EURIM Working Group

Status Report

October 2004

Data Sharing and Matching: the Law in Practice

1 Introduction

Many believe that the law no longer provides an adequate framework for the way in which public services are being organised and delivered. Data-sharing powers are deemed insufficient, preventing public bodies from meeting policy objectives and from securing a step change in service delivery. In parallel there are concerns over lack of effective data protection, especially with regard to material handled by contract staff, outsourced or requisitioned under investigatory powers.

Severe problems have been encountered with data sharing at the practitioner level and there are specific problems in terms of lack of powers for statutory and common law bodies to share data even where the individual has given consent to data-sharing. There is a growing view that the current situation, with fragmented data collection and updating often outsourced, and with sharing forbidden except when it is mandatory under legacy powers, gives the worst of all worlds: duplication, waste, error and confusion without credible protection against fraud or abuse.

The EURIM Personal Identity group has therefore prepared this report of current issues, and will consider the value of a follow up exercise calling for greatly improved guidance and, if necessary, primary legislation to enable consent driven data sharing under democratically accountable governance.

2 Data Sharing

2.1 Concerns

There are many recent examples (including the Soham murders, and British Gas cutting off a couple's energy supply for failing to pay their bills) demonstrating the need for increased guidance and clarification of the legal environment, particularly the Data Protection Act (DPA). Many public sector organisations have been extremely cautious in interpreting this law, including Edinburgh City Council, which prevented photography of school nativity plays for child protection reasons.

Other government initiatives and legislation, such as the decision to publish a draft Bill on identity cards, the Children's Bill, and the emerging problem of identity fraud also demonstrate the issue's relevance. The legal environment is shaped further by other Acts of Parliament that deal with Human Rights (HRA), Freedom of Information (FoIA), and the Regulation of Investigatory Powers (RIPA). The Department for Constitutional Affairs published guidance recently to help clarify the situation for central and local government but this is generic and many concerns about the DPA, privacy and confidentiality remain:

- Those handling personal information need to know to whom they should pass which data, to whom, under what circumstances, including how to check the identity and authority of those access and who to ask when circumstances arise which are not covered in their basic training.
- Departments and Agencies should, wherever possible, use similar processes when claiming access to information under statutory powers. – The main current processes are those drafted

by the Association of Chief Police Officers (ACPO) for claiming access to communications data under RIPA and by DWP for those claiming access to records of all types with regard to investigating Benefits Fraud.

- Organisations also need policy documents setting out their minimum security requirements and staff roles and responsibilities - although documents of this nature do not mean that the processes are necessarily lawful.

The drivers for sharing information include:

- Public demand for more personalised, joined-up services, where they do not have to tell numerous agencies if their details or circumstances change.
- e-Government initiatives and the pressure to make all services available electronically by 2005.

However, citizens are also concerned about their privacy and many have serious fears and suspicions of a 'Big Brother' state.

2.2 The Data Protection Act in Principle

The DPA already deals with privacy issues, but remains unclear to many people. It applies when:

- Processing personal data that relates to living, identifiable individuals. Previously, this was interpreted as anything that included people's names, but the recent Durant vs Financial Services' Authority case restricted this definition to something that is biographical and focuses specifically on the individual's personal, family and/or professional life.
- The information is automated or filed manually through a system that is structured according to the individual or criteria relating to him/her, and easily accessible.

The DPA's 8 ‘principles’ are:

1. Personal data shall be processed "fairly" (Schedule 2) and "lawfully" (Schedule 3), and collected for a "good reason" (with the individual’s consent, as part of a contractual arrangement, under a legal obligation, to protect vital interests, or help with public functions etc). People should be given information about the organisation and individual that collects the data, and what they intend to do with it at the point of collection or as soon as is reasonably practical after that. They should then have the chance to opt out if their data is going to be used for marketing purposes.

2. 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.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. The organisation should keep the information only for as long as is necessary for its specified purposes. The Records Management Society keeps a number of best practice examples on its website, at www.RMS-uk.com

6. Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

An organisation should take reasonable steps to ensure the information is protected against unlawful/unauthorised access or destruction. The issues here relate to IT security and staff awareness - access should be on a need-to-know basis. Individuals have a number of rights under the Act, most notably that of "subject access" - the right to see information that relates to them within 40 days of making a request. In addition, every organisation has to provide an annual "Notification" to the Information Commissioner's Office, detailing the data it holds and any data sharing initiatives it may be involved in. Not having a notification or failing to keep it up-to-date is a criminal offence.

There are a number of exemptions that allow for the use of data when an individual has not been notified or given consent. These cover the areas of national security, crime, taxation, journalism, literature, and for use in a personal, domestic or family sphere (this last meaning that taking private photographs at nativity plays does not run contrary to the Act).

However, in the case of crime prevention, organisations do not have a duty to disclose the information - it is discretionary. If they do decide to share the data, they should set up a clear audit trail to explain exactly what has been disclosed and why.

2.3 The Data Protection Act in Practice

The Information Commissioner is responsible for issuing Guidance and Codes of Practice on the Data Protection Act 1998, and is also responsible for enforcing the data protection regime. Data Controllers are required to notify with the Commissioner, which includes setting out the purposes for which data will be processed, and the persons or organisations to which data may be disclosed. In most cases where there is a dispute about processing, the Commissioner's preference is to resolve the matter through discussion, and this is what happens in most cases. The Commissioner also has the power to issue an enforcement notice requiring a data controller to cease certain actions or to take others, a notice which can be appealed to the Information Tribunal. There are a limited number of criminal offences identified in the Data Protection Act, in particular the unlawful obtaining and disclosing of data. However, it is important to understand that that means, for instance, the deliberate and unauthorised disclosure of data for financial gain, rather than accidental or unintended disclosure of data.

2.4 The Effects of Human Rights Legislation

The Human Rights Act and issues of confidentiality restrict the ability of organisations to share and match data. The Human Rights Act (HRA) enshrined the European Convention in the main body of UK law, meaning that citizens can enforce their rights in a local county court rather than having to go to Strasbourg. This has also become a live issue recently; given the Government's response to terrorism that many argue threatens human rights.

The Act has 14 articles, and for data sharing issues the most relevant is Article 8 concerning privacy. This enshrines the right to "respect for an individual's private and family life, home and correspondence" and has led to a number of high-profile court cases, including when Catherine Zeta-Jones and Michael Douglas took on Hello magazine. This and other cases suggest that courts will enforce rights to privacy, particularly when photographs are involved.

The Act therefore has implications for local authorities' CCTV footage, both inside and outside buildings. Organisations should develop a code of practice for its use and ensure that their staff are aware if it is present in the workplace. Further complications result from mobile video surveillance, since the public cannot be kept up-to-date with the location of cameras.

Public authorities also have a duty of confidentiality if they are given information that has 'quality of confidence'. But this is not absolute and can be overridden if disclosure is in the public interest, which may be the case when the protection of children or vulnerable adults is an issue. For example:

- If a known paedophile moves to a new area, should the new local authority be informed? Issues to consider are whether they are being supervised, or whether they have been convicted of committing a crime.

- In the case Maddock vs Devon CC, a woman applied to go on a social work course and the council disclosed that her children were previously taken into care for neglect. The mother sued for breach of confidence, but the court found in favour of the authority.

The Robertson vs Wakefield case in 2001 found that the authority breached a citizen's right to privacy by selling its electoral roll data to marketing companies. Councils now need to have two versions, a 'full' list and another one that can be sold - and citizens have the right to opt out of the latter. The full list should be available for legitimate council functions, but the edited version must be used for any marketing purposes.

Particularly controversial has been the use of photographs. In another case, a picture of someone who had been convicted on 57 counts of burglary was to be published in a police brochure as part of a crackdown on crime. The individual claimed that this breached his right to privacy, and the case was eventually dropped after the police withdrew their campaign. However, this was not before the court said the force should have considered the claimant's right to privacy, and the rights to the privacy and safety of his family and friends.

2.5 The Interplay of Data Protection, Human Rights and Administrative Law

Administrative law - that which is expressed or implied by statutory powers - also plays an important role in this area. For example, Section 2 of the Local Government Act 2000 confers a power of 'well-being' onto councils, suggesting that they can do anything (including the sharing of data) which they consider would contribute to the well-being of persons within its area, or the local economic, social or other situation. Although central government is keen for local authorities to use this power, they should still consider whether other legislation and enactments prohibit information sharing in particular areas, as they do not override this law.

It is important to have a protocol in place when data is shared on a regular basis, for example between partners. Although merely having a protocol does not mean the sharing is lawful (and the agreement itself is not legally binding), the Information Commissioner is likely to be more lenient towards organisations that break the law if they have one in place.

However, there is deep concern that no one really knows what the nature of the data sharing problem is, although there is widespread agreement that there definitely is a problem! It may be that this relates to the DPA being inherently complicated, and what is needed is better guidance to the Act. On the other hand, it can be argued that the complexity arises from the circumstances to which the Act must be applied, and people are very anxious about making decisions that are compliant in different situations that they do not fully understand. Here, no amount of explanation of what the DPA requires will help, because ultimately a judgement is needed. DCA feel that people are asking for guaranteed compliance, not vague principles, and DCA cannot provide this.

Where there is no power to share (or acquire) data, giving consent will not provide that power. An individual may consent to an unlawful act, but that would not make it lawful. Primary legislation would be needed. However, the draft ID Cards Bill proposes to introduce legislation specifically to allow data sharing, without consent. This legislation might be extended to provide for an individual who gives consent to use the ID card to access data, This is an area which the group believes needs a follow up exercise.

3 Data Matching

Data Matching involves linking different information sources to identify fraudulent activity - for example, comparing benefit and tax records could help assess whether an individual is claiming jobseekers allowance whilst working. Data matching raises similar human rights and data protection issues as data sharing, and the legal environment is similar:

- Human rights - privacy issues arise when using data for a purpose for which it was not originally intended (this also brings in the DPA)
- Data protection - information should be used fairly and lawfully, although Sections 29 and 35 of the DPA instruct organisations to disclose it when required by law through a court order.

The Information Commissioner has expressed concerns about data matching for reasons of privacy and the due process of law. In addition, it changes the emphasis on the presumption of innocence, since individuals are being investigated without their knowledge for evidence of criminal activity, and are never above suspicion until no match is found.

Nevertheless, employers sometimes undertake internal data matching exercises to try and detect fraud, often using payroll data - local authorities might want to known whether their employees are paying council tax for example. Provided staff are made aware of this and consent to it (perhaps by including it in their contracts), this is fine.

The biggest exercise in data matching is the National Fraud Initiative (NFI), a UK-wide exercise undertaken by the Audit Commission every two years. This involves collecting data from a wide range of organisations to identify various types of fraud. Central and local government departments, devolved administrations, the NHS, DWP, pensions' providers and a number of large private sector companies all participate in the scheme.

The NFI involves standardising and cleaning the data, before loading them into a software program that identifies matches. This is graded according to the following criteria:
1. NI number.
2. Name and date of birth - if the name is very common, the software can assess the likelihood of a match.
3. Address - this provides additional authentication of an individual and identifies common inhabitants of a property. However, it can be difficult to prove that people who share a home have a financial relationship.

Some of this information is filtered, before 'weaker' matches are removed. The Audit Commission sends each participating organisation a CD containing relevant matches, and the organisation is then responsible for acting on the information (the NHS releases this information to primary care trusts). The last exercise in 2002 identified over 1m matches, leading to a variety of actions against fraudsters.

The initiative has delivered savings exceeding £81m from various areas, particularly in housing benefit fraud, pensions and unsuccessful asylum seekers. Fraudsters often operate in more than one area, and so identifying one case can often uncover other examples of fraud by the same individual:

- Housing benefit fraud often occurs when an individual does not declare an increase in earnings. One example of this involved a local authority employee who claimed benefit but did not declare their income from the council on the form.
- Pension fraud frequently takes the form of payments that are made to people who are dead - over 100 of these have been identified, leading to savings of over £3m and one local authority identified a 10-year old fraud worth £7,000. Once this type of fraud has started it is very difficult to stop, since the fraudster would need a death certificate to demonstrate that the pension was no longer required. Another big fraud in this area relates to employees who return to work without declaring it, and receive a pension in addition to their salary.
- Failed asylum seekers are not entitled to remain in the UK and it is therefore a criminal offence to employ them (though employers are unlikely to face charges unless they continue to provide them with work after they are identified). This is a difficult area, since they move around frequently and are often granted the right to stay on appealing their initial decision. Consequently, organisations need to check back with the Home Office to see whether their status has changed before pursuing the matter further.

Results from the most recent exercise suggested that the same individual appeared to be working simultaneously at two NHS organisations that were 100 miles apart. This raised concerns that one individual working in the health sector will not have the qualifications they say they have, and identity theft is becoming a real problem. The two organisations concerned are now dealing with the matter collectively, using biometric identification of the people concerned.

The NFI has a number of benefits:

- It fits with the government agendas of joining-up and combating fraud.

- It is in the public interest, delivering £190m in savings since its introduction, and helping to identify people who work in the public sector that could put citizens at risk.
- There is a legal requirement related to internal data matching - provided they inform staff and only collect relevant information then they should be okay. A code of practice on data collection should be drawn up, in tandem with protocols for exchanging information with partners. These should cover details about:
    - Who can access the information
    - How the results should be stored (preferably in a walk-in safe or locked cabinets)
    - How and when results will be destroyed
    - Internal auditing

In future, the Audit Commission is looking to bring in data from other sources to improve the exercise. These include:

- Mortgage lender records - few circumstances exist that allow property owners to claim benefit.
- Inland Revenue.
- Companies' House information on business transactions.
- Intelligence integration for organised fraud and landlord fraud.

Some may feel that the NFI is controversial, given civil liberty, legal and privacy issues. Although the legislation allows data to be transferred to help prevent or detect crime, this is normally done with particular individuals in mind rather than involving the whole population, as is the case with the NFI. There may be a case for a single national organisation to be responsible for the entire exercise - although any legislation to authorise a UK-wide system would be controversial.

4 Some Practical Case Studies and Conclusions

1. In their one-stop-shops, a council did not have paragraphs or protocols to enable citizens' data to be shared locally - instead national templates were being used. A policy document should be drafted outlining how their authority wished to use this information and present it to citizens at the one-stop-shop. The key issue concerned 'fair processing' of data by telling people at the point of collection that it will be passed on. Calderdale Council had previously used posters in their centres to inform the public that their information would be shared with other agencies.

2. Another council disclosed social services information to the local primary care trust for medical action - not the purpose for which the data was collected originally. Provided the individuals concerned are aware of this, such transfer is okay (GPs have duty to disclose information to social services where applicable) - the key is to inform them and get their consent.

3. Can schools disclose class lists to help with the distribution of birthday party invitations? It is recommended that the addresses be retained and children encouraged to hand out the invites in school rather than post them, since most children would know each other anyway.

4. One organisation discovered that someone they were hiring as a consultant was registered to work with another council and receiving sick pay. The employing council now wanted to know when this consultancy was undertaken to confirm their suspicions. Under the DPA, most information should be kept confidential, unless it can lead to the prevention or detection of crime. As a result, it should be established whether this was a criminal or civil offence. Although it could be argued that the charge of theft and deception could be levelled at the individual, the police would probably see it as a disciplinary issue to be dealt with by the authority. Nevertheless, the individual concerned would be unlikely to take the matter to court if the information was passed on to his employer.

5. Another council talked about its wish to share information with voluntary organisations and create a database listing all children in the city. When more than one organisation flags up a potential problem with one child, they get together to discuss the situation. Such an initiative would require parental consent - although this would probably not be difficult to acquire.

6 Modern medical care increasingly demands the rapid availability to health care professionals of accurate information from a variety of sources on the treatments that a patient is (or has been) receiving. In their Status Report 'Right Data, Right Place, Right Time – Joined-up Medical Records?' of January 2003, EURIM's Medical Records Group considered the split of roles and responsibilities between information officers tasked to make information available and data protection officers tasked to prevent abuse (with the consequent risk of adversarial approaches) to be counter-productive. They recommended that in order to ensure that information remains controlled, the current adversarial structure in which Caldicott Guardians' work to a set of principles focused on protection should be changed so that an Information Officer would have a Caldicott Guardian to advise on the handling of clinical data (including ensuring that it is available when needed, as well as protected from abuse), with accountability for the balance between availability and protection subject to external review. The full report is at:
http://www.eurim.org.uk/resources/status_reports/EURIMStatusReport8_ModGov.doc

Data sharing and matching remain grey areas - and this will probably continue unless and until an Act of Parliament is passed on the issue. Data sharing is not an end in itself, and the key to making it a success is building public trust on the issue. Without this, citizens will not be willing to hand over their information to public bodies.

5 Now add the effects of Freedom of Information

The Freedom of Information Act 2000 will also increase the importance of information governance issues in the public sector. It imposes a legal duty on public authorities to make more information available and therefore make it more accountable. Several groups of people (including journalists, politicians, private companies or communities) are likely to use the Act to access embarrassing or important information once it comes into force in January 2005.

It may well be the case that citizens end up confusing the DPA with the FoIA, even though the latter's scope is not restricted to personal data - financial, personal or political information can be released under its auspices. Other legislation, such as the Regulation of Investigatory Powers Act, which allows some public sector organisations to access the telephone and email logs of suspected criminals, is also relevant. The Government recommends that public authorities appoint a single person to deal with information governance and help spread awareness of the legal implications; this has already happened in some authorities.

Scenario 1
A local authority wants to set up a call centre as a one-stop-shop for all council service enquiries, contracted out to a third party. When a member of the public calls (or visits the centre in person) and identifies him/herself, a screen will appear in front of the operator with live links to all the files held by the council on that individual, to prompt the operator to discuss those issues. Markers will also appear which indicate if the individual is in arrears with any other payments to the council such as library fines etc.

Considering whether this could be done lawfully, it was decided that the authority could share any data except that which is connected to council tax. Good practice would be to inform the individuals at the point of capture, emphasising how this would help to deliver improved customer service. Details of the arrangement should also be included in the council's notification to the Information Commissioner.

Scenario 2
The Citizens Advice Bureau asks the local council for a list of people who are in arrears with their rent so they can offer them a money management course. The local authority cannot provide this information, as it would amount to marketing by a third party that would be using the data for a different purpose from which it was originally intended. However, the council could pass on details about the course to its tenants, provided they gained consent in some way.

Scenario 3
The local police chief asks you, as the area housing officer, for a list of all the Muslim students living on a particular housing estate. He claims this is so that they can be protected after a number of violent attacks on students in the city recently. Assuming the housing department had this information, it

could be passed on to the police under Section 29 of the DPA, provided the council was satisfied that the list would be used for the purpose stated. However, the local authority is not under an obligation to share the data.

Scenario 4
Recently there has been a lot of damage and graffiti in local bus shelters. The Passenger Transport Executive now wants to take pictures of the alleged offenders from the CCTV system and put them on posters on bus shelters and bus stations for people to recognise and phone Crimestoppers. Some of the pictures appear to be of young children.

Passing over the footage would be illegal for privacy reasons. The individuals concerned are only alleged offenders, and displaying pictures of children (who may not be old enough to be charged anyway) in public is always risky. It is also unlikely to solve the problem of graffiti.

Scenario 5
Each council department has developed its own 'blacklist' of abusive or violent customers. Some keep track of places where the officers think there may be problems; others issue this list to all their officers who go to visit customers in their own homes. Some post it in staff canteens in council offices. The local one-stop-shop, comprising of council, health service, Inland Revenue, police and benefits agency have expressed an interest in sharing lists compiled by the local authority of violent or abusive customers amongst its clerks.

The council should develop a coherent policy on the list, to be 'owned' by one individual, detailing how long the information should be kept and objective criteria outlining examples of behaviour that would lead to an individual being blacklisted. Ideally, the people concerned should also be notified, though this might aggravate the situation. Having a list is fine for internal purposes (though it should not be displayed publicly), but sharing it with other organisations could be controversial, even though they may have legitimate concerns about protecting their employees. The information should be provided on a need-to-know basis in both the council and one-stop-shop, rather than being accessible to all staff.

6 Proposals for Further Activities

At the EURIM data sharing group meeting of 29 July 2004, it was acknowledged that the generation of a data-sharing process map was presenting difficulties, which reflected on the severe problems encountered with data sharing at the practitioner level. It was, nevertheless, agreed that the process map idea should be pursued, however difficult. A process map or flowchart should be able to help decision-making where circumstances can be predicted; at least it should expose the blocks to data sharing, and identify whether these are attributable to the DPA or not. EURIM will approach the Information Commissioner with the aim of constructing a process map or flowchart of steps leading to data sharing decisions at the practitioner level, so that practitioners could be assured that the decisions they take are *intra vires*.

The idea of a process map or flowchart is to help people with interpretation, and to help break down the issues into a number of areas that define the type of data sharing to be applied. The flowchart might be constructed according to questions that should be asked for sharing data, although it is acknowledged that there is a limit to the assistance that a flowchart can provide in respect of the detailed questions that arise.

EURIM will also organise discussion on the desirability and/or practicality of legislation on the issues of consent, the lawful acquisition of data (perhaps along the lines envisaged in the ID Cards Bill but going beyond ‘mere’ identity) and governance (including penalties for unauthorised access, amendment and abuse (already raised in the context of the draft ID Card legislation).

The working group is grateful for the help of Ibrahim Hasan, trainer and writer on information law issues with Act Now Training (www.actnow.org.uk*) and IPF Associate, in the preparation of this report.*

