



# **Research into the use of personal datasets held by public sector bodies**

Final report for Council for Science and Technology (draft)  
**October 2005**

working with you

to improve social results

**252B Gray's Inn Road, London WC1X 8XG**

**tel: 020 7239 7800 fax: 020 7837 5800 email: [office@opm.co.uk](mailto:office@opm.co.uk) web: [www.opm.co.uk](http://www.opm.co.uk)**

## Contents

Summary .....	2
1. Overview of participants' attitudes.....	4
Forming a view.....	4
Three views on the topic.....	5
Factors contributing to views .....	7
2. Stage 1 .....	9
Introduction .....	9
Trust.....	9
Access .....	10
Efficiency.....	10
Accountability.....	11
3. Stage 2 .....	12
Introduction .....	12
Any change in attitude? .....	12
Trust.....	13
Guiding principles and safeguards.....	13
The case studies.....	16
4. Recommendations for future public dialogue .....	19
Appendix 1. Methodology and sample .....	20
Appendix 2. Discussion guides.....	22
Stage 1.....	22
Stage 2.....	25
Introduction – 5 minutes.....	25
Warm-up – 5 minutes.....	25
Video clips – 10minutes .....	25
Case studies – 20minutes.....	26
Developing common principles – 20 minutes .....	26
Feedback and discussion – 20 minutes.....	26
Public engagement – whole group discussion – 15 minutes .....	26
Final Review and wrap – up – 5 minutes .....	27
Questionnaires – 5-10 minutes .....	27
Appendix 3 – Research materials.....	28
The Khan family has the answers at last .....	38
Easy driving .....	39
Is your health information secure?.....	40
Pensioner gets the cash .....	41

To request a large-text version of this document, phone 020 7239 0877

## Summary

### Objectives, Methodology and Sample

This report provides findings from a project commissioned by the Council of Science and Technology. The overall objective of the project was to understand attitudes towards the use and sharing of personal datasets by public bodies.

- There were two parts to the research
  - Stage 1: 7 x 1.5 hour focus groups
  - Stage 2: 7 x 2.5 hour workshops (reconvened)
- Work was carried out in Belfast, Birmingham, Bradford, Cardiff, Glasgow and London. Sixty seven people took part in the first stage: sixty-six took part in the second stage.

### Key findings

- Participants fell into three broad groups:
  - Uninterested
  - Undecided
  - Objectors (tend to be from professional backgrounds)
- Participants' found forming firm views difficult, for the following reasons:
  - Lack of knowledge of existing data-sharing amongst public bodies
  - The proposals they were asked to consider being somewhat abstract, leaving many with unanswered questions
  - An assumption that the government can already find out what it wants about any individual, making it hard for them to see what difference would be made by greater sharing of information

The groups share in common a feeling of powerless or resignation, assuming that 'this is going to happen whatever we think'.

- Greater information sharing across public agencies is not seen as individually 'enabling' and many participants found it difficult to identify the specific advantages to them personally
  - Many felt that the advantages would all be on the government side, with individuals being left to pick up the tab
- Primary concerns were:

### Trust:

- In the ability of the government to undertake information sharing on a grand scale, a scepticism based on experience or awareness of problems with the CSA, Working

Families' Tax Credit, Passport Agency and their own experience of dealing with other government agencies

- In the integrity of Ministers and civil servants entrusted with their information

#### **Efficiency**

- A more streamlined interface between the individual and public agencies would be welcomed
- However, poor experiences lead to doubt in the capacity of government and public bodies in general to deliver the efficiency benefits suggested by greater sharing

#### **Accountability**

- The prospect of a large 'faceless' database not attached to a recognised government function (eg, health, taxation, policing, social security etc) leaves participants feeling of powerless

#### **Positive views**

- Attitudes towards information stored and used by healthcare professionals, for the purposes of individual healthcare or health research, are noticeably different to those towards information stored and used by other agencies and overall are positive
  - Affection for the NHS, together with more easily identifiable benefits, may explain this difference

#### **Principles & safeguards**

Participants identified a number of fundamental principles and safeguards that should govern any future plans for increased sharing of personal datasets held by public bodies:

- Protection of individual privacy is paramount
- The reasons for sharing information and the agencies having access to information should be clearly defined, agreed between the government and the individual and set down by law in advance of systems becoming operative
- Individuals must have easy access to their own information and details of how and with whom it has been shared
- The government should take responsibility for the accuracy of information held
- Information should be kept for a limited period only and then individuals should be asked to provide all information anew
- An independent auditor should oversee the system
- The Data Protection Act should be updated and strengthened
- If more efficient services are promised by the government as a result of the introduction of this system, the resources to ensure that this happens need to be in place

#### **Future consultation**

There is considerable enthusiasm for future consultation. However, proposals should be more clearly explained, with evidence of the difference to individuals that would follow from increased data-sharing and information provided on management, security and access

## 1. Overview of participants' attitudes

Attitudes towards the sharing of personal information are largely informed by the experience of providing information to commercial organisations. This gives rise to particular concerns, many of which are unlikely to apply in the case of public agencies. Foremost amongst these is being targeted for marketing purposes.

A majority of respondents said they gave personal information to both public and private sector bodies with little or no thought about the use to which it would be put, the extent to which it would be shared and with whom, or the protection afforded them under the law. A few respondents were aware of the Data Protection Act; most of these were not aware of its specific contents, though one who came across it in the course of his job suggested its scope was very limited. Others commented on how poorly it was drafted.

### Forming a view

Many participants found it difficult to formulate definitive views on many of the issues discussed, primarily because their knowledge of the current situation is limited. Knowing little of what information sharing is currently possible and permitted, what legal and other protections are in place and what mechanisms of redress exist, participants find it hard to weigh up the benefits of an increase in information sharing.

*"We need more information on what's shared now, what might be shared in the future, how exactly this would work. It's difficult to define 'need to know' when you're not sure about these things."*

This limited knowledge is combined with the assumptions that government access to and sharing of personal data is greater than it actually is and that the government can already find out what it wants about any individual. This makes the benefits to individuals in particular very hard to assess. Many participants vacillate between support for and rejection of any increase in personal data sharing, depending on the argument most recently proposed by a fellow participant. This in itself points to a need for further dialogue on this issue, with presentation of more concrete proposals and management options, well-defined examples of the differences those proposals would make to a range of services and clearly defined security and accountability principles.

*"We've got mixed feelings and we keep going round in circles. Sometimes you think 'oh no, I wouldn't want that' but then someone also makes a point and you think 'yeah, that sounds ok, what would it harm' and then you think 'why should they know that?' We can't make up our minds."*

Additional factors which need to be taken into consideration in looking at responses to the issues in this research are that participants are working with a basic desk-top PC model of technology and few are sufficiently convinced by current security to bank or shop on line.

Across the whole sample, fewer than 10 people banked on line, with only 2 or 3 more shopping on-line. The option of individuals taking control of – and responsibility for – their own information is too remote from their experience for them to think through the issues from that perspective. Information is seen as stored in government computers. Individuals are seen as obliged to take the security of these on trust and information which is rightly their own is seen as accessible only on request. Whilst they argue that their personal information belongs to them and has a value, with the information currently available to them makes it difficult for them to see how things might work differently. An alternative picture of how increased information sharing could work and what the impact of mobile technologies could be, might give rise to other suggestions for how it might be kept secure – or, indeed, other views on its benefits and disadvantages.

These factors contribute to the view that increased information sharing across public agencies is not individually ‘enabling’. The most frequently identified benefits are social, including reduction of the costs of crime and anti-social behaviour (eg, identification of perpetrators, preventing illegitimate benefit claims) as well as and increased road safety (eg, people with health problems having their license removed).

In Stage 1, people found it difficult to discuss data sharing for the purposes of research alone, or to pinpoint any particular difficulties or benefits to themselves that might follow from this. In Stage 2, the position on research stabilised, becoming linked exclusively to health research and, as such, viewed positively. Indeed, information sharing for the purposes of improving individual and public health and healthcare was widely supported. The primary concern here was that insurance companies would get hold of this information and that this could impact negatively on individuals.

Some respondents, in discussing the issue generally, distinguished between the ‘ideal’ system – which they felt would probably bring benefits – and what would happen in the ‘real world’, in which the benefits would be outweighed by the problems, whether these resulted from inefficiency or from illegitimate access to and use of personal information.

### **Three views on the topic**

Overall, participants’ attitudes can be categorised by three broad themes:

1. Uninterested
2. Undecided
3. Objectors

Groups 1 and 2 began as a single group, which was largely uninterested. However, as discussion progressed and people became engaged with the issues, the number of those who were undecided grew.

Two common threads connect the three groups. The first is the feeling of powerless or resignation. Participants feel that ‘this is going to happen whatever we think’ and appear, for the most part, resigned to this. The second is that the questions raised in this research

are, to some extent, making explicit what most believe is already possible, which is the ability of government to 'find out whatever it wants' about any individual, if it is so inclined.

A further point of interest about attitudes across the sample as a whole is that those who have some prior knowledge of or interest in this area (which is predominantly those from the higher socio-economic groups) tend to have negative attitudes. Following group discussions, those who have little or no prior knowledge tend to fall into the 'undecided' group.

The position of the great majority of participants did not shift between Stage 1 and 2.

### **1. Uninterested**

This attitude is most prevalent amongst respondents from socio-economic groups C2DE. Their interest in engaging with the debate is limited and most appear uninterested in the potential benefits or disadvantages of greater sharing of personal datasets by public bodies. Whilst all groups express a sense of impotence with regard to government decisions, this group is most likely to resort to the view that their attitudes are irrelevant and it is therefore somewhat pointless in them discussing the issues it raises.

### **2. Undecided**

Undecided participants are able to identify both benefits and concerns in greater use and sharing of personal datasets across public sector bodies. (Specific benefits and concerns are covered later in this report.) The relative mix of positive and negative views held by participants in this group is varied. Some appear to lean towards the negative whilst others lean towards the positive. However, for the majority of participants in this group, views are neither strong nor strongly held so may be open to persuasion, in either direction. Some might more properly be described as ambivalent, simultaneously holding two conflicting positions. Most had not arrived at the point of articulating such a conflict.

This group recognises that the existing system is costly and inefficient and acknowledges the need for rationalisation. However, this is tempered by concerns over access, accountability and other issues (noted below). This group is also most likely to be swayed by the negative experiences of others. For example, in two different groups, a respondent recounted tales of identity theft and the difficulties they had encountered in correcting the situation. These accounts had a clear impact on the views of others within those groups.

The difficulty – or unwillingness – of these participants to arrive at a decision may be attributed to the somewhat abstract nature of some elements of the proposals – for example, how exactly will the information be managed, accessed, kept secure and how exactly will it improve services for individuals?

### **3. Objectors**

Objectors constituted a small but very vocal and convinced group, together with a smaller number of less committed objectors who were more open to alternative views. These participants are most likely, though not exclusively, to come from the higher socio-

economic groups and to have some prior knowledge of the area. They are least likely to change their views through discussion. Their objections tend to be based on both principle and on scepticism about the capacity of the government / public bodies to manage the technical aspects required to deliver more effectively targeted services.

Objectors placed their arguments within a wider context too, looking to the potential for future abuse. They felt that the threat to personal freedom and the capacity for surveillance would be heightened if more information was shared or if more agencies shared existing information. Whilst this might not be a problem with the current government, they were concerned that it could be in the future.

Other 'objectors' included men from Caribbean backgrounds who felt that they were in general more likely to experience difficulties in their relationship with public bodies and based their objections on this. These men were also amongst the only participants to disagree with one of the sample headlines: 'nothing to hide, nothing to fear', again, on the grounds that black men were disproportionately subject to suspicion. Whilst these views were not strongly expressed, this should not be taken as an indication that they were not strongly held. BME participants in mixed groups may express this kind of point less strongly in a mixed group than they would if they were in a group comprising only those who they feel are likely to share the same experiences. Similarly, there is often a degree of resignation behind this kind of comment, which may appear to detract from its importance. More research would be needed to explore this issue.

### Factors contributing to views

Participants' views on whether or not it is appropriate to provide information to public agencies, or for these agencies to share information provided are informed by a variety of factors:

- Which agency is asking for the information
  - Information is shared most readily with health professionals; a relationship of trust exists here that seems absent from relationships with other government agencies
  - Most are willing to provide information to police, though people from BME groups are more reticent to do this (see below)
  - Agencies seen as 'faceless' are treated with most suspicion; this seems to mean agencies with whose employees the public has little interaction – for example, the Inland Revenue

*"If some people ask, like the police or the doctor, then you'd provide it, but if they're invisible and you don't know who they're sharing it with, you feel like it's a loss of control."*

- What benefits appear to follow from providing the information
  - The benefits of providing information to health professionals appear to be clear and the disadvantages negligible or non-existent

- Improved health is seen as both a public and a personal good. With the exception of one participant, all respondents acknowledged benefits to wider society and to themselves or their children and grandchildren in health research and in the NHS sharing health records across current boundaries (as in Connecting for Health).

*“If it’s going to make an improvement to people’s health, then you don’t mind.”*

- The circumstances under which the information is requested
  - If the interests to the individual asked to provide information are clear, or if there was an expectation that information would be asked for, it is given more readily
- Previous experiences of providing information and of how this has been handled
  - Those with experience of identity fraud, of errors or inefficiency in the management of personal information, of difficulties in correcting mistaken information, etc appear more likely to question the need to provide more and to raise doubts about increased sharing
  - Groups most likely to raise these issues include benefit claimants, in particular those with experience of the CSA and of working family tax credits
  - Anecdotally, people from BME groups tend also to be more circumspect about providing information, because of previous experiences of racism
- Wider attitudes towards the government
  - Mistrust of the government emerged more strongly as a factor in the second stage of the work and contributes to attitudes taken in discussion. The extent to which this mistrust impacts on actual behaviour is unclear, however
  - A small group hold principled objections to providing more information to the government and to any increase in information sharing, on the basis that it will alter the relationship between the government and the individual.

## 2. Stage 1

### Introduction

Initial discussions focused on the use of personal data by both public and private sector organisations. The following provides a broad overview of the issues raised:

Public sector / government	Private sector
Do not sell data	Sell data
Technically inefficient	(In general) more technically efficient
Limited or no redress seen as possible in case of misuse of data – channels known to exist but extremely difficult to use, with a lot of problems encountered	Possible redress if data misused – eg, withdraw business, write to consumer programmes/pages, circulate bad experiences through word of mouth
Absence of choice about whether or not to provide information	Choice about whether or not to provide information, based on perceived advantages/disadvantages in doing so
Social benefits easy to identify – eg, fraud prevention. Individual disadvantages easy to identify – eg, access to personal information by unauthorised individuals; identity fraud.	Benefits and disadvantages to the individual can be identified –eg, value of purchase/service to individual weighed against cost/risk of providing information

### Trust

In Stage 1, the ‘crisis in trust’ said to characterise the current relationship between citizens and the state did not emerge strongly as a general theme in relation to the use of personal datasets by public bodies. The exception to this was amongst people in the ‘objectors’ group.

When trust did emerge as an issue it tended to be with specific reference to the capacity of the government to manage the technical aspects involved. Reference was made to previous or current government projects which were seen as supporting this mistrust, including the Passport Agency, Child Support Agency and Working Family Tax Credits. Whilst not all of these involve difficulties with IT, they were cited as examples of large scale government projects which evidence inadequacies in public sector management of relevance to the issues under discussion.

Questionnaires completed before the groups indicate that, when asked about government trust in general, participants tend to be suspicious. Thirty-five respondents agreed with the statement “*I don’t trust government agencies enough to want them to share any more of my personal information*”, 20 were neutral and 8 disagreed. However, when greater

information sharing is couched in terms of more personalized services, the trust issue is less apparent, with neutral respondents moving to a position of support. Forty-two respondents agreed with the statement *“I would support greater use of my personal information by government agencies if it led to services that met my needs better”*, 12 were neutral and 9 disagreed.

## Access

Respondents were concerned about how access to their personal information would be controlled. Many suggested that, whilst there might be efficiency and cost benefits in the development of a single database, this would be at the expense of security. The current situation, in which personal information is distributed across several databases, is felt to offer greater protection because access to information held on one of these does not necessarily provide access to information held on the others. A single database was seen as ‘concentrating power’ and opening the potential for future abuse.

There was some debate about the possibility of setting up ‘filters’ which would limit the access different agencies or individuals had to that information; for example, someone in customer service at the tax office might have restricted access, whilst the police would have greater access. Many commented that the government could already find out whatever it wanted about people anyway. It may be that this view contributes to the focus on the service delivery aspects, rather than on any infringement of personal privacy.

In addition, people felt they should have access to their own information, to be able to check details were correct and to be able to monitor by whom and how it is being used.

## Efficiency

All groups acknowledged that a more streamlined interface between the individual and public agencies, with fewer requests for repeat information and a reduced capacity for conflicting information, would have benefits.

At present, both the process of providing information and the accuracy of the information held are questioned. Many participants have tales of difficulties experienced in dealing with public agencies, from Customs and Excise to the NHS to the Inland Revenue. These included attempts on the part of individuals to return over-payments, problems updating or correcting records and other incidents which lead them to question the efficiency of public bodies, with regard to information gathering, holding and sharing. These experiences informed their views on the capacity of the government and public bodies in general to deliver efficiency benefits implied by a new system.

*“I work in an MOT station and they’ve been going on about computerisation now for about 6 years – it was supposed to start up in about 2000 and we didn’t start until April this year, we’ve had that many problems. All the information is supposed to be on a computer and shared with the DVLA. But even their records are wrong. You look for the information and you get about 2000 cars and you have to try to narrow it down. Sometimes you put the registration number in and it says it’s a Ford Escort*

*but you're looking at a Honda Civic on the ramp. But that's just a car; it's not your health."*

## **Accountability**

Both 'undecided' and 'objector' groups wanted information on who would be accountable for the accuracy and security of personal information. Whilst respondents feel it is currently difficult to correct errors and that public agencies resist apologising for mistakes, they are confident about whom they should contact (the agency which they see as responsible for the error). They are concerned that if a single database were to be built, this process would become even more difficult. This concern seems based largely on what is perceived as a 'big brother' aspect to data sharing. Theoretically, it might be assumed that it would in fact be easier to correct details if they were held on a single database, since there is no possibility of these conflicting with information held elsewhere. However, the prospect of a large 'faceless' single database not attached to a recognised government function (eg, health, taxation, policing, social security etc) seems to increase feelings of powerlessness.

*"You know where to go if you want to correct the information. You know who to phone, and you can speak to someone at the end of the phone if you want to correct the information. It's the psychology of being faced with a big entity... that loss of control."*

*"I don't think you'd ever get accountability because it's always pass the buck."*

Concern is also raised over who would be accountable for ensuring that access was limited to the appropriate bodies. Several respondents talked about denial of coverage if insurance companies got hold of data held on an individual's health or on the history of their family's health.

One group suggested that a named individual would need to be responsible for these issues and that the route through which complaints could be made should be clear and easily accessible to all.

## 3. Stage 2

### Introduction

All but one participant returned for Stage 2. Whilst the raised incentive for the second part will clearly have played some role in this, it should be noted that those in Belfast came out on the night following riots. The city was gridlocked and many had some difficulty in getting to the venue. That they took the trouble to come on such a night suggests that they had a strong interest in the subject.

At the close of Stage 1, participants were provided with some suggestions of activities they might undertake before returning for Stage 2. These included discussing with their friends and family the issues raised, looking out for relevant media coverage and asking relevant agencies if they could see any information held about them.

About one-third of participants undertook some activity. Most either talked with friends and family or asked their GP or other health professional if they could have access to their medical records. All health professionals approached were very willing to provide access and none was reported asking participants the reason for their request.

*“I talked to three of my closest friends and their concept of the thing was really very much the same as mine. They didn’t mind sharing, providing they were told about usage and there was a guarantee that it would only be used for the purposes it was given.”*

*“I asked the hospital if I could see my son’s notes but I worried they were going to write ‘paranoid mum’ on them afterwards.”*

This latter comment illustrates a concern raised by other participants regarding the consequences of asking to see information held about them or their dependents. Some of the safeguards and principles which should govern information sharing may help to address this: this issue is covered later in this report.

*“Last time I was quite negative about it but it seems that the more you thinking about it the more positives you can see.”*

*“I’ve got more negative. I’d only want sharing with health.”*

### Any change in attitude?

Overall, views remained consistent across stages 1 and 2, with a majority of participants falling into the second, ‘undecided’ category. As remarked earlier, indecision was characterised by rapid shifts between identifying benefits and then disadvantages and back again. Responses to the questionnaires completed at the beginning of Stage 1 and the end of Stage 2 provide some indication of a change in view, however. Following Stage 2,

more people said they felt informed about the information held about them by public agencies; more people said they were concerned about government agencies sharing their personal information; more people disagreed with the statement “If you’ve got nothing to hide then you have nothing to fear from government agencies sharing your personal information”: and finally, more people agreed with the statement “I don’t trust government agencies enough to want them to share any more of my personal information”.

It is difficult to gauge the extent to which these changes are a consequence of increased uncertainty introduced by becoming aware of the complexities of the issues involved. Based on the discussions within the groups, however, we would suggest that this plays a major part in the shifts of opinion. For whilst people may feel more informed, as no doubt they were, information gave rise to more nuanced debate and tended to unseat previously confident views. This again points to the need for future public debate to present a more fully developed and concrete picture of the options and suggestions in play.

## Trust

The issue of trust arose more strongly in Stage 2. Whilst in Stage 1 it was limited largely to scepticism about the technical efficiency of systems, in Stage 2 people expressed mistrust of the government as such and in ‘anonymous’ civil servants who might be using the database.

*“I wouldn’t trust the Ministers, I mean the actual government people who are dealing with your information because they’ve lied to us about everything. How could we possibly believe them?”*

*“It doesn’t matter if it’s on paper or on a computer – the issue is being able to trust the person that’s got access to it.”*

*“You trust your doctor and you go to see them if you’ve got a problem. How many people go to see their MP if they’ve got a problem? How many people even know who their MP is?”*

Participants’ specific concerns were that the government would use the greater store of information to ‘juggle figures’ and ‘tell you things that were wrong’. These concerns were raised by the ‘undecided’ group and the shift is reflected in responses to the questionnaires completed at the end of Stage 2.

## Guiding principles and safeguards

There was considerable consistency across the seven groups over the principles that should guide public agencies involved in sharing personal information. These principles were to apply to all information held on an individual, including that held for health research purposes.

### **Protection of individual privacy is paramount**

Ensuring that individual privacy is protected is seen as most basic requirement, taking precedence over wider social benefits. A range of safeguards were seen as helping to achieve this:

- don't rush the introduction of any new information-sharing systems – make sure it works first
- a federated system, rather than a single database, was preferred, each one being 'themed' – eg, a health database, a crime database etc
- more research into security should be done, by commercial and public bodies
- provide training in security, legal context and protocols to all those using the system(s)
- access to personal information by individual government employees should be limited to what is essential to their specific responsibilities
- individuals cannot be expected to keep up to date with the latest anti-viral protection, firewalls etc: the government should be responsibility for security
- sharing of information with commercial organisations should be prohibited, for both now and the future
- an independent 'privacy protector' should be able to check use of the system and the information being shared, and by whom, unannounced and in response to any complaints
- misuse of personal information should be punishable by imprisonment

### **The reasons for sharing information and the agencies having access to information should be clearly defined, agreed between the government and the individual and set down by law in advance of systems becoming operative**

- any changes to this should be subject either to open debate and further legislation
- agencies sharing information outside the agreed / legislated framework should be subject to investigation
- individuals should receive compensation for information sharing outside the agreed / legislated framework
- users of the database needing to sign something equivalent to the Official Secrets Act was suggested, alerting them to the severity of misuse of the information to which they had access

*"If they did a book that told you under what situations your information would go to another person and you signed it and they signed it to say you agreed with it, then I don't see the problem. It would be like a contract."*

*"We should be asked if people want to look at the information, apart from people we've already agreed could."*

**Individuals must have easy access to their own information and details of how and with whom it has been shared**

- the government should provide the appropriate technology to those without it, not through libraries or other public places, but in their own homes.
- Information should also be accessible by telephone, mail or in person
- the interface to government databases should be user friendly and accessible to people with disabilities: if this is not the case, support must be provided to facilitate access
- Individuals should be able to check easily who has accessed what information held on them, the purposes for accessing this information and any agencies with whom it has been shared

*“The reason I’d want access to my information is so that I could make sure it was correct. Then I’d be happy.”*

*“There’s still a whole world out there that’s not part of the information age.”*

**The government should take responsibility for the accuracy of information held**

- Individuals would be responsible for the accuracy of information provided

**Information should be kept for a limited period only and then individuals should be asked to provide all information anew**

- This is seen as a way of checking on both fraud and inaccuracy

**An independent auditor should oversee the system**

- The auditor’s responsibility should be to individuals on whom information is held, rather than to the government

*“I wouldn’t trust the government to audit this information.”*

**The Data Protection Act should be updated and strengthened**

- No specific suggestions were made, since knowledge of existing legislation is very limited

**If more efficient services are promised by the government as a result of the introduction of this system, the resources to ensure that this happens need to be in place**

- Employing and training individuals to act on new knowledge arising from information sharing is seen as essential
- It will help to allay suspicion over this exercise being to ‘make life easier’ and save money for the government, rather than for individuals

*“The big question is who’s going to pay for it? It’s all going to come back to us, isn’t it?”*

## **The case studies**

The case studies brought many of the issues to life, by providing examples of how the sharing of personal information might impact on individual’s day-to-day life. It should be noted too that, of all the information provided in the ‘talking head’ video clips shown in the second stage, one was seized on with most recognition, because it was a situation with which many were either personally familiar or at least aware of. This was the example of how the issues with which people have to deal following a death in the family might be simplified by data sharing. This was received very positively, though it should be noted that the person benefiting from the increased simplicity was not the person to whom the information attached, but the deceased. However, it does illustrate the value that recognisable and familiar situations can have in discussions about this issue. (Case studies are included in the Appendix.)

There were four case studies, based around the following themes

- information sharing for health research
- a traffic management scheme
- security of health information kept electronically
- automatic identification of individuals qualifying for receipt of benefits

### **Information sharing for health research**

Attitudes towards information sharing for health purposes occupy a different space to information sharing for other purposes. In part, this is because the NHS is seen as at one remove from the government and as trustworthy in a way that other government agencies are not. The benefits to individuals are also clearer. Finally, the context is also different, since information would be pseudonymised.

In two groups, conversation around this case study focused on the possible wider consequences of the discovery of environmental pollution in specific areas being damaging to health. Participants raised the issue of property prices falling, of residents being unable to move away from an area and other related problems. Following some short-lived uncertainty about whether such information should be made public, participants agreed that the government should take responsibility for this eventuality and provide the necessary support, both financial and medical, for people harmed as a consequence of such discoveries.

### **Traffic management scheme**

Attitudes towards information sharing for the purposes of traffic management were generally positive. Benefits to individuals were identified spontaneously and included being able to avoid traffic jams, less chance of being involved in an accident and easier tracing of

stolen vehicles. Under prompting about the wider benefits, people mentioned reduced pollution. However, this was not seen as a major advantage. There was little concern expressed about 'the government knowing where you go' – indeed, this issue was treated very lightly with more people worrying about their wife knowing.

The primary concern was whether such a system would be fair to people living in rural areas or people who used their cars for business purposes. Some balance between the amount of traffic on the road and distances travelled was seen as necessary to ensure that the former did not end up paying too much. It was seen as the responsibility of employers to cover the costs of travel for work purposes.

*"We thought the main social benefit would be if someone stole your car, they could find it."*

*"There'd be less accidents and less congestion."*

*"Another advantage would be that everyone would be taxed and insured."*

### **Security of health information kept electronically**

This case study gave rise to a lot of discussion, primarily based around people's awareness of scams along these lines currently taking place – for example, emails purportedly from E-Bay and banks, asking individuals to update information and directing them to fake websites. Many felt that whatever steps were taken to enhance security, this type of scam would always have a degree of success because a lot of people lack knowledge of how to spot them.

*"The hackers are getting cleverer and cleverer everyday. They can get into anything – they wouldn't have any difficulty getting into a government file."*

The question of how information should be updated arose primarily from discussion of this case study. There was support for the overall project of connecting health information across Trusts, so that wherever you were in the country, your records would be available, should you have an accident or medical emergency. However, many participants said they would be uncomfortable about providing information on-line.

More generally, whilst individuals felt they alone were in a position to provide details of a change in circumstance, they were also concerned about this leading some people to provide inaccurate information, for fraudulent purposes. Many people resolved this by arguing for paper-based communication of changes in circumstance, on two grounds. First, this would address their worries over the security of on-line updates and second, that it would provide a record of the information provided by individuals, which could be used to demonstrate fraud, if necessary. Those individuals who were less anxious about on-line security – some of whom felt it was largely down to lack of knowledge – were still concerned about the possibility of fraudulent entries if people were allowed to update their own information.

The resort to paper is perhaps a consequence of participants' limited knowledge of available technologies that could serve the same purpose, but electronically.

*“Individuals shouldn’t have responsibility for updating their own information – there would be too much fraud.”*

*“Each person’s individual information is changing constantly. It could change within a week and then change in another way within a week. How would you actually get this information to the necessary place so it was updated? The only way I could see is if individuals had a password so that they could go into their own records and change it. But that’s not going to work from another point of view. People could just go in and put something in that suits them and may not be truthful. So there’s a very grey area there about how this information is going to be kept updated.”*

Password security was also raised as an issue, prompted by the suggestion from some participants that they might use their children’s names or birthdates as passwords. Others argued that this was very insecure, as it was information that might be discovered quite easily and attached directly to particular people. Participants thought that the government would be responsible for ensuring that this type of security issue was widely understood before sensitive personal information was kept and accessed electronically.

*“This should be paper-based so that people can feel secure about putting everything down that they need to.”*

#### **Automatic identification of individuals qualifying for receipt of benefits**

Responses to this case study were somewhat at odds with the wider discussion about needing to complete long forms and provide the same information to different authorities. Some participants voiced the suspicion that this one was a ‘set-up’, written to look positive so that people would be persuaded of the benefits of information sharing. Others said it demeaned older people, suggesting they were not capable of completing forms.

The major concern was about the amount of information that would be held on an individual for this system to work automatically. When it was explained that, currently, this information would need to be provided anyway, participants argued that at present the individual would have a choice whether or not to pursue a claim. In the case study, this choice was felt to have been removed.

## 4. Recommendations for future public dialogue

A majority of participants said they would be happy to be involved in for further consultation on this topic. Responses to the project overall were positive, with participants saying they felt it had been open and honest. The only suggestion of bias was in relation to one of the case studies, as noted above.

Recommendations for future consultation focused on both breadth and depth of involvement. To deepen the conversation, people felt that some of those taking part in this work should be invited to contribute to any further work, since they would have considered some of the basic issues involved already and could get to grips with more detailed information quite rapidly.

They felt too that a wider dialogue needed to take place. Whilst a survey-approach was seen as reached a large audience, the complexities of the issues involved were felt to require a deliberative approach, with conversations, debates and relevant information provided. Most important was providing an opportunity to talk with 'neutral' IT experts and government representatives and "grill the people who decide things." This reflects the concern amongst the 'undecided' group in particular that they were not sufficiently informed about the options, technologies and safeguards, or the current situation, to arrive at firm views.

A crucial factor in any future consultation would be providing participants with more fully realised models of the possibilities for establishing, managing and using the database(s). Many participants in this project had questions about the details of how such sharing would work and it will be important for these questions to be answered, to enable people to make a more fully considered judgement on the issue.

The questionnaires in the Appendix provide a more detailed view of where people's preferences lie for future public dialogue.

*"I think they should follow it through – ask us what we think, because they might come up with this magic plan but have misinterpreted what we've said."*

*"Perhaps two or three people out of each of the groups could be invited to get involved in what they think is the solution."*

*"They should involve more people up front before they make any decisions."*

## Appendix 1. Methodology and sample

### Methodology

The overall objective of the project was to understand public attitudes towards the use and sharing of personal datasets held by public bodies. The specific aims were to:

- Identify what key questions people raise in relation to the use of their personal data by government and researchers
- Explore what benefits/aspirations and concerns people perceive that greater use of their personal data by government and researchers could bring.
- Explore the way that individuals make decisions between the benefits of greater use of their personal data and the potential losses of personal privacy
- Identify common principles that might help guide development of future government policies on data linkages and access
- Explore how best to engage in discussion with the public on the issues raised, in particular the level of public interest in further engagement, their views on how this might take place and their expectations in terms of the legitimacy of the process.

There were two stages to the research:

- Stage 1 – 1 ½ hour focus groups, focusing on the first two aims
- Stage 2 – 2 ½ hour workshops, reconvening participants from stage 1, focusing on the remaining three final aims

Participants were provided with stimulus materials, including information on databases that currently share data and case studies through which they could explore some of the issues involved. All research materials are included in the Appendix.

Brief 'talking head' videos were also presented, in both stages, to provide participants with a range of 'expert' views. Each contribution lasted 4 – 6 minutes. Contributors were:

- Casper Bowden, Chief Privacy Adviser for Microsoft in Europe
- Professor Wendy Hall, Professor of Computer Science, University of Southampton
- Gus Hosein, Visiting Fellow London School of Economics
- Tom McArthur, Director, Operational Services, Police Information Technology Organisation
- Gareth Crossman, Policy Director, Liberty
- Mark Walport, Director, Wellcome Trust

We would like to thank the above for contributing their time to this work.

## Sample

Participants were professionally recruited to the following specification:

<b>Location</b>	<b>Age</b>	<b>Gender</b>	<b>SEG</b>
England (Bradford)	18 – 25	50:50 M/F	C2DE
England (Birmingham)	26 – 45	50:50 M/F	ABC1
England (Birmingham)	31 - 45	50:50 M/F	C2DE*
England (London)	45 – 60	50:50 M/F	C1C2
Scotland (Glasgow)	18 – 25	50:50 M/F	C2DE
Wales (Cardiff)	26 – 45	50:50 M/F	ABC1
Northern Ireland (Belfast)	46 – 60	50:50 M/F	C1C2

Each group, with the exception of that in Belfast, included at least two people from BME groups. Sixty-seven people took part in Stage 1. Sixty-six people took part in Stage 2. Participants received a cash ‘thank-you’ for contributing their time to the project.

## Appendix 2. Discussion guides

### Stage 1

#### AIMS OF STAGE 1 GROUPS:

- To identify what key questions people raise in relation to the use of their personal data by government and researchers
- Explore what benefits/aspirations and concerns people perceive that greater use of their personal data by government and researchers could bring.

#### INITIAL LOOK AT:

- The way that individuals make decisions between the benefits of greater use of their personal data and the potential losses of personal privacy

AS PEOPLE ARRIVE, GIVE THEM THE QUESTIONNAIRE: IF POSSIBLE, THIS SHOULD BE COMPLETED BEFORE DISCUSSION.

#### Introduction – 5 minutes

Welcome, thank you for coming.

Brief explanation of project: remind about second session / date

Basics:

- Toilets / refreshments etc
- Confidentiality – gain permission to tape
- Mobiles off
- Want to hear from everyone – really is a case where there's no right and wrong answers – everyone's views are equally important etc
- Any questions?

#### Warm-up – 5 minutes

In pairs: get to know neighbour. Age, occupation, family status. Each person to introduce their neighbour.

#### What is personal information? (10 minutes)

Brainstorm: what sort of information do you think of when I say 'personal information' – (flipchart)

Of these different types of personal information, which have you ever given to a government agency (eg, DH, DVLA, police, Inland Revenue, a Job Centre, Benefits Agency, your doctor or hospital, etc)?

What do you think happens to information you give to the government (eg, on forms, over counters, on-line etc?)

### **General attitudes towards use of personal data by government – 15 minutes**

Brainstorm, prompted by 'headlines' (see attached).

If people talk about 'privacy', 'snooping', etc, get them to define what they mean by these terms. Explore any differences in attitude between personal data used in the context of government research/service delivery and use of personal data by businesses.

### **Benefits of government use of personal data**

What benefits might there be to individuals if government agencies shared personal information about them? Brief general discussion followed by card sort exercise, allowing people to prioritise benefits.

Are there any groups of people who would most benefit? Why / how?  
Who wouldn't benefit? Why / how?

Are there other sorts of benefit? Prompt on use of data for government research – use examples (eg, health research)

### **Concerns individuals might raise to government making greater use of personal data**

What concerns do you think individuals might have about the government using personal information about them?

Do you think these concerns affect any particular groups of people or individuals? Why?  
What could be done to reduce your concerns? (PROBE: is it just more information? Clear complaints system? Giving active permission for data-sharing?)

Thinking about the use of personal data for research purposes: do you think we should have any concerns about this use of personal data?

### **Wrap – up**

Brief review of discussion: categorise benefits / concerns to individual and wider public (research)

**Principles** (eg government 'in principle' shouldn't have / has right to access to all this information about individuals)

**Technology** (technology is moving that way / technology not good enough / too complicated / have-havenots etc)

**Law:** (eg, not enough / sufficient legal protection)

**Talking heads**

Show video: explain that transcripts will be available for people to take away with them and consider.

Get brief responses to video – NOTE POINTS THAT ARE HIGHLIGHTED AT THAT STAGE

Distribute briefing materials. Go through briefing notes to ensure everyone understands them.

Any questions?

Thank and close

## Stage 2

### AIMS OF STAGE 2 WORKSHOPS:

- Continue to explore the way that individuals make decisions between the benefits of greater use of their personal data and the potential losses of personal privacy
- Identify common principles that might help guide development of future government policies on data linkages and access
- Explore how best to engage in discussion with the public on the issues raised, in particular the level of public interest in further engagement, their views on how this might take place and their expectations in terms of the legitimacy of the process.

AS PEOPLE COME IN, ASK THEM TO SIT NEXT TO SOMEONE DIFFERENT FROM LAST TIME

### Introduction – 5 minutes

Welcome, thank you for coming.

Brief review of project / discussions

Review basics:

- Toilets / refreshments etc
- Confidentiality – gain permission to tape
- Mobiles off
- Questions?

### Warm-up – 5 minutes

In pairs: the things that stuck in your mind from the last discussion. Whether you were able to do any of the activities suggested in the packs (eg, talking to friends etc, finding materials from newspapers etc). Outcome of these. What you think the major issues are etc.

Everyone introduces neighbour – discussion of interim activities / changes in attitude & what caused these.

### Video clips – 10minutes

Clips: Gareth Crossman, Liberty

Mark Walport, Wellcome Trust

### Probes:

- Respect for privacy: Which types of people are likely to experience less respect for their privacy? How could these people's privacy be ensured?

- Auditing information – What responsibility do you think individuals should have for ensuring information held about them is correct? Are there some people who might find this difficult?
  - What do you think could be done to support these individuals? Should there also be an agency that audits information held and shared? Who would you trust to audit information? Should it be a new agency?
- Is it ok for government to hold information that *might* be of use in the future – eg, for future policy planning, planning use of public resources, etc?

### **Case studies – 20minutes**

Split group into two. Each group to have one / two case studies to discuss. After discussion, feedback to the other group, followed by questions, clarification.

### **Developing common principles – 20 minutes**

**Group 1: Public Service Users Group-ICT sub-committee:** Develop some common principles that should be kept in mind when information is shared between public agencies. (See attached sheet).

**Group 2: Public Service Users Group-ICT sub-committee:** Develop some advice for the government on the safeguards that should be in place to:

- Protect individual privacy
- Ensure individuals have access to the information that is held about them

### **BREAK – 10 minutes**

### **Feedback and discussion – 20 minutes**

Feedback from both groups. Questions, clarification and discussion. Develop a final set of principles / safeguards that whole group is happy to sign up to (explore any disagreement/problems).

### **Public engagement – whole group discussion – 15 minutes**

If you read in the paper that the government was going to introduce a new policy on information sharing and had done some public consultation – and referred to the work that you have taken part in – what would you think? (PROBE: legitimacy of consultation; issues about how you take findings from public engagement into account; number of people involved etc).

Would you be interested in taking part in further discussions on this issue? What more information would you need to help you think about these issues in more detail? How do

you think these discussions should take place? Who do you think should be involved?  
**Probe** on anything they've told friends/family about etc. – if they showed interest etc).

### **Final Review and wrap – up – 5 minutes**

Review common principles & safeguards  
Review priorities for further engagement.

Any questions?

### **Questionnaires – 5-10 minutes**

Ask people, before they leave, to complete questionnaire.

Thank and close

## Appendix 3 – Research materials

### Questionnaire (Stage 1)

(Stage 2 findings for some questions are provided in parentheses. Numbers may not add uniformly since some respondents did not provide answers to all questions.)

**1. What sort of information do you consider to be ‘personal information’? List as many examples as you can think of.**

Address, Age, Bank Details, Salary, Children Details, Telephone, D.O.B, Health, Tax, Police
Services, National Insurance, Customs, E-mail, Occupation, Mortgage, Credit Cards,
Benefits, Debt, Ethnic Background, Education, Criminal record

**2. How well informed do you feel about what information different public services hold on you?**

Very informed	2	( - )
Quite well informed	11	(18)
Neither informed not uninformed	24	(22)
Not very well informed	14	(21)
Not at all informed	6	( 4 )

**3. Can you give an example of personal information you have recently given to public services?**

National Insurance number, postcode, relationships, name, address, inland revenue information, customs, DHSS, salary, police, youth club, Benefit Office, DOB, police, doctor, children’s school, religion, sex, mobile number, tourist information office, DVLA
--

**4. Where would you go to find out what information public services hold about you?**

Don’t Know, electoral roll, approach department or agency direct, Public Records Office, internet, library, town hall, council, Lloyd House (sic), Citizens’ Advice Bureau, Land Registry, neighbourhood office (sic), government website
---

**5. How concerned are you about different government agencies sharing your personal information?**

Very concerned	13	(20)
Quite concerned	20	(33)
Neither concerned not unconcerned	14	( 8 )
Not very concerned	4	( 4 )
Not at all concerned	3	( - )

**6. How much do you agree or disagree with the following statements?**

	Agree strongly	Agree slightly	Neither agree nor disagree	Disagree slightly	Disagree strongly
If you've got nothing to hide then you have nothing to fear from government agencies sharing your personal information	<b>11</b> (5)	<b>17</b> (16)	<b>9</b> (8)	<b>16</b> (22)	<b>5</b> (14)
I would support greater use of my personal information by government agencies if it led to services that met my needs better	<b>7</b> (14)	<b>30</b> (33)	<b>11</b> (10)	<b>6</b> (6)	<b>2</b> (2)
I don't think computer systems are secure enough yet for government agencies to share my personal information	<b>25</b> (33)	<b>18</b> (16)	<b>8</b> (7)	<b>5</b> (9)	<b>1</b> (1)
I would support greater use of my personal information by the government, for research if this led to better policies	<b>8</b> (11)	<b>23</b> (25)	<b>14</b> (15)	<b>7</b> (11)	<b>5</b> (3)
I don't trust government agencies enough to want them to share any more of my personal information	<b>12</b> (22)	<b>17</b> (20)	<b>21</b> (17)	<b>6</b> (5)	<b>1</b> (1)

**7. How often do you use a computer?**

Every day	<b>37</b>	About once every 2 to 6 months	<b>2</b>
About once a week	<b>11</b>	Less than every six months	<b>2</b>
About once a month	<b>4</b>	Never	<b>1</b>

## Questionnaire (Stage 2)

### 1. *How well informed do you feel about what information different public services hold on you?*

Very informed	-
Quite well informed	18
Neither informed not uninformed	22
Not very well informed	21
Not at all informed	4

### 2. *How concerned are you about different government agencies sharing your personal information?*

Very concerned	20
Quite concerned	33
Neither concerned not unconcerned	8
Not very concerned	4
Not at all concerned	-

### 3. *What three things could the government do to make you feel confident that the personal information about you that it holds and shares is secure?*

i)reassurance information is safe, secure password, more training for staff, tell me what information is held on me, who has access to my information, regular feedbacks, show trustworthiness, create external agency,
---

ii) someone who is capable of setting up large system, make no money from it, have proper protocols, no sharing information, coding, relevant information only for relevant users, sworn to confidentiality, give us more information, annual reports of 'who has my information'; how can I check my information
---

**4. How much do you agree or disagree with the following statements?**

	Agree strongly	Agree slightly	Neither agree nor disagree	Disagree slightly	Disagree strongly
If you've got nothing to hide then you have nothing to fear from government agencies sharing your personal information	5	16	8	22	14
I would support greater use of my personal information by government agencies if it led to services that met my needs better	14	33	10	6	2
I don't think computer systems are secure enough yet for government agencies to share my personal information	33	16	7	9	1
I would support greater use of my personal information by the government, for research if this led to better policies	11	25	15	11	3
I don't trust government agencies enough to want them to share any more of my personal information	22	20	17	5	1

**5. Here are 7 statements. Please put these in order of importance to you. Put a number (1) against the most important, a number (2) against the next most important, etc.**

	1	2	3	4	5	6	7
Having a single, named person who is responsible for the security of the database that holds my personal information	3	5	7	4	16	10	14
Access to all information about me held by public agencies	18	7	5	9	5	6	9
Some form of compensation to be paid to me if information about me is misused or stolen	1	9	6	4	12	14	13
The right to opt-out of having my information shared across different public agencies without this affecting my right to public services	13	8	11	6	7	8	4
A simple and effective complaints system that I can use in person, on the phone, by letter or over the internet	5	4	8	12	5	10	12
An annual check on the security and use of my personal information, done by an independent organization	10	15	14	9	5	4	0
Access to details of which agencies have looked at or used my personal information, and why	9	10	8	15	7	4	5

**6. What would be the three benefits TO YOU PERSONALLY of more information sharing between public agencies?**

i) hospital records available, better healthcare, lower taxes, not having to fill in so many forms, better education, easier for medical records, accurate info, less time wasted, time,  
 ii) convenience, faster service, NONE, only one agency, avoid duplication, not having to speak to more than one person about something, easier to claim benefits, anonymity of individuals

**7. What do you think would be the three benefits TO SOCIETY AS A WHOLE of more information sharing between public agencies?**

i) stopping benefit fraud, illegal immigrants, health share info, finances, better national security, more efficient services, marketing companies, hackers, better crime prevention, better travel, trust, few staff, cost, identify criminals by DNA sampling, quicker,

**8. What would be the three disadvantages TO YOU PERSONALLY of more information sharing between public agencies?**

i) personal security at risk, losing my private life, my info being sold, junk mail, mistakes being made, info being used in negative fashion, insurance, 'watching my every move', paying more, false judgment, failing credit checks, distributed without knowledge

**9. What do you think would be the three disadvantages TO SOCIETY AS A WHOLE of more information sharing between public agencies?**

i) being taken advantage of, open to abuse, invasion of privacy, info mix up, profiteering, mistakes, increase costs, misuse, access, risk of ID fraud and crime rate increase, system crashes, view government more as 'big brother', reduced civil liberties, people more vulnerable, could cause conflicts

**10. The government would like to learn more about what the public thinks about these issues. Below, there are 7 things that might be included in these discussions. Please put these in order of importance to you. Put a number (1) against the most important, a number (2) against the next most important, etc.**

	1	2	3	4	5	6	7
Lots of opportunity for small group discussions	9	8	10	11	4	8	7
Having 'neutral' experts in IT there, to answer my questions	12	16	10	8	6	1	3
Written information that I can take away with me to read and think about	9	10	11	7	6	6	7
Case studies and examples of what the plans would mean for people like me	3	12	10	17	7	2	5
Having government representatives there to answer my questions	16	8	5	0	15	11	4
An opportunity for small group discussions with IT experts / government representatives	7	7	7	5	13	12	5
Video presentations from experts, so I get a range of different views	2	1	5	3	8	13	26

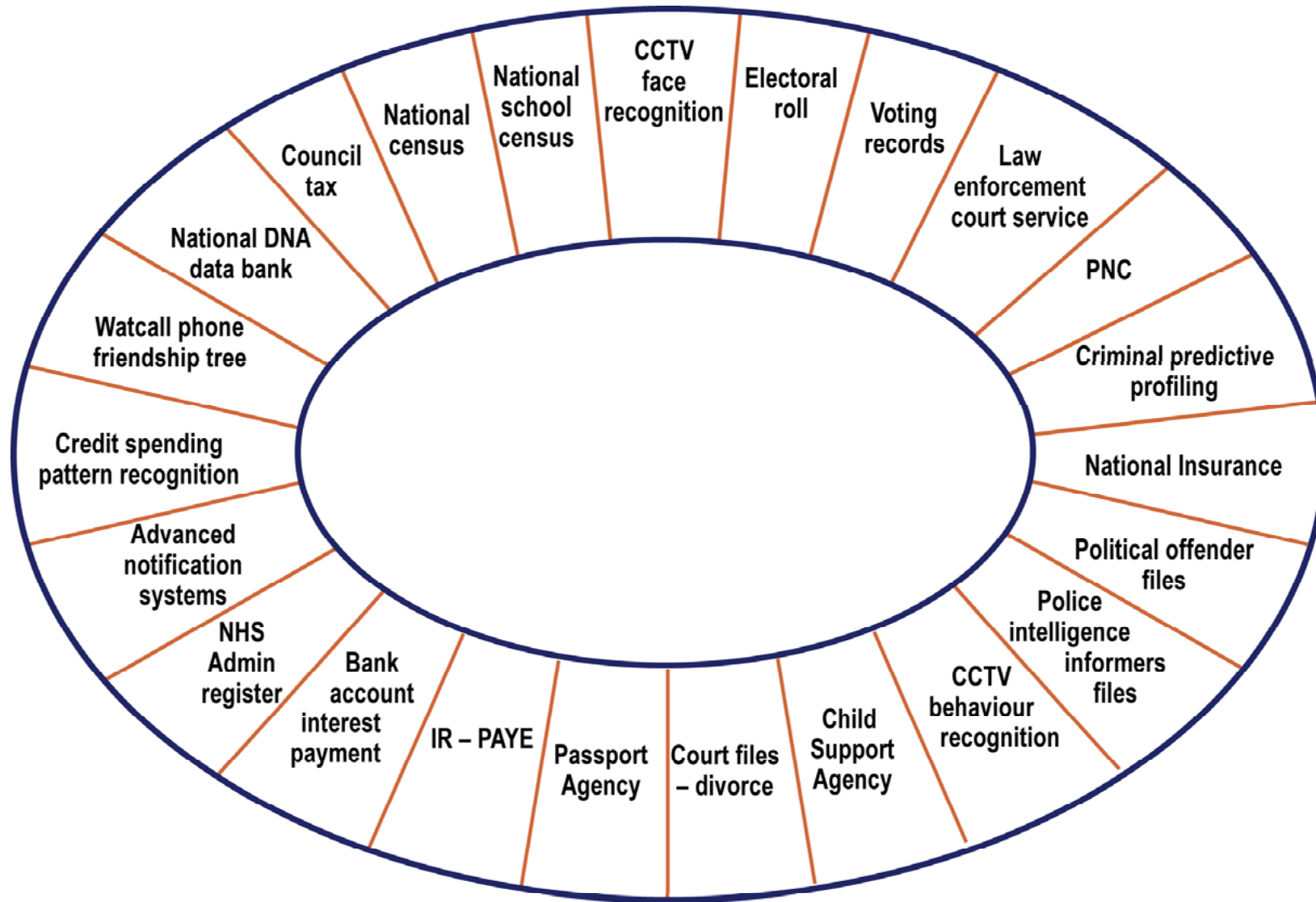
**11. Public discussion about these issues can be done in a number of different ways.**

**From the following list, please put a tick in the box next to the two ways that would suit you best.**

A process lasting 2 -3 days so I would get an opportunity to hear lots of different views, learn about and discuss the issues in depth.	22
More short discussion groups or workshops like the ones I have been involved in	33
Surveys with 'tick box' answers.	23
A public meeting in my area, which anyone can go to	28
A dedicated on-line discussion group (eg, on a blog)	9

**12. Finally, how often do you use a computer?**

Every day	45	About once every 2 to 6 months	2
About once a week	10	Less than every six months	3
About once a month	3	Never	1



## If you have time...

### between now and the next meeting, you could...

- Talk with your friends and family about the issues we've discussed – what are their views?
- Save newspaper or magazine articles that you think it would be interesting for us to look at
- Ask your GP surgery if you can see any personal information they hold on you...how do they respond?
- Record the number of times you are asked to give personal information between now and the next session, who asks you for it and what they ask for
- Ask someone who requests personal information from you who they are going to share it with
- Make a list of all the public and private organisations you think hold information about you



nothing to hide,  
nothing to fear

**Medical  
research  
comes up  
with the  
answers**

**Got something  
to hide?**

Man opts out  
of NHS database

**Benefits Agency owes hundreds  
to pensioner living in poverty**

**Police IT  
consultant  
leaves laptop  
on train**

**Doctor informs DVLA of  
man's head injury**

**WPC killed by  
man with  
paranoid  
schizophrenia**

**Computer systems unable to deal with  
all the 'odd' cases claiming benefits**

**Mrs Ellis gets income support**  
- without having to fill in forms

## The Khan family has the answers at last

Two of the Khan family's four children have been born with birth defects and Mr Khan has recently been diagnosed with heart problems. The Khans are health addicts and Mrs Khan was very careful during her all of pregnancies to watch her diet and get plenty of exercise and rest. The doctors who looked after the two youngest children couldn't give the Khans an answer when they asked what could have caused the defects.

Government information-sharing has finally provided an answer. Over the past ten years, health researchers have looked at information on birth and death records, cancer registrations, birth defects, hospital and GP, and benefits data. They have looked at this information together with the records of where people have lived throughout their lifetime to see if they can spot any patterns. When this research was published, the Khan's consultant thought that it might help her to explain what had caused the birth defects.

It did. They had moved house two years before Mrs Khan became pregnant with her two youngest children and the health research showed that environmental pollution in the area meant that children conceived there more likely to develop problems in the womb than children living elsewhere in the country. The health researchers learned too that people who had lived in that area were more likely to develop heart problems. The consultant can't say for sure that this is behind the Khan's problems, because the identity of all the people tracked in the research remains protected. But it's given them more information than they've so far and that's taken a great weight off their minds.

- What safeguards would you want to see in place before information sharing of this kind took place?
- Can you think of any benefits to your children or grandchildren if health research based on this kind of information sharing started to take place within the next 5-10 years?

Do you have any concerns about health researchers using information in this way?

## Easy driving

Most of the time these days I ride my bike – it's so much easier for short journeys and it keeps me fit. But there are some occasions when only a car will do. There's this new system now, that makes things easier. It links up two systems that have been around for a while. There are two bits to it. One is for me, really. There's a gadget in my car that I use to tell a big computer which routes I use regularly – say from home to work, or from home to my daughter's house, which is around 200 miles away. I can tell it the sort of routes I like too – like avoiding motorways. I can even tell it how often to send me new traffic updates. When I go on a journey, the phone tells a big computer somewhere and the big computer works out the best way to get there and tells me. It doesn't just look at a road map but takes all the other information it's getting, from other people on the road I suppose, and maybe from the traffic police, about road conditions – things like accidents and traffic jams – though I'm not sure about how easily it recognises the large groups of sheep in the road that I meet on the way to my daughters!

The other bit collects information on where I'm going and when and how well I'm driving! Instead of paying a fixed road tax rate, I pay depending on how much I use my car and when – so if I use it at busy times I get charged more. When my friend had her car stolen, they used this system to find it, because when she told them they could track it using the gadget in the car. Insurance companies are using it too, to work out insurance premiums – if you use your car a lot, your insurance costs go up.

- What would be the main social benefits of this system?
- What would the advantages be to you personally?
- What concerns do you have about linking insurance company and DVLA databases?
- What are the disadvantages to you and society of such a system?

## Is your health information secure?

You've probably noticed how efficient your doctor is these days. The brown cardboard folders stuffed with notes written in handwriting that no-one could understand have gone. Everything is at your GP's fingertips. There is enough information on you to build a full picture of your social, sexual, religious and occupation history. If your GP needs to prescribe a drug for you, she can call up the different options available, to find the one that suits you best – and what the side effects might be. If you go visit accident and emergency or have to go into hospital for a while, they'll have access to all this information, so they can make sure you get the right treatment, the right drugs. It's all plain sailing now.

But for Mark Robinson, things got bumpy. Mark's a smart young man, used to computers and alert to scams - like those emails that ask you for information about your bank account or credit card. Recently he got an email from his GP. It said they were updating records to make sure information was correct and included a link to a secure NHS website. So he clicked on the link, filled in all the information he was asked for and thought no more of it. What Mark didn't know was that the email didn't come from his GP, but from an internet fraud ring. Hundreds of thousands of people around the UK have been directed to this site, which looks just like the secure NHS site, and many of them will not have realised that it was a scam. Police don't yet know the extent of the fraud or what the fraudsters intend to do with the information they have gathered.

- Do you think individuals should have responsibility for updating the information that is held about them – for example, going to a secure website to register a marriage, a divorce or a change of address or other circumstances?
- Do you think individuals should have responsibility for the accuracy of the information that is held about them?
- What protections could be put in place to make sure that frauds like this one are reduced to a minimum?

## Pensioner gets the cash

Under the government's pension credit scheme, Mrs Smith will be entitled to income support when she retires next month. Mrs Smith didn't know that, but this didn't matter. New information sharing across public agencies means that Mrs Smith has already been identified as someone who will be entitled to help once she stops working. Now, there will be no need for her to grapple with the 35 pages of notes to help her fill in the 15 pages of the application form.

It's a lot of information sharing:

- current income, including any benefits
- who lives with her in her household,
- her savings and her partners, including any stocks or shares
- details of her mortgage
- any private pension schemes she or her partner pay into, or other pension payments she might be due
- any work she does

Before this new information sharing scheme was introduced, Mrs Smith would have had to sort out the documents, looking for proof of all these things, fill in the form, send it off, wait to hear if she'd filled it in correctly...it would have taken ages and been quite stressful for her. Now, because this information is held on a single database, she doesn't have to bother with any of this – she just has to wait for the money to appear in her bank account!

- Do the benefits to Mrs Smith outweigh any concerns she might have about all this information being shared?
- What safeguards do you think should be in place to make sure that Mrs Smith's information is secure?

-