

# 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

### List of questions for response

We would welcome responses to the following questions set out in this consultation paper. Please follow the question order as set out in the consultation paper, leaving a blank response box for any questions not answered.

Please email your completed form to [contact@datasharingreview.gsi.gov.uk](mailto:contact@datasharingreview.gsi.gov.uk)

Alternatively you can send a hard copy response to:

**Data Sharing Review Secretariat**  
**5.26 Steel House**  
**11 Tothill Street**  
**London**  
**SW1H 9LJ**

Thank you.



Please note that the response below is not a statement of COI policy but a considered opinion based on experience from practitioners.

### Section 1: Background

Question 1.

Comments: **Background**

Whilst many Government Department's may be rightly looking at this paper from an operational viewpoint and looking more at the identify authentication, fraud prevention type issues data sharing can help with, COI as a communications and information provision is considering this mostly from that viewpoint and our response is framed in that manner.

COI operates in partnership with various government departments and NDPBs to deliver publicity messages through a range of media (paid and unpaid) to the citizen. These

messages result directly from government policies and there is a duty (statutory or presumed) to inform the citizen of their rights and responsibilities.

As well as more broadcast media, key channels that have proven successful over the last two decades are those that involve direct communications to the individual using individual data, primarily direct mail, but lately email and SMS text. Lists of contact details and other appended data (to allow for segmentation and individualisation of messages) are therefore sourced from:

- a) The commercial sector (list owners, brokers, questions, lifestyle surveys etc)
- b) Internal departmental data, where this is made available

and communications are sent to alert citizens in the existence of initiatives and/or as part of ongoing programmes to affect behaviour change.

We would therefore generally require name, address and contact details as the key elements but also e-mail and phone number. Subsidiary to that other data fields such as income levels, marital status, employment status, number of children in household, socio-demographic status (usually delivered from postcode) and a potential host of other declared interest or derived factors then allow us to:

- a) Segment a broad audience into specific groups
- b) Target those groups through personalisation and individualisation of content, tone, emphasis or format to make the communication more lively, relevant and motivating
- c) Exclude those groups who clearly would not be eligible / interested etc and thus reduce wastage

Data is generally held within our supplier base of data bureaux / analytic companies, mailing houses and contact centres. Data sourced from departments is usually difficult to obtain. This is partly because of ignorance of the application of the DPA or the fact that the data was not 'opted-in' in the traditional marketing sense but captured as part of the regular transactional operational services with that department. It would be unlikely at point of capture that any department could also offer the opt-in to a host of other initiatives or departments that could potentially be of benefit to that citizen.

This may in part be due to a lack of understanding or clarity of the DPA and how it applies in a Government context and also and the skills to forward plan data collection, in terms of the opt-in to a wider communications within a department, also the type of data you can request and once you have the data what you are permitted to do with this information

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

Question 2.

Comments: Often on a given communications campaign we are using quite broad media (eg TV, Radio) to find people to get them to 'hand-hold' and identify themselves, when it is obvious that the data on that individual is already held within either the sponsoring department or another department and a more direct approach, instead off or alongside the

more awareness driving media, would be more beneficial. However in many cases this data is either

- a) Not known to be available or;
- b) Not made available for these purposes.

An example some years ago was a campaign for DWP who were trying to locate people who had been long term sick in a particular category. The department held data of these individuals but would not release it for direct communication and instead field marketing and posters in GP's surgeries needed to be deployed involving a lot of unnecessary waste.

Conversely an example of successful data sharing occurred when UK Online allowed access to Bite Size to their response data. UK Online was trying to convince people to go online and be more computer literate. Bite Size offered free courses for people, many of which were computer skills. A perfect match and a joint mailing ensued.

Another example might be (and indeed I have suggested this in the past) is data sharing between Blood Donation and Organ Transplant Donation as the people who sign up for one are more likely to sign up for the other. The organisation is, in fact, now one and the same yet keeps very separate.

There are numerous opportunities a 'joined up' approach to data sharing for information campaign purposes could bring which benefit individuals, society and government through:

- a) Better targeted more relevant initiatives
- b) Less wastage (both economic and impact on the environment)
- c) More joined up messaging
- d) More cost-effective routes to market and response generation

People instead tend to opt-in to various isolated initiatives creating little 'pots' of data that can only be used for that purpose – again wasteful duplication.

Sharing information at the moment in government, where it does happen is very much restricted to fraud prevention and/or identification verification.

### Question 3.

Comments: It is odd that the Data Protection Act and general fear of data misuse, identify theft etc is such that it convinces citizens not to part with their personal data, interests etc and as a result commercial marketers and government are thus less able to precisely target them leading to a more 'scattergun' approach which can annoy them. Whereas if they did give information or were happy for data sharing they could be approached in a more tailored fashion or excluded from the communication. This does however rely on all useful and sharers of data being responsible and sharing only when it is appropriate.

## **Risks**

- a) Inappropriate sharing leads to message or approaches that are unexpected or unwelcome and not what would be considered 'reasonable usage'.
- b) Transfer of data between parties increases the risk of data loss or misappropriation (through this should be easily minimised through proper IT security moves)
- c) Sensitive data or other data that isn't required for the purpose at hand is transferred alongside the core 'needed' data
- d) Reinforces a 'big brother' government knows everything about me (that said some pensions credit research we have suggests that people have kept expectation and often think government should know more what it makes contact and is surprised when it doesn't and sometimes annoyed when they have to give the same information over and over to multiple departments).

For example Health are about to launch an obesity programme to create a database and CRM programme. A core at risk audience of parents (some 500,000) already sit on the Healthy Start programme database. Fortunately this one will permit some form of sharing as the original data-capture 'opt-in' was quite wide in terms of healthy eating messages.

'Piggy-backing' and combinations of message from different departments would show a joined up 'whole life' approach recognising the different factors at play at any given situation or life stage.

There was talk of a central 'data spine' some years ago with ONS in the lead which subsequently was morphed into identity cards. At the time the main purpose was to have a central register of basic details departments could share to avoid duplication, citizens having to inform government departments by department of charges, and prevent fraud. However little thought had been given of that time as to the implications for:

- a) 'Marketing' communications to the citizen from government
- b) Data Protection – eg can a citizen 'opt out' of communications from government, wholesale, department specific or campaign specific? Are all citizens (and businesses) by definition 'customers' of government so there is a presumed relationship and duty in terms of communicating rights and responsibilities? This is a fundamental question.

Question 4.

Comments: No specific comment

Question 5.

Comments: No specific comment

Question 6.

Comments: No specific comment

Question 7.

Comments: No specific comment

Question 8.

Comments: No specific comment

### **Section 3: The legal framework**

Question 9.

Comments: No specific comment

Question 10.

Comments: The second DPA principle is, in theory, sound. However there are issues on interpretation and often there is a struggle to transfer a very private sector orientated act into the Government space. The primary reason behind the Act appears to be to prevent unwarranted or unwelcome marketing or sales approaches to an individual and to hold data securely to prevent misuse.

For government this presents an immediate issue. Whilst we may use the terminology of the marketing communications industry and the same media and vehicles of communication as the private sector, is what government imparts 'marketing messages'? Rather they are information alerts, attempts at eliciting, behaviour change, notification of law, rights and responsibilities or offers of support – all designed to improve the workings of society and the life of the individual so targeted – even if they don't want to hear that message to drink sensibly, give up smoking, exercise more etc.

Can someone opt out of receiving, say, a leaflet on preparing for Emergencies or Pandemic flu, which impact not only on that individual but society as a whole? Under present legislation technically they can. Should they be able to? As their ignorance could affect the safety of others. Is it unreasonable to suggest that a person who responded to a campaign of giving up smoking could subsequently be targeted with an 'exercise more' or 'drink sensibly' message from the same department – or is that a move too far? But, if a person of low income responded to DWP on a benefits campaign might it not be sensible for the OFT to see if that person has debt problems? Or Health to see if an elderly person receiving winter fuel payments needs help with keeping warm. The list of possibilities are endless and the benefits potentially massive. However a strict reading of the second principle of the DPA would prevent all such 'cross-fertilisation' and is often cited as the reason for such initiatives never being suggested or taken up.

That said, who decides what is 'reasonable usage' of data between public bodies, and indeed what constitutes a public body. There are numerous non-departmental - public bodies and some that are limited companies – e.g. Action 2000 or Digital UK that did/do public work but aren't technically government.

Would DWP be able to, for example, pass a list of elderly disadvantaged people to Digital UK for them to follow up with direct messages or how to convert to digital – since they are the most 'at risk' group?

A further example might be BERR or Home Office communicating legal information to businesses, such as use of Illegal Immigrants or the creation of the new Independent Safeguarding Authority or changes in paternity rights. Could they have access to business data held by HMRC, for example, to try and maximise coverage (and save money) where a commercial business might not have such reach. Can a business opt out of communication (they can subscribe to MPS). Would such an opt out be a valid barrier if we are communicating a legal change? Would the same apply if it was just communicating business advice?

Question 11.

Comments:

Question 12.

Comments: The provisions of the Act we based on good practice common sense and thus should be sufficient. The ICO's own website shows many large companies and government organisations have been required to comply with the Act and sign declarations to that effect. However one suspects that most offenders will be smaller companies who are not aware of all the principles or do not have the mechanisms in place, yet may never be investigated, as they are too small. Some further clarifications on exemptions and some formal statement on levels of security that is acceptable to the ICO would be valuable.

Question 13.

Comments: No specific comment

Question 14.

Comments: The Privacy and Electronic Communications Regulation 2003 would have an impact on data sharing and the possibility of one part of government being able to contact an individual about a related or appropriate issue by electronic means (ie email or phone or text.)

Citizen's registering for the TPs, since it is a complete 'opt-out', to avoid marketing calls from the private sector could be denied to a government department trying to inform a citizen of their rights and responsibilities or even invite them to a local event that would be to their benefit. Similarly the provisions for e-mail marketing are focused on marketing messages from commercial concerns who are allowed to communicate if they meet the there criteria (obtaining details through a sale, similar products or services, and the opportunity to refuse was given when details were collected).

Who is to say whether information or giving up smoking and not drinking heavily are 'similar services'? And, when data is collected it tends to be specifically by campaign or department and it is not impossible to offer anyone the ability to 'opt-out' of communication from government as a whole. Indeed it is fairly impossible to allow someone to 'opt-out' of communication from one department given the decentralised nature of many departments.

Question 15.

Comments: No specific comment

#### **Section 4: Consent and transparency**

Question 16.

Comments: Because of the nature of government and the various legal forms government takes – e.g. the crown is invisible but some parts of 'government' could actually be separate legal entities and even with limited companies it would not always be clear when consent is required. In such cases it would be a burden on the tax-payer to communicate with all the people to alert them, ask for their permission or 'opt-out' eg 'I'm writing to you to tell you we want to write to you'.

Question 17.

Comments: An example: The Navy has a shortage of pilots and yet the RAF has many respondents who have asked to be a pilot but not enough vacancies. Do the RAF have to write to these people to ask for their permission to allow the Navy to contact them? Or do they pass the details to the sister service (part of MOD) who contact the individual to say that whilst the RAF don't have any vacancies, they could potentially be a pilot in the Navy (something they may not have thought of because the Navy is about ships for most people), referencing that the RAF have passed their details on. Such a common sense approach would help all parties. Again a strict reading of the data protection act as regards sharing without consent would potentially prevent this.

Question 18.

Comments: Potentially communications could identify the source of the record that prompted the communication in the first place. For example, the Navy could highlight the fact that the RAF passed the data on as a 'big benefit' and sharing sensible 'joined up' Government that is acting on behalf of the citizens. Similarly commercial concerns can often say 'our records show you're interested in' or similar. However sometimes such disclosure could be seen as a bit clumsy in a creative context but nonetheless a more open policy could be pursued.

Question 19.

Comments: The new framework is very useful, though was not publicised well. Privacy Impact Assessments -the process looks quite detailed and cumbersome and time heavy, which may be very difficult in a marketing context where speed of opportunity is often of the essence.

## **Section 5: Technology**

Question 20.

Comments: No specific comment

Question 21.

Comments: In light of recent events it would be very useful for minimum levels of security to be enshrined. It has also become apparent that accepted methods of security in the private sector are often not acceptable in the public sector (whose systems and approaches often lag behind and where caution is higher).

Question 22.

Comments: No specific comment

## **Section 6: International comparisons**

Question 23.

Comments: No specific comment

Question 24.
--------------

Comments: No specific comment
-------------------------------

Question 25.
--------------

Comments: No specific comment
-------------------------------

Question 26.
--------------

Comments: No specific comment
-------------------------------

### **Section 7: Additional questions**

Question 27.
--------------

Comments: For government communications a review of the DPA and data sharing gives opportunities for some clarification on what can be potentially permitted in an area which does not quite fit into the commercial sector model and where much of the use of data is both of benefit to the individual citizen and to society as a whole.
---

Question 28.
--------------

Comments: No specific comment
-------------------------------

### **Overall summary**

This is a significant issue within Government as the literal reading of the DPA currently prevents much inventive cross fertilisation and channel opportunities to get key Government messages across. As mentioned whilst we use the terminology of marketing, are Government communications sufficiently different (and indeed coming from a different strategic objective – to improve society as opposed to making profit) to merit some different treatment as regards the DPA? Is this a blanket treatment or does this vary by topic area or degree of seriousness/risk? What is considered reasonable and who makes that decision?