
- The three existing lists have been 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 maintains 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.

51. The definition of 'vulnerable adult' is in section 59 of the 2006 Act. It is very different from the definition under ROA 1974. Broadly, a person is a vulnerable adult if he is in certain settings or situations or receives certain services. 'Regulated activity' is defined in Schedule 4 to the Act: part 1 deals with children and part 2 with vulnerable adults. There are four possible bases for inclusion on the either barred list: (1) automatic inclusion; (2) automatic inclusion, subject to consideration of representations; (3) inclusion on grounds of behaviour; and (4) inclusion on grounds of risk of harm.¹³ 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.
52. 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)). The new scheme operates 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.
53. The 2006 Act is being brought into force in stages.¹⁴ 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 were 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.

¹³ See Schedule 3 to the 2006 Act.

¹⁴ 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>

54. The scope of the scheme is potentially very wide indeed. It is anticipated that once it is fully operational some 11 million individuals may be subject to ISA monitoring. One aspect of the scheme has however already been highly controversial, namely that part of the scheme which determines the degree of contact with children which would trigger the requirement to register with the ISA. This controversy has moved the Government to amend the definition of 'frequency' and 'intensity' in the legislation so as to ensure that, in effect, those who have only relatively occasional or sporadic interaction with children are not caught by the legislation. See further on this Ed Balls' Statement to Parliament on 14 December 2009 in response to Sir Roger Singleton's report on the new ISA regime.¹⁵

March 2010

¹⁵ <http://www.isa-gov.org.uk/Default.aspx?page=414>.