New Powers against Organised and Financial Crime

Home Office

October 2006

Chapter 1: Data Sharing

General Comments

There is undoubtedly a need for the greater capacity for government departments to share data. Greater data sharing could help to reduce fraud, and should make the delivery of public services more efficient. However, greater data sharing brings with it increased potential for intrusion into peoples' lives and infringement of their privacy. Hence, any data sharing should be carried out in a manner that minimises the negative impacts on privacy.

People occupy many roles. For example, one person may be someone's employee, someone's parent, a member of a support group, a hospital patient, a member of several professional bodies, a victim of a crime, the holder of a free bus pass, a receiver of state benefits. In principle, it is always possible for an individual to keep these roles separate, and there may be legitimate reasons for their doing so – for example, they may not want their employer to know personal information about their current or past health, or they may not want their employment history known to their doctor and so on. The more that information about the different parts of an individual's life is linked together, the more full a picture of them is created – revealing their history, their day-to-day activities and their general behaviour. The more a full picture of them is available, the more restricted the personal privacy they can enjoy and control.

In a report to be published later this year, entitled 'Dilemmas of Privacy and Surveillance: Challenges of Technological Change', The Royal Academy of Engineering has investigated the potential impact of technologies – especially technologies for collecting and processing personal data – on individuals' privacy. In the report the Academy looks at the kinds of society that would develop if technologies are developed and used in given ways. The report distinguishes between a 'big brother' society and a society of 'little sisters'. In the former society, authorities have access to a great deal of personal information, and can know almost everything about citizens, while the citizens are not always aware of exactly what is known about them. In this society people have little privacy – their lives are transparent.

In the little sister society, there is no single big brother watching everyone, but many little sisters (eg, government departments, banks, health clinics or doctor's surgeries) that have 'secrets' about you. If none of the information known to little sisters raises concerns, they will keep it secret. It is only if the information that little sisters have arouses significant suspicion will it be shared with other little sisters. Only once these lines of communication are made is a fuller picture of an individual revealed. But this is only done where there is good reason.

Depending on how they are carried out, the proposals in this consultation could lead to either a big brother or a little sister society. If data matching goes on routinely, without anonymising that data, a 'big brother' will be created who is privy to the private lives of most citizens. But if data matching only goes on when there is very good reason, then we might have a society of 'little sisters' who can be trusted to protect privacy until they have good reason not to.

The Academy's report would certainly recommend that it be made easier for different departments to share information. The current situation is not yet big brother nor little sister – but is a somewhat chaotic situation where data is kept by different institutions without clarity or consistency over who controls and maintains it, and how it is kept

secure. This situation is in itself a threat to peoples' privacy as their personal data is not properly maintained. More systematic ways of dealing with personal data are necessary. This will make data sharing easier – though data sharing must still be strictly controlled, as the answers below indicate.

Response to the Consultation Document

Q1 Should public sector information on suspected fraudsters be shared more widely within the public sector and with the private sector to prevent and detect fraud? What sort of safeguards would you expect to see? What do you believe the most appropriate vehicle for data-sharing would be?

Information on suspected fraudsters should be shared when, but only when, there is good reason to suspect fraud. The process should initially be rolled out by sharing data only amongst key bodies (ie, those listed in the consultation document). If the data sharing is deemed effective, and provided there have been no significant technical problems or misuses of shared data, then the process may be expanded.

The following safeguards are necessary:

- Any searches that do not turn up a case of fraud should be destroyed swiftly, so that there is nothing associated with a person's records that suggests involvement in fraud when investigations have revealed no further evidence of fraud.
- Any checks to ensure an individual's entitlement to a public service should not go beyond that which is necessary for establishing entitlement. Records of data irrelevant to the application should not be shared when checking the application.
- People should be made explicitly aware that if they apply for a service, checks will be made on them, and they should be made aware of the nature of the information that will be checked. They should explicitly consent to this checking. It is acceptable to state that they cannot access the required service or receive the required benefit unless they consent, but they should be given this choice.
- The operatives doing the data sharing and accessing the data should be well trained and closely supervised so that the personal data of individuals is not put under threat due to negligent or malicious misuse.
- If data sharing to prevent fraud becomes routine, it is essential that there are very stringent methods in place to ensure that the data is perfectly up to date. If suspicions of fraud arise because data held about an individual is out of date – eg, it has not been recorded that they have ceased collecting housing benefit – this will put them under unfair suspicion and will mean that information about their private lives is put under scrutiny without good reason. Obligations need to be placed on those who store or communicate such information as to its security and integrity. This might extend to formal obligations to update and validate such information and detail the conditions under which data might be held or deleted after a period of time. Obligations should extend to those accessing or using the data and details regarding how long such data might be retained should be released with the data.
- Similarly, it is essential that errors in peoples' data are minimised and if made are rectified swiftly. Individuals should be able to access the information that government departments and agencies hold about them so that they can discover any errors that have been made and have them rectified.

- There should be statutory compensation (without the need to prove negligence) for anyone who can show that they have suffered non-trivial damage as a result of the sharing of inaccurate data, the retention of data about an investigation that proved negative, or the misuse of personal data.
- Specific Codes of Conduct may need to be published to give confidence to the citizen as to how such information may be retained and used. A separate Statement might be published to explicitly state the rights of individuals and detail how they might validate information held on them. This would be a right to validate the items of data, rather than to know how it might be used or the details of any investigation.
- The role of the Information Commissioner may need to be expanded or a similar body created to 'regulate' such use of information. The use of data could be subject to regular independent scrutiny, as for example with some aspects of information gathering for intelligence and security purposes, with an independent report on the veracity of any processes produced on a regular basis. There could be parallels to those implemented as part of RIPA (Regulation of Investigatory Powers Act 2000) in relation to interception of communications.

Q2 Should the scope of the National Fraud Initiative be expanded and placed on a statutory footing in order to increase its capacity to detect fraud within the public sector?

The National Fraud Initiative may involve the kind of data matching that is routine for credit checks that are carried out when a person applies for a financial product, but they have the potential to be more intrusive. This is because they are likely to reveal facts about a person's health and any sickness benefit they have claimed, racial or ethnic origin – information that is generally considered 'sensitive' in the Data Protection Act 1998. Hence, the safeguards on such an initiative need to be more stringent than those on credit checking processes.

It is again essential that, if data matching is to be carried out, all of the data that is to be matched is kept up to date, so that people are not put under suspicion due to inconsistencies between outdated records. The burden of keeping data up to date should not fall on the individual, except where that duty already exists. If the Home Office initiates an investigation, it should first verify the data that led to the suspicion. Again there should be statutory compensation for people damaged by investigations that prove groundless – otherwise there is a risk that the investigations themselves can be used as a form of oppression – as IRS investigations in the USA are sometimes seen to be.

In order to protect peoples' privacy, the datasets that are matched in the NFI should be anonymised until reason for suspicion arises, so that the NFI exercises do not reveal full pictures of any given individual as a matter of course.

Q3: We would welcome your views on SOCA matching Suspicious Activity Reports received from the regulated sector against a range of public sector databases.

This kind of data matching seems to be acceptable, as it appears to be the kind of situation where a 'little sister' has good reason to reveal information. However, details about the kinds of information that would form the basis of a Suspicious Activity Report and would hence give reason for matching that data against public sector databases must be made public and be supported with clear justifications.

Q4: We would welcome your views on what you would regard as appropriate and targeted data mining of public and private sector databases to detect and prevent criminal activity, and what the appropriate safeguards for such exercises should be.

It is absolutely essential that if large scale data matching or data mining processes are to be carried out the data should be anonymised until there is reason for suspicion. Otherwise data mining and data matching will seriously encroach on individuals' rights to privacy, since it will piece together and present together various pieces of information about different parts of their lives.

Profiling can often be unsophisticated, and people can fit bad profiles for innocent reasons. Hence there must be a very strong reason for following up the results of data mining and data matching, and the profiling techniques should be frequently revisited to make sure that they are as effective as possible. It is essential to ensure that the technology used for data mining is state of the art, including the technology for encrypting the data. It is, again, necessary to ensure that the data mined is up to date. Without tight controls on the quality of the data and of the technology used, peoples' privacy and personal freedoms are at risk.

Access to the records to be profiled and the results of the profiling should only be granted to well-trained and closely monitored staff in order to limit the possibility of negligent or malicious misuse of the data being processed and the results that are generated.

There should be regular audits to show that the costs of data mining are outweighed by the benefits. These costs include the time it takes, the financial cost it incurs, and also the potential threat to peoples' privacy.

People should be made aware that their personal data may be subject to profiling, and what might happen if they are found to fit a dubious profile. They should be made aware when any action taken against them is due to the results of profiling. They should be given the right to explain why their behaviour fits such a profile, if they believe it is for innocent reasons.

There should be statutory compensation for mistakes that occur as a result of data mining or profiling. If mistakes were to be routinely compensated, then the profiling method would be more likely to be accepted. The small amount of money needed for compensation would a small price for the public purse to pay to compensate individuals for damage done as a side-effect of the greater good.

Submitted by:
Mr Philip Greenish CBE
Chief Executive
The Royal Academy of Engineering

Prepared by:
Dr Natasha McCarthy
Policy Advisor
17th October 2006