

# Data Sharing Review

Richard Thomas and Dr Mark Walport

## Consultation paper on the use and sharing of personal information in the public and private sector

### Section 1: Background

#### Question 1.

Founded in 1991, The REaD Group plc pioneered a new, more efficient approach to direct marketing in the development of data suppression which improves the effectiveness of direct marketing practices.

The practice of direct mail has grown dramatically over the last two decades. In 2005 3.4 billion items of addressed direct mail and 13 billion items of unaddressed direct mail were sent out to UK households and businesses. Since 2003, volumes of unaddressed mail appear to be increasing at a rate of 1-2% a year. While targeted direct mail allows firms of all sizes to advertise their products and services to a wider customer base, it is important for companies, consumers and the community that this is done efficiently, effectively and with regard to the environment.

The REaD Group provides an extensive range of business to consumer and business to business data suppression products. It is instrumental in helping direct marketers clean-up their mailing lists by removing obsolete or unwanted names and addresses. This has benefits in improving the efficiency of direct mailing, reducing waste and the potential for identity fraud. Today, more than half of all direct mail sent out in the UK is cleaned by one or more of The REaD Group's suppression products.

#### What kinds of personal information do you collect, hold and share?

	<i>collect</i>	<i>hold</i>	<i>share</i>
fullname	25.9m	25.9m	25.9m
last known address	25.9m	29.5m	29.5m
date of birth	2.8m	2.8m	nil
date of death	2.8m	2.8m	2.8m
current address	2.8m	2.8m	10.2m
new occupier	nil	nil	3.8m
next of kin details	2.8m	2.8m	nil

#### How do you collect, hold and share such personal information?

<i>collect</i>	<i>hold</i>	<i>share</i>
through a variety of sources including methods completed by individuals i.e. forms, website, etc.	on secure servers	via secure ftp sites and under strict licence agreements supported with onsite visits

**For what purposes do you collect, hold and share such personal information?**

To enable direct marketers to clean-up their mailing lists by removing obsolete or unwanted names and addresses.

**Section 2: Scope of personal information sharing, including benefits, barriers and risks of data sharing and data protection**

**Question 2.**

By using high quality data suppression techniques to ensure organisational databases only contain accurate and up to date information about private individuals, it is possible to eradicate instances of direct mail and communications being incorrectly addressed. This sharing of personal information benefits individuals, organisations and the environment by:

- stopping the annoyance or distress of repeat incorrect mailings
- drastically reducing unnecessary environmental waste
- increasing the efficiency of mailings, and
- helping to reduce deceased identity fraud

The direct marketing industry has been identified as a source of unnecessary waste and is often viewed as an annoyance. Currently the Direct Marketing Association actively promotes the Mailing Preference Service (MPS). This service aims to stop direct marketing by enabling consumers to have their names and home addresses in the UK removed from the databases and lists used by the industry. However, MPS often fails to fully stop direct mail and provides no middle ground for the consumer to pick and choose which organisations may send them information. *itsmypost.com* was set up by The REaD Group to offer more choice to the individual about what direct mail they receive. For a small annual fee the system will send emails to those companies from which the individual no longer wishes to hear. The company will then be legally obliged to stop sending direct mail to this person under Section 11 of the Data Protection Act 1998.

Inaccurate and out-of-date databases often lead to direct mail being sent to deceased individuals, sometimes over ten years after their death, which can cause emotional distress to bereaved families. Furthermore, direct mailing of this sort can lead to instances of Impersonation of Deceased (IoD) fraud. Identity fraud is a national problem; a credit card application sent after an individual has died to someone who has deceased falling into the wrong hands can contribute to that deceased's identity being stolen.

**Reducing waste**

There is no doubt that direct marketing is responsible for a significant amount of waste. Direct marketing material is estimated to account for approximately 550,000 tonnes of the household waste stream, which is around 4.4% of the UK's annual consumption of paper and board.

The REaD Group is committed to reducing the effect of the direct marketing industry on the environment and we have developed many of our products with this goal in mind. By ensuring that direct marketing is not sent to individuals who have moved, deceased, or people who do not want to receive certain mailings, we can make direct mailing more efficient for companies and reduce the amount of material being produced whilst empowering the consumer to have a choice about the post they receive.

### **Making organisations more efficient**

Direct marketing is a valid and effective way of enabling both public and private sector bodies to contact a large number of people at one time. However, direct marketing is often carried out in an inefficient and irresponsible way due to the misuse of personal information. By using up-to-date and accurate information for mailings, as opposed to out-of-date lists which include people who no longer live at the address or who are deceased, organisations produce less direct marketing but will achieve a similar success rate.

We believe that the responsible use and maintenance of data is therefore in the best interests of organisations who can then target their mailings more accurately, but also guard against the inappropriate use of data and information.

### **Question 3.**

The REaD Group's services, *The Bereavement Register* and *itsmypost.com*, operate data suppression on the basis of the informed consent of individuals, thereby balancing the right of organisations to advertise with the privacy of individuals. The sharing of data without proper consent, or safeguards, carries with it a number of risks outlined, namely:

- increasing the annoyance or distress of repeat incorrect mailings
- increasing the likelihood of identity/impersonation of deceased (IoD) fraud
- creating unnecessary environmental waste, and
- ensuing that mailings remain inefficient

In terms of IoD fraud there are a number of well-publicised cases where unrestricted data sharing has led to criminality.

#### *Case study 1: Rosemary Osmand*

*Four months after the death of Rosemary Osmand, 86, bailiffs were sent to her address to demand the payment of thousands of pounds in bills charged up by her credit card. Following an investigation, it emerged that Rosemary Osmand's identity had been targeted by a sophisticated criminal gang, which had monitored the local press for death notices. The gang subsequently were able to gain access to the empty house via estate agents and steal junk mail, including a credit card application form, which had been sent to Rosemary in the intervening period. (Source: How ID Fraudsters target the dead, BBC, February 2006).*

According to the UK's Fraud Avoidance Service, CIFAS, in 2006 there were 70,000 similar cases in Britain last year affecting more than 16,000 families. An estimated £250 million is lost a year through stolen credit cards and bank accounts.

**Question 4.**

There needs to be clearer definition on the criteria which guide the types of companies allowed to receive certain data. We highlight in our answer to Question 27 our concerns about the Supply of Information (Register of Deaths) Regulations 2007 Statutory Instruments, which we see as being framed too broadly and without adequate safeguards.

In the light of technological advances with encryption, the Review should also consider how information is transferred to organisations. The use of CD data sent by registered post to organisations on a regular basis and without proper safeguards, exposes public and private bodies to unacceptable risks.

**Question 5.**

It is not fully known how much data is currently being held by public authorities. As such we are not able to add further to this question. However this does highlight the lack of transparency for individuals regarding what information is held about them and where.

**Question 6.**

The practice of 'data warehousing' in the private sector, whereby personal information is stored in one place, but potentially used for multiple purposes is of concern. 'Club' or 'Reward' cards from high street retailers store large amounts of information which can be purchased by third parties. This can result in potential invasions of privacy, either directly or through assumptions about consumer behaviour.

At the moment there is little transparency about how this information is stored, how long it can be stored for and to whom it is shared. Current 'opt ins' and 'opt outs' to data disclosure for consumers do not use standard language, leading to misinformed consent about the disclosure of personal information to third parties.

**Question 7.**

Data cleaning and suppression should be seen as standard good practice across the public sector. This would have added benefits of improving the efficiency and customer service of public bodies involved in direct communication, consultation or correspondence with private individuals.

Lacking some of the commercial drivers that private sector organisations have can inhibit public sector bodies from realising some of the more immediate gains, which also can be felt in terms of waste prevention.

The new Government Strategic Marketing Advisory Board (GSMAB), to be formally launched in February 2008, should investigate how central government can use data suppression to increase public sector productivity.

**Question 8.**

The REaD Group plc has raised concerns with HM Treasury and the Registrar General about the Supply of Information (Register of Deaths) Regulations 2007 Statutory Instruments. Our full concerns are set out in Question 27. Further clarification on the process by which companies are vetted and policed are needed to ensure that the sharing of these important data set is not open to abuse.

**Section 3: The legal framework****Question 9.**

The REaD Group has no comment to make on this question.

**Question 10.**

The REaD Group has no comment to make on this question.

**Question 11.**

The REaD Group has no comment to make on this question.

**Question 12.**

The REaD Group has no comment to make on this question.

**Question 13.**

The REaD Group has no comment to make on this question.

**Question 14.**

The REaD Group has no comment to make on this question.

**Question 15.**

The REaD Group has no comment to make on this question.

## Section 4: Consent and transparency

### Question 16.

The REaD Group are strong believers in the use of consent as a key device in the use of personal information by third parties, especially in relation to direct mailing.

We estimate that on average each person in the UK gets about 120 pieces of direct mail a year. Research from YouGov shows that 72% of consumers want between 90% and 50% of their junk mail stopped – a staggering 1.8 billion items; (YouGov, January 2006) The REaD Group's **itsmypost.com** service was created specifically to ensure that customers only get the mail that they want. **itsmypost.com** provides an automated email or letter service that sends a request to stop processing your data to chosen companies by using the Data Protection Act 1998 to ensure that these companies stop processing your information. **itsmypost.com** generates automated emails that get sent directly to your selected companies. This service costs £4.95 a year and is currently used by over 85,000 customers.

This differs from the Mailing Preference Service (MPS). While this service is widely used by the direct marketing industry members, it will not stop mail from companies that people have dealt with in the past, it will only stop mail from companies that people have never had contact with before.

In using **itsmypost.com**, customers communicate directly with these companies (using the suggested wording of the Information Commissioner's Office) to tell them they do not want that organisations mail, forcing firms to desist.

Once the selected company has received an email or letter from the private individual they are obliged by law to remove their name from their database or mailing list. The service has been designed to be brand specific enabling people to make their own choices.

The issue of consent is more important for those involved in information exchange following the case of Brian Robertson and the Electoral Roll. In this action, the European Court of Justice determined that supplying the Electoral Roll for non-electoral purposes without knowledge or consent of subject was, in principle, an interference with the right to private life and privacy. Consequently, there are now two versions of the Electoral Roll, a full version (all UK residents) and an edited version (only residents who have give permission to have their details made publicly available). Currently only Government Departments and credit reference agencies have access to the full version.

### Question 17.

The REaD Group has no comment to make on this question.

### Question 18.

The REaD Group has no comment to make on this question.

### Question 19.

The REaD Group has no comment to make on this question.

## Section 5: Technology

### Question 20.

On account of the low costs associated with data storage, organisations are now more likely to hold onto data for much longer than they need to or should do. Historically, paper based or magnetic databases/information would have been disposed of much sooner as “junk”. Due to the technology revolution, it is today possible to store thousands of gigabytes of data within a very small area that a decade ago would have filled a storage building.

We believe that data is much more likely to be stored on a server which (a) may make information more accessible to people that ought not have access to it and (b) over time may become more vulnerable as initial security steps are overridden by complacency or changing practice and procedures.

Additionally, it is invariably cheaper to buy new information technology rather than upgrade existing infrastructure/equipment. Combined with the Waste Electrical and Electronic Equipment Directive (WEEE) it is also harder to dispose of such equipment. This means equipment with sensitive information is more likely to be dumped with the information potentially readily accessible to all.

### Question 21.

It is our understanding the law already does provide for technical safeguards however it is not effective enough. There are no punishments for breaches and organisations are currently not held accountable in the same way a bank that loses information is liable to refund any stolen money from an individuals' account.

We believe if the law included explicit requirements there is a danger that the requirements may become outdated or, if a hacker finds a way around the explicit requirements, that the law may end up recommending a failed process.

### Question 22.

As a general principle, if there is no need for specifically personal information to be held within data, it should always be anonymised. However, if the reason for data sharing is to share personal information then this would be counter-productive. For example, a key purpose of our products and services is to identify individuals that should no longer be mailed; were the data to be anonymised this would not allow organisations to identify such individuals. Owing to the nature of our business, it would not be appropriate for us to use such techniques in the vast majority of circumstances.

We do not believe there currently is sufficient advice regarding the deployment of such techniques.

## Section 6: International comparisons

<b>Question 23.</b>
---------------------

The REaD Group has no comment to make on this question.
---

<b>Question 24.</b>
---------------------

The REaD Group has no comment to make on this question.
---

<b>Question 25.</b>
---------------------

The REaD Group has no comment to make on this question.
---

<b>Question 26.</b>
---------------------

The REaD Group has no comment to make on this question.
---

## Section 7: Additional questions

### Question 27.

The Supply of Information (Register of Deaths) Regulations 2007 Statutory Instruments, which were laid before Parliament on 10 December 2007 and became effective in January 2008 complicate the situation as regards the scope of this consultation. While it is important to cleanse databases of outdated records, this process must be undertaken in a way which prevents rather than exacerbates the potential for identity fraud or personal distress. As such it is surprising such measures were taken outside of the scope and recommendations of the Walport Review.

Our primary concern is that the wording of the Regulations as they currently stand is very broad in nature and need clear safeguards to protect against identity fraud. They permit the supply of information contained in any register of deaths held by the Registrar General potentially to a wide range of recipients including credit reference agencies, banks, building societies, pension schemes and “any person or body undertaking list cleaning as defined in these regulations”. The purpose of the scheme merely “envisages” the data being used for the “prevention, detection, investigation or prosecution of offences.”

We have a particular concern that the wording of the regulations is so broad that an unintended consequence will be that any individual or organisation with a claim to undertaking ‘list cleaning’ will be able to access this data. As we noted above, death registration information is particularly vulnerable to identity fraud, with fraudsters able to use the detailed information currently held to impersonate the deceased.

An associated risk is that death registration information could be used for commercial purposes. There is already evidence of personal data being used by unscrupulous firms seeking to promote products to the recently widowed or bereaved, causing people unnecessary distress by targeting them with ‘junk mail’.

Additionally, whilst deceased individual information is not covered by the Data Protection Act, if this information were to fall into the wrong hands, it is, more often than not, the bereaved who will suffer any abuse of the deceased’s information. We would argue that such data sharing could result in an invasion of bereaved’s right to private life and privacy as with the Electoral Roll case as referred to in Question 16.

We believe that this consultation and the Review should examine further safeguards to ensure that death registration data is indeed used for the purposes of prevention, detection, investigation or prosecution of offences. We remain concerned that there is not a clear set of safeguards concerning breaches of these uses, or proper policing of how these rules would work in practice.

### Question 28.

The REaD Group has no comment to make on this question.