

ALL PARTY GROUP ON JUNK MAIL – INVESTIGATION INTO DATA MANAGEMENT

EVIDENCE SUBMITTED BY THE INFORMATION COMMISSIONER

I welcome the invitation to submit evidence to the enquiry being conducted by the All Party Group on Junk Mail into the management of personal data in the public sector.

I note that the Group's remit is ambitiously broad. Given the breadth of the inquiry it would be possible to submit many pages of evidence and comment. However, partly because the timescale is quite tight, I will confine myself to making a brief and focussed submission.

OUR FOCUS

You make clear that your primary focus is on fraud and waste arising from mismanagement of data. Our focus is on whether organisations comply with the 'rules' of good information management set out in the Data Protection Act 1998 (see Annex) and the detriment that is, or may be, caused to individuals where these 'rules' are not followed. Whilst the detriment, or potential detriment, may well include becoming a victim of identity fraud (which can obviously cause victims a great deal of distress and difficulty) our focus is on the mishandling of personal information that leads, or may lead, to detriment rather than the detailed nature of the detriment itself. Similarly, whilst failure to comply with the 'rules' will often lead to inefficiency and waste (for example, inaccurate records leading to over-payments), our focus is on the failure to comply with the rules, and the consequences this has for individuals, not on the waste itself.

It is inevitable that we have a better appreciation of what can and does go wrong than of best practice models within the public sector. It is inevitable that we hear of things that have gone wrong. Those who are exemplars are much less likely to come to our attention for the simple reason that they are unlikely to provoke complaints from individuals or adverse media reports.

SECURITY BREACHES

Recently there has been, quite properly, a great deal of focus on security provoked by a series of high profile incidents, particularly the loss of the HMRC discs. There have been a number of reports and a greatly increased focus on strong corporate information governance. Correctly there has been great emphasis on board level responsibility.

It is clear that large public sector organisations face particular challenges. HMRC, the product of the merger of the tax and customs authorities, is a very large organisation, employing nearly 100,000 people on many hundreds of sites. Ensuring that staff throughout such an organisation are fully aware of their own roles in the proper handling of personal information is a major challenge. Inevitably there can be tensions between trying to be efficient and to avoid unnecessary costs on the one hand and ensuring personal data is properly protected on the other. We think it is important that organisations make clear to staff that it is right to raise any misgivings they may have about how the organisation handles personal data.

PRIVACY IMPACT ASSESSMENTS

We firmly believe that that sensible planning and forethought are essential. We are pleased that government departments are showing a growing interest in carrying out Privacy Impact Assessments. PIAs are intended to be built into the planning process when organisations are considering initiatives which will involve the processing of personal data. They are designed to ensure that potential privacy risks are identified at an early stage so that less privacy invasive alternatives may be considered or steps taken to mitigate the risks.

PRIVACY BY DESIGN

We are keen to promote Privacy by Design and commissioned a report which is publicly available. This concept is intended to encourage organisations to design privacy into their systems. This involves considering privacy risks at the outset with processes developed, and appropriate technology used, to minimise those risks.

The Privacy by Design philosophy is not only relevant at time of commissioning major new IT systems. It is important to review existing processes and practices to see if there are ways of reducing privacy risk by adopting a 'data minimisation' approach. This involves collecting and using the minimum information necessary in the particular circumstances at hand. To give a practical example: if a government department is writing to pensioners to advise them of pension payments made it is unlikely to be necessary to include full details of the pensioner in the letter (full name etc) or the full details of the bank account including account number. From time to time those using automatic envelope stuffing machines find that something goes wrong. This can mean that one individual receives another's details, perhaps in addition to his own. Without data minimisation the additional information provided may be sufficient to enable an unscrupulous opportunist to use it to perpetrate identity fraud.

MINIMISING THE RISK

Where information needs to be disclosed to, or shared with, others only the information the other party needs should be released. When things go wrong, as from time to time they inevitably will, this can reduce the potential detriment caused to individuals. It is through important to recognise that depending on how records are structured and maintained, removing non-essential information may involve a cost.

We recently commissioned a report on the Business Case for Privacy which we expect to publish by the end of the year. It is intended to help organisations put a value on taking steps to minimise privacy risk, not just in terms of avoiding reputational damage and the costs of review and reparation, but also in terms of any more positive benefits in fostering trust.

Not surprisingly the major focus of our Regulatory Action Division currently is on breaches of security which put personal data and the individuals concerned at real risk. Many of the incidents we deal with arise from the risks posed by portable media – laptops, discs, pen-drives etc. Our view is that those using portable media to take personal data out of a secure office environment should ensure that they use appropriate encryption. Rather worryingly over the past year we have seen significant numbers of security breaches involving personal data of considerable sensitivity such as child protection records or medical records. It is a real concern that several

Healthcare Trusts have lost medical records, especially given that the importance of medical confidentiality has been established for centuries and certainly long before there was data protection legislation.

OUR POWERS

Our powers to take action in response to security and other data protection breaches are currently somewhat limited. We can issue enforcement notices to require organisations to change their practices, for example to require the encryption of all laptops used for processing personal data. Failure to comply with an enforcement notice is a criminal offence but we have no general power to punish organisations that fail to handle personal information responsibly. The Criminal Justice and Immigration Act 2008 introduced a power for us to impose monetary penalties on organisations for serious breaches of the Data Protection Act's good practice principle where these occur as a result of conduct that is knowing or reckless. This is a major step forward for us. We are currently working with the Ministry of Justice to develop statutory guidance and are waiting for them to set the maximum penalty so that the power can be brought into effect.

We do not have a general power to inspect organisations that are processing personal data to check that they are complying with the law unless we have the organisation's consent to do so. In wake of Government data breaches the Prime Minister gave us an assurance that we would be able to carry out what he termed "spot checks" of Government departments. The arrangements for such checks are now set out in an agreement with the Government, and the first such checks have taken place. More recently the Coroners and Justice Bill, which is currently completing its passage through Parliament, has introduced the possibility of my office issuing "assessment notices" which will give us the powers to enter premises to check compliance with the Data Protection Act. If the Bill completes its passage as currently drafted we will have a statutory basis for inspecting government departments without necessarily having their consent to do so. However this power will not extend to other public authorities or to private sector organisations unless the Secretary of State decides to designate them by order.

MATCHING RECORDS

You express an interest in ascertaining how effectively the government matches records with existing data bases. We do not have any detailed experience of working with government departments in this area though we do have experience of working with the credit reference agencies. These agencies hold consolidated records of the way that individual have conducted credit arrangements which are used to help lenders make lending decisions. Some years ago an individual's credit record was likely to contain records in a variety of variations of their name (e.g. John Jones, J, Jones, J. J. Jones, Jonathan Jones). Whilst usually this simply reflected the way that different lenders collected, recorded or reported the names of their customers it was difficult to be certain that all the records related to the same person, especially where a household contained more than one adult generation. This highlighted the unremarkable point that a uniform approach to collecting and recording names greatly increases the confidence with which you can match records from different sources. The agencies embarked on a concerted programme to ensure that contributing lenders provided them with identification information in a standard format which has

led to much greater certainty in linking individuals to records of the conduct of credit accounts.

Finally, and to end on a positive note, we have been involved with the Tell us Once initiative led by the DWP. This has involved the piloting of arrangements for enabling citizens to report major life events, birth and death, just once rather than having to separately report to a large number of bodies. Whilst this sounds deceptively easy in practice it is very complicated. The trials and pilots have been carefully managed to take into account citizens' needs, and to ensure the approach is viable. The pilots have demonstrated that there are unexpected benefits from adopting a more joined up approach which helps to ensure that those who need to be aware of a bereavement are informed (e.g. those responsible for issuing disabled parking permits or for medical equipment such as oxygen cylinders). Quite properly there has been great emphasis on careful planning, on testing hypotheses, and on learning from trials.

Christopher Graham
Information Commissioner

August 2009

Data Protection Act 1998

The Eight Principles of Good Information Handling Practice

Anyone processing personal data must comply with the eight enforceable principles of good practice.

They say that personal data must be:

- 1 fairly and lawfully processed
- 2 processed only for limited purposes
- 3 adequate, relevant and not excessive
- 4 accurate and up to date
- 5 not kept longer than necessary
- 6 processed in accordance with the individual's rights
- 7 kept secure
- 8 not transferred to countries outside the European Economic Area unless the country has adequate protection for the data.