Office for National Statistics

Beyond 2011

Beyond 2011 Public Attitudes Research: Report on 2010 Focus Group Research

April 2014

Background

The Office for National Statistics is currently taking a fresh look at options for the production of population and small area socio-demographic statistics for England and Wales. The Beyond 2011 Programme has been established to carry out research on the options and to recommend the best way forward to meet future user needs.

Improvements in technology and administrative data sources offer opportunities to either modernise the existing census process, or to develop an alternative by re-using existing data already held within government. Since methods for taking the traditional census are already relatively well understood most of the research is focussing on how surveys can be supplemented by better re-use of ‘administrative’ data already collected from the public.

The final recommendation, which will be made in 2014, will balance user needs, cost, benefit, statistical quality, and the public acceptability of all of the options. The results will have implications for all population-based statistics in England and Wales and, potentially, for the statistical system as a whole.

About this paper

This paper provides the results from a set of focus groups carried out by the Data Collection Methodology Census and Social branch (DCMCS) of the Office for National Statistics. The research was carried out to explore public attitudes towards data sharing. It led on from a quantitative study which was conducted by the Beyond 2011 team in 2009. The aim of the focus groups was to gauge public opinion on the use of administrative data, the creation of a social statistics database and the creation of a social register. This report details the findings of the focus groups with a view to informing future strategies for communicating with the general public. It is one of a series of papers being published providing details of the public acceptability research undertaken by the Beyond 2011 Programme.

For more information

- Data Sharing between Government Departments: Report on Public Acceptability (November 2009)
- Beyond 2011 Programme Public Attitudes Research: Report on 2012 Opinions and Lifestyle Survey
- Beyond 2011 Programme Public Attitudes Research: Report on 2012 Focus Group Research
- Beyond 2011 Programme Public Attitudes Research: Report on 2013 Opinions and Lifestyle Survey
- Beyond 2011 Programme Public Attitudes Research: Report on 2013 Cognitive Testing by Independent Social Research Limited

Search Beyond 2011 @ www.ons.gov.uk or contact : beyond2011@ons.gov.uk

1 Executive Summary

In February 2010, the Data Collection Methodology Census and Social team was commissioned by the Beyond 2011 Project to undertake qualitative research investigating public attitudes towards government data sharing. This research consisted of six focus groups (44 participants) held across England and Wales and followed on from a quantitative study conducted by the Beyond 2011 Project in 2009.

Key findings

- Participants did not have a clear understanding of what data was held by the Government, which government departments hold this information, what it is used for and who it is shared with. It was suggested that a central database may already exist, but it was felt that only separate databases were used.

- It was clear that it was difficult for participants to translate data into statistics, and statistics into decisions, actions, and ultimately benefits for the public. There was also a lack of awareness regarding the distinction between the use of data for statistical purposes and its use for operational purposes.

- Participants' acceptance of data sharing had certain limitations, such as a clear reason why the data needed to be shared. There was an expectation that providing information to the government would have a direct, beneficial effect on that person.

- Participants' opinions and views of the Government were based on their own knowledge and experience, rather than any direct communication from the Government. It appeared that gaps in their knowledge were filled by negative communications from the media.

- It was felt that government departments did not communicate with the public regarding what data they hold, and what they use it for.

- The Government was perceived to be incompetent, and this idea had been reinforced by the media. It was also felt that the Government did not take its responsibility for the public's personal data seriously, and was not seen to be accountable for it.

- It was evident that there was a need to regain some control of the public's data, as it was felt that it was the public's right to view their own data, and the Government should ask permission to use it.

- Security of the public's data was a major concern for the groups. The groups' acceptance of the central database was dependent on appropriate security being in place. It was feared that the use of the database would result in identifiable data being released.

- The security implications of data about every member of the population in one place was also a concern, but levels of access to the database, dependent on need, were thought to be reassuring.

- There were sometimes high, misguided expectations of how the database could benefit the public, which were related to a misunderstanding of its purpose, for example that it would be used for administrative purposes.

- Concerns were raised about the future of the database. It was feared that a change in government may result in the database being used for malicious reasons. An option to 'opt-out' of the database was thought to be important but not expected.

- In terms of the implications for a central database, these mainly focus on communicating with the public, and educating the public. It was recognised that an understanding of the uses and potential benefits of statistics might help to increase the public's acceptance of the central database. The high expectations for the database will also need to be carefully managed.

- Reassurance about security is key. Again education about how statistics are kept anonymous will be important. Participants' concerns about the potential future misuse of the database would also need to be addressed.

2 Introduction

The aim of the Beyond 2011 project is to investigate how the needs of users of socio-demographic data can be met following the 2011 Census. In February 2010 Data Collection Methodology Census and Social Team (DCMCS) was commissioned by Beyond 2011 to undertake qualitative research investigating public attitudes towards data sharing between government departments. The focus group work described in this report complements other work packages undertaken to investigate the feasibility of alternative systems to a decennial census. It leads on from a quantitative study which was conducted by the Beyond 2011 team in 2009:

Data Sharing between Government Departments: Report on Public Acceptability (published in November 2009).

The aim of the focus groups was to build on this quantitative research and explore the issues identified in more depth. The report will detail the findings of this research, which will then inform future strategies for communicating with the general public.

3 Background

In April 2009, the Beyond 2011 team used the Office for National Statistics' (ONS) Opinions and Lifestyle Survey to investigate public attitudes towards data sharing (ONS, 2009). The team commissioned a module of seven questions, designed to investigate the public's understanding of how the Government holds information about the population, their preferences for how data is held, and their views on the creation of a population database. The study found that over 50 per cent of respondents were aware that this type of database did not exist, and that approximately two-thirds of respondents were supportive of the government creating a population database. Two-thirds of respondents also felt that a population database would reduce fraud, tackle terrorism, and keep track of asylum seekers, refugees or immigrants. Those who opposed the creation of such a database (18 per cent of respondents) were concerned about data security and too much information being shared across government. These results were comparable to those found for a similar project, the Citizen Information Project, in 2004.

Following on from the quantitative research, the purpose of this qualitative work was to investigate the public's understanding of the issues in more detail. This report presents the findings from the focus groups and discusses the implications of these findings for sharing of data between government departments and the creation of a central population database.

4 Methodology

4.1 Sample

4.1.1 Composition

A total of six focus groups were conducted, involving a total of 44 participants. Taking the subject matter into account, it was felt to be important to separate the groups by educational attainment level so as not to disrupt the group dynamic, i.e. to try to avoid any sense of intimidation and to ensure that discussions could be held at the same 'level' of complexity . At each location the participants were split into two groups which dictated which focus group they attended; 'more highly educated' (MHE) (above A-level or equivalent) and 'less highly educated' (LHE) (A-level or equivalent and below). The groups comprised a mix of age and sex. Participants with a range of ethnicities were represented in the groups, including those who identified as White British, Black African, Black Caribbean and Indian.

The focus groups took place in three locations: Cardiff, London and Manchester. The earlier quantitative research had shown some variation in opinion by location (e.g. 30 per cent of respondents in the North West believed a central database already existed compared to 19 per cent in London) which influenced the location of the focus groups.

4.1.2 Selection

The recruitment of participants was conducted by the assistant moderators using purposive sampling techniques. This technique involves selecting respondents with particular features or characteristics which will enable detailed exploration of the research objectives. The sample is intended to cover the range of characteristics of interest. It is not the purpose of qualitative research for statistical inference to be drawn from findings, or for samples to be representative of the proportions of the characteristics of interest in the population. Participants with the desired characteristics were identified in the ONS respondent register. This is a register of respondents who have taken part in the ONS Opinions and Lifestyle Survey and have given their permission to be contacted again to take part in other research. Recruitment using the respondent register was augmented by other recruitment techniques, including flyers and advertisements.

As is common practice, participants were given £40 as a token of appreciation for their time and to cover travel expenses.

4.2 Research technique and procedure

DCMCS undertook this research using a series of focus groups. Focus groups allow participants to interact with each other; they can discuss their own thoughts and opinions, and also consider those of others. Listening to the experience of others in the group allows participants to reconsider and refine their own views, further stimulating the discussion. As Ritchie and Lewis (2003) explain, 'as the discussion progresses (backwards and forwards, round and round the group), individual response becomes sharpened and refined, and moves to a deeper and more considered level'.

Each focus group was conducted using a protocol to serve as a plan for the focus group. This not only ensured that relevant issues identified in advance were covered but also allowed discussion of other related issues that arose. Protocols also provide consistency where more than one moderator is contributing to the work, as was the case for this research. The protocol covered three main areas; awareness of data sharing, preferences for data sharing, and views on a single population database. The protocol used for the focus groups can be found in Appendix A.

4.3 Analysis

After completion of each focus group, a written summary was prepared by the assistant moderator. These summaries were based on the assistant moderator's notes that were taken during the focus group, and were shared with the groups at the end of each session to ensure that the main messages were captured. The recordings were then transcribed by an external transcription company.

A thematic approach was used for the analysis which was carried out jointly by DCMCS members. The transcriptions formed the basis for the analysis which commenced with a stage of familiarisation with the data. This familiarisation involved careful reading and re-reading of the transcriptions, followed by organisation of the text into themes, ideas, concepts, anomalies, similarities or inconsistencies. These findings are drawn together into the results presented later in this report. Verbatim statements by participants are presented in italics.

4.4 Confidentiality and ethical issues

DCMCS followed the Royal Statistical Society (RSS) Code of Conduct and principles set out in the UKSA Code of Practice while carrying out this research. In line with ethical guidelines the participants were informed at the beginning of each focus group about the purpose of the focus groups; that their participation was voluntary; that they could withdraw from the study at any time; and that the information they provided would be kept confidential to the research team, and reported thematically along with information provided by other participants. Additional measures such as encrypting files, separation of personal data and use of secure storage were also employed to protect the confidentiality of the participants and the data.

5 Public understanding of government data sharing

5.1 Knowledge of what data is held and by whom

As an introduction to the topic, initial discussions in each focus group covered what types of information the government holds, and which departments hold this information. This exercise provided an insight into participants' knowledge of what data is held and who it is held by and also allowed the subsequent discussions to be more focused.

A range of examples of personal data that is held by the government were provided by participants. Some examples were general across a range of departments, including information such as date of birth, while others were more specific to certain government departments, for example driving licence:

Addresses; date of birth; marital status; benefits; criminal records; driving licence; tax codes; National Insurance number; travel records; passport; employment records; births, marriages and deaths; DNA; blood group; medical records; religion; residency in the UK; pension records; credit rating; membership of lobby groups; civil court proceedings; income; sex; ethnicity; immigration status; NHS number; bankruptcy; biometrics; phone number.

Appropriate examples were also given for the government departments who held this information:

DVLA; NHS; police; Department of Health; Social Services; Home Office; Foreign and Commonwealth Office; National Archives; local education authorities; DWP; Passport Office; ONS; MI5; MI6; Inland Revenue; Customs and Excise; Her Majesty's Court Service, local councils; Department of Transport.

However, although it was evident that there was awareness that data was held by the government, and who might hold this information, there was also a lack of understanding regarding exactly what data was held and by whom:

> *"What is stored exactly on there. You know, does it go right from your birth date down to what books you're taking out in the library, how much?" (LHE Cardiff)*

5.2 Understanding of how data is obtained and stored

It was understood that personal data could be obtained by the government via several methods, such as surveys, the census, and other forms and applications relating to the administration of services. It was also acknowledged that the public provide the government with this data:

> *"We very kindly give it to them." (MHE Cardiff)*
>
> *"Forms basically, just forms you fill in." (LHE Manchester)*

It was thought that the government could also obtain data covertly, although this was discussed in the context of criminal behaviour. A distinction was made between data that is held by government, and data held by private organisations that the government can have access to if required.

It was suggested that a central government database may exist, but, as found in the quantitative research, it was felt that only separate databases were used:

> *"It's not held in one block…it seems that it's all around different offices for different things." (LHE London)*

In contrast to what was found in the quantitative work, there appeared to be no regional variation in this opinion.

5.3 Understanding what the data is used for

There was an awareness of the commercial value of personal data; it was stated that private sector organisations traded in the public's personal information, and this data was described as a 'commodity'. This understanding of the value of their data meant that they felt protective of it, as discussed later in the report.

However, there was uncertainty regarding exactly what the government used personal data for:

> *"I actually don't know much about it…I don't know a lot about why information is kept or what it's used for." (LHE Manchester)*

Planning and statistics were given as examples, and there was some awareness that statistics were used to make decisions:

> *"Economists plan what's going to happen, how government is able to make policies, whatever policies they need to, they think, they feel they're going to deal with, whether it's social issues such as health or criminality…all these different type of statistics build a picture of what society, where society is going." (MHE London)*

Using the data for statistical purposes was deemed to be acceptable, and recognised as useful, on the condition that statistics are anonymous:

> *"I'm happy to be represented as a statistic." (MHE Manchester)*

> *"Anonymous statistics, it doesn't bother me." (LHE Manchester)*

However, it was clear that there was a difficulty in translating data into statistics, and statistics into decisions, actions, and ultimately benefits for the public. Administrative purposes were cited as a use for the public's personal information. Examples provided by participants were mainly associated with administrative uses, such as payment of benefits. A distinction was made between data used for statistics and data used by the government for monitoring an individual's behaviour:

> *"Everybody's given sort of a general comment, a generalisation of it's for trends and for data…but we're checked if we've got a driving licence, we're checked if we have points on our driving licence, we're checked if we've got a TV licence…it's not just the general information as a collective; its down to individual information." (MHE Cardiff)*

The lack of certainty concerning how the public's data was used was apparent from the misunderstanding that the government uses the public's personal information to target votes.

5.4 Knowledge of data sharing

There was no consensus regarding whether data sharing took place or not. Participants' knowledge of data sharing was tied in to their own personal experience with the government. For example, instances where contact details had been changed for one government department but not updated for the others:

> *"I don't think they communicate with each other." (LHE Manchester)*

Those participants who worked for government departments sometimes had direct experience of data sharing, and were therefore confident that it took place. However, others were unsure:

> *"I don't know how many government departments have a record of me, and I don't know if they're joined up." (MHE Cardiff)*

It was assumed that sharing takes place, but the public has not been made aware of it. Sharing was seen as a way for government departments to work efficiently, and criminal record checks were cited as an example of how this worked in practise:

> *"The CRB is a very good example of how data's shared." (LHE Cardiff)*

Other reasons for data sharing were given, such as investigating fraud, for the security of the country, and for criminal or child protection purposes. These examples were salient for participants, as they had heard about certain cases in the news:

> *"It's only very recently the police have just shared information isn't it…so you had the Soham murders…because the information wasn't shared then his criminal record wasn't thrown up." (MHE London)*

Initial discussions concerned data sharing between government departments, but reference was also made to sharing between the government and commercial companies. Participants gave the example of buying car tax online from the DVLA, and how this must mean that this government department shares data with insurance companies. The links between the government and commercial organisations are discussed later in the report, but there was a general feeling of uneasiness about this idea:

> *"I think it becomes more worrying when the information we give to the government is linked to some external agency, that if insurance companies could find out the state of our health." (MHE Cardiff)*

It was also thought that data sharing took place between government departments in the UK and abroad. Participants also seemed wary of this idea:

> *"It's a worldwide system now…there's a relationship between one government and another government and what they pass between them, and your information could be sent to someone in authority in any country on the face of the planet, and you know nothing about it, you don't know it's gone." (LHE Cardiff)*

In contrast to these examples of personal level uses of data, it was also recognised that sharing might take place in order to facilitate government planning and to target funds:

> *"It's just to build up a sort of overview of sort of the population and who lives in what areas." (LHE Manchester)*

> *"They can target funds more accurately." (MHE Cardiff)*

The groups acknowledged the benefits of data sharing. It was recognised that it could benefit the government in terms of efficiency, but also benefit the public in terms of reduced burden:

> *"For speed and efficiency." (LHE Cardiff)*

> *"It may also reduce the burden put on you the citizen." (MHE London)*

5.5 Preferences for data sharing

The groups' acceptance of the idea of data sharing was dependent on why the data needed to be shared:

> *"If they use it for the right reasons I don't see any problem." (MHE London)*

Data sharing for the purposes of child protection, or to investigate criminal behaviour, was thought to be acceptable as there was a clear purpose and benefit:

> *"I agree with it if, do you know what I mean, somebody's doing wrong that information should be openly available to the agencies that need that information." (LHE Manchester)*

Data sharing was acceptable if it resulted in a personal benefit to the individual. Examples given related to efficiency:

> *"Or hospitals. So, for example, when I go in they know what my blood group is and it's beneficial that way." (MHE Cardiff)*

There appeared to be an expectation that providing personal information to the government would have a direct, beneficial, effect on the person providing that data. These expectations were sometimes unrealistic or unrelated to the purpose of data collection for statistics:

> *"If you're getting all the information from me, I expect to have it work against any fraudulent people trying to get my identification." (LHE London)*

This expectation was carried forward to the idea of the central database, as discussed later in the report.

It was noted that the personal benefits of data are not obvious, which makes it difficult to support government initiatives involving personal data:

> *"the problem is I think that you, no one trusts that information going out there because it's never proved to be useful to members of society…maybe people like us need to be able to ask what are you using it for, and have the right to be told what you're using it for, and just have it explained" (LHE London)*

However, it was made clear that the groups' acceptance of the idea of data sharing had certain limitations. It was felt that the most important factor was that government departments who want to access certain information should have a concrete reason for wanting to do so:

> *"There should be certain steps they have to go through to prove that they have the right to look at that information and what they want it for and be fit for purpose." (LHE London)*

It was also felt to be important that departments only receive the minimum amount of information necessary, and that they don't have access to more than they require:

> *"They should only share relevant information I would say…they shouldn't give them the whole book." (LHE London)*

There was recognition that not every piece of personal information will be relevant to every government department, and therefore there should not be open access to personal data:

> *"At* [name of government department] *we put down what qualifications people have. But the Inland Revenue's not going to want that information." (LHE Manchester)*

Participants were wary about the idea of government employees looking at identifiable information held by other government departments, without a clear purpose:

> *"The thing that makes me very uneasy is the fact that maybe if I, I don't know, worked in the Ministry of Justice I'd be able to go to the DWP database, be able to type search someone's name and date of birth and be able to have everything about them." (MHE Manchester)*

Regarding which data shouldn't be shared, specific examples were rarely given as their acceptance of the idea of data sharing was dependent on the reason for data sharing, and therefore what is and isn't acceptable could fluctuate. However, it was clear that there was concern about the potential disclosure of certain, more sensitive data, such as religion or political affiliation:

> *"I think personal beliefs, like religious beliefs or political beliefs, anything that is subjective to a person should not be in the public domain, that should be private." (MHE Cardiff)*

It was feared that if this type of information was disclosed, it could lead to unfair judgements:

> *"I think other people can make subjective assumptions." (MHE Cardiff)*

There was also a concern that sharing took place without their knowledge:

> *"What would worry me is that access would be for reasons that you're not aware of, that you don't know." (LHE Cardiff)*

It was evident that there was some difficulty in formulating an opinion of data sharing. It was recognised that on the one hand there was an expectation for more efficient services from the government, but on the other hand there were concerns about security or being monitored too closely:

> *"I like two ways, I mean I like the idea that if a child had a problem with the parents before that's known to the school, but I also like the idea that someone can move to a different county and have a fresh start, but the two don't go together completely do they?" (MHE Cardiff)*

The consequence of this was an acceptance that the benefits of data sharing have to be considered against the disadvantages:

> *"If they do get that information of my address change, so there is a seamless flow of information between these two government bodies, that could bother someone who may not wish to share information. But if it doesn't flow then there is a redundancy that you have to inform the Inland Revenue that okay look, I have changed my address." (MHE London)*

> *"Sharing information is good in certain, but again, if that information gets in the wrong hands…" (LHE Manchester)*

> *"Really we take two different attitudes aren't we, convenience for ourselves and concern about our security." (MHE Cardiff)*

In summary, how the data is shared, rather than what data is shared, appeared to be an important distinction.

5.6 Awareness of rules surrounding data sharing

Participants believed that there were rules regarding the collection of data and the sharing of that information. Regardless of whether they referred to a particular law, it was felt that rules existed, and should be followed:

> *"There are laws…you have to comply with a particular law." (MHE London)*

> *"There are certain things you can do and certain things you can't presumably." (LHE London)*

> *"There's the Data Protection Act isn't there. They're only allowed to use the data for specific purposes and what it's been gathered for." (MHE Cardiff)*

Those with experience of working for the government noted that there were rules governing their access of a database, but were sometimes surprised at how government departments shared data:

> *"Obviously you have to sign everything and get things checked that you're not kind of searching for people you shouldn't be, but I was actually quite shocked that there was quite, okay it was limited but there was a certain amount of like information shared*

> *between, even like when they're completely unconnected. It's quite scary." (MHE Manchester)*

It was acknowledged that data sharing rules could be too strict and therefore hinder efficient working practices, however this was mentioned in relation to sharing to solve crime. Reference was made to high profile child protection cases, where a lack of communication had resulted in tragic circumstances:

> *"Where the departments had not communicated at all with each other, so there's something falling over there." (MHE London)*

It was presumed that there were laws or rules governing how data can be stored and used, but there was varying confidence in how well the government protects data and whether these rules are followed.

It was suggested that permission had to be sought from the public in order for the government to share personal data. This idea had been reinforced by the experience of the NHS asking permission for medical records to be included on their database. There was an expectation that permission would be sought for their data to be shared, and this idea is explored in more detail later in the report:

> *"I'd always want to be asked and to give my permission or have the opportunity to withhold my permission if I wanted." (MHE Manchester)*

5.7 Acceptance of data as part of life

It was acknowledged that government departments need to collect, hold and use the public's personal data, and that this is widespread across government:

> *"Every sort of government body that exists will have some sort of information about you at some point in your life I should imagine." (LHE Cardiff)*

The groups were of the opinion that advances in technology, i.e. the internet, have led to easier access to data. It was also felt that if the government wanted to find out certain information about an individual, then that could easily be done:

> *"I think if an agency wants to find out about you they can find out everything about you more or less." (MHE, Manchester)*

There was also an understanding that personal data had become a part of everyday life. In some cases, there was more concern about how personal data could be used by a commercial organisation, rather than the government:

> *"I'm more worried about the commercial world like you say, and the [name of large retailer] of this world that are Big Brother, you know, and they watch everything you do…the commercial world scares me more than the government world." (MHE Manchester)*

There was also an acceptance that data sharing would become a part of life:

> *"Whether I like it or not it's going to happen and I sort of face that fact." (LHE Cardiff)*

However, there was also concern about this acceptance. It was felt that the more data collected, the more accepted it becomes, and it would be difficult to then change the situation. Participants were wary about being too accepting of the situation, and where this would leave them:

> *"The danger is once you stray over it then it's very difficult to get back because some people grasp that information, use that information and say ah it's vital. You have to be so very careful as to what is vital, and if you're not careful all sorts of things can stray over that line." (LHE Cardiff)*

5.8 Contributing factors to public's understanding

Participants had several sources of information regarding government data sharing, none of them being communication from the government itself. Their views and opinions are based on their own knowledge and experience which hasn't been influenced by the government directly.

One of their sources of information was personal experience of dealing with government departments. This was either for administrative purposes, such as for the payment of benefits, or alternatively, participants had experience of requests from government departments for their data to be used, such as for an NHS database. In some cases, participants worked for a government department, or had previously been employed in the civil service, and shared their experiences with the group. It was also noted that participants' gained their information 'on the grapevine' i.e. hearing stories from friends and family and 'word of mouth'. However, the major source of information, which appeared to play a strong role, was the media:

> *"Mostly the media I think and Google." (LHE London)*

> *"I think a primary source for me is the news, just reading the paper." (LHE Manchester)*

5.8.1 The role of the media

In terms of communications from the media regarding the government and personal data, it was recognised that these communications are often negative. In all groups, reference was made to high profile cases of data security being compromised, such as CDs being left on trains or USB sticks going missing, and the frequency of these reports appearing in the media:

> *"Look at how many times people in the government, MPs and government officials, you've seen it in the news, have lost paperwork or memory sticks." (LHE Cardiff)*

> *"You'll see week after week government emails are leaked." (LHE Cardiff)*

The effect of these stories was evident in that all of the groups raised these issues repeatedly. It appeared that regardless of how many incidents of data security compromises there have actually been in government, this is what is remembered when thinking about government data. However, it was acknowledged that the media's coverage of these incidents may not be entirely accurate, or may have been exaggerated. The effect of these stories, i.e. increasing anxiety, was also noted:

> *"Well the thing that scares me, okay it's something that I've obviously read in the media and has probably been escalated but it's when you hear things about discs being left on trains and like computers thrown out." (MHE Manchester)*

> *"I think at the moment in society as well there's quite a big hype around identity fraud. Like any tiny story related to identity fraud is immediately picked up in the media…so I think people are quite fearful about it." (MHE Cardiff)*

> *"I think we're made to feel quite anxious about the media, possibly unnecessarily." (MHE Cardiff)*

There was an awareness of the impact of the media on the public's views about government initiatives. For example, the media's negative coverage of the idea of ID cards was thought to have contributed to its failure:

> *"I suppose it's the negative publicity from the media is probably one of the reasons why the ID thing isn't going to come in." (MHE Manchester)*

Participants felt that they would feel more comfortable with the idea of data sharing if the government could be relied on to be competent, but also if negative stories were not reported to the extent that they are in the media:

> *"If they were competent and if you didn't read stories in the press…then I wouldn't feel – well I don't know, I've still got reservations but I'd feel a bit happier if what they had remained secure." (LHE Cardiff)*

It was suggested that more publicity for positive stories might increase public confidence in the government. However, it was recognised that the media strongly influence what is reported, and that a positive government story is not necessarily what the general public wants to read. Nevertheless, a different strategy to ensure that the government received fair publicity was thought to be important:

> *"I think one problem that anyone and everyone is going to have, when something goes wrong that is always heavily publicised. When things go right, yes, the media aren't going to pick up on it because it's not an interesting story but perhaps there could be a way to publicise that better. And that would maybe increase confidence, but the country is rather controlled by the media so I don't know." (LHE Manchester)*

5.9 Lack of distinction between statistical and administrative purposes

Throughout the discussions, it became clear that participants did not have a good understanding of data, statistics, and their purpose. Consequently, it was evident that a clear distinction was not made between the use of data for statistical or administrative purposes. This resulted in high expectations for how a government database, which will be used for statistical purposes, would benefit them; for example solving crime or helping an application go through.

However, some participants did demonstrate an awareness of how their data was used for statistical purposes by the government:

> *"I suppose demographics is another area, where we live, what we do, how long we live, and that I would think would lead to government departments being able to say well we shall need to spend X in the future on pensioners…you have to have some kind of plan because you can't just have the same monies paid out from taxes and all the other revenues that are raised if you don't have any statistical information to support what you're going to spend it on." (LHE Cardiff)*

> *"Benefit take up has been more in the last five years that we envisaged it was going to be so, do you know what I mean, you're using it." (LHE London)*

> *"To help the government to have an idea of what everybody's doing, and then to help them to make decisions about…where to go with things." (MHE Cardiff)*

Specific examples were occasionally given of how they felt statistics could influence decisions:

> *"Say there's loads of children being born in Milton Keynes they'll know that they've got to start building primary schools." (MHE Cardiff)*

6 Communication of statistics and their use to the public

As noted in the previous chapter, there was a lack of understanding regarding exactly what data was held by the government, which government departments hold this information, what it is used for, and who it is shared with. The groups' views were based on their own knowledge and experience, rather than on direct communication from the government. The media was thought to play a significant role in informing participants of the government's ability to hold data. It was also evident that there was a lack of awareness regarding the difference between data that is used for statistical or administrative purposes. All of these findings can be related to a lack of communication from the government.

6.1 Lack of transparency

Gaps in the knowledge of the participants obviously pointed towards a lack of communication from government departments. However, there was also felt to be a lack of transparency regarding what data is held, who holds it, what it is used for, and whether it is shared:

> *"I think they're very secretive, far too secretive about where it all goes." (LHE London)*
>
> *"You don't know how the information is going to be held and therefore possibly passed on." (MHE Cardiff)*
>
> *"I think we don't always know how our data is going to be used by the different government bodies." (MHE Manchester)*

The consequence of this was that participants felt there was a need to know how to find out this information. However, there was also felt to be a lack of transparency regarding how to go about finding out what data the government holds:

> *"But who does? Who knows how to go about doing it? Whereas if it was a protocol then you knew how to do it, you know, I think that'd be quite a fair thing to do." (MHE Manchester)*
>
> *"I did actually look on the internet today to see what kind of information the government provides about the information they hold on people. But there wasn't anything." (LHE Manchester)*

This lack of transparency appeared to extend to how the public's data is held:

> *"Once they take your information it disappears and then we haven't got a clue who's got access to it." (LHE Cardiff)*

It was felt that if the government was more open about what data it held and how it was handled, this might increase the public's confidence in the government and reduce any sense of government 'monitoring':

> *"I think they just need to be more transparent, say, from the departments about what information they hold. I mean just in general, not saying we specifically hold all this, and*

> *what they do with it; do they let it go out of that department, which departments are they letting it go to, just to give I suppose the public more confidence in their handling." (LHE Manchester)*

> *"Be more open about things so people don't feel like it's them being snooped on." (LHE Manchester)*

6.2 Direct communication from Government

The groups demonstrated an interest in how their data was handled and were keen to know about the uses of data and statistics. There was a need to know how statistics resulted in decisions, and how these would benefit the public. Participants were particularly interested in the personal benefit to them. It was felt that if the benefits of data and statistics are communicated to the public, then this might increase public acceptance:

> *"If you know that some good is going to come from people knowing this information about you then you don't mind them knowing it." (LHE Manchester)*

It was thought that the lack of awareness of the use of statistics was the result of poor communication by the government:

> *"Half the time it's just bad communication because when somebody. Sorry if* [participant's name] *thinks that, genuinely thinks the only purpose of the census is for voting you've done a really bad PR job as a government or civil service." (LHE London)*

It was noted that there was little communication direct from the government. However, it was felt that more communication from the government would be welcomed, particularly to inform the public that their data is being used:

> *"I would like an acknowledgement as well to say they're looking at my information or can you check this information is correct…you are notified it's being checked or information's being passed." (MHE Manchester)*

The visibility of the government was also mentioned. Government surveys were cited as a means of seeing the government at work, and it was felt that this was reassuring:

> *"I think it's better that you go out into communities and get people to fill in surveys and things like that, it's nice to know what the government are doing, what you're doing really. It gives people more confidence rather than it just being all computer-based and nobody knows you're doing it but you're constantly gathering this information, it's a bit unsettling actually." (LHE Manchester)*

6.3 Government incompetence

The view of government departments who hold personal data was not positive. Personal experience of episodes where data had been lost were recounted to the group, and high profile cases in the media were also discussed. In later discussions there was scepticism about plans for a central database as it was felt that the government was too incompetent to take this idea forward.

Government departments were not referred to in a positive way:

> *"I mean the ridiculous mistakes that they make all the time." (MHE Cardiff)*

There was a suggestion that the government did not have adequate procedures in place for storing personal data. This idea had been reinforced by reports in the media:

> *"When it comes to the government, yes, we'd like to hope and feel that it would be safe but the reality if you look at obviously news stories of people leaving data files on trains, planes, taxis, wherever else you want to call it, we know reality that there doesn't seem to be a procedure as a whole." (MHE London)*

The groups' perception of an incompetent government was also reinforced by their experiences of interaction with the government and discovering that their data was inaccurate. As a consequence, it was felt that it was important for the public to be able to view their own data, not only to check for accuracy, but also because it was felt that they have a right to view their own information.

6.4 Awareness of other Government databases

Participants cited other databases that they had heard the government is creating.
In particular, participants referred to the failure of particular government databases that they had heard about in the media:

> *"I think in England there's a new computerised service that's been a disaster I think, it's cost something like £200 million more than it should have and it's not working." (LHE Cardiff)*

> *"I've read about the NHS data switch they've been attempting to set up, because I read Private Eye, from what I've been able to glean from that it's been an absolute disaster." (MHE Manchester)*

There was concern that if one government department could not collate their own records together, then sharing data was unlikely to work. There was scepticism that the government would be able to carry out data sharing efficiently, and concern that there was no guarantee it would work:

> *"If this is just the issue they're having with one agency and getting all their records together, you're then talking about all agencies sharing, the amount of potential cost and time and the lack of guarantee that something is, that everything will be perfect about it…they can't get it right." (MHE Manchester)*

It was also felt that government databases are not accurate. This perception of the databases was sometimes linked to personal experiences, and meant that there was a need to check if their data was correct.

There was almost a feeling of contempt that the government were perceived to be so incompetent and wasteful:

> *"*[discussing the NHS database] *The concept of it was a good concept but they've just, as usual, a government agency's kind of cocked it up…there's so much waste" (MHE Manchester)*

In some instances there was a direct reference to a breakdown in trust between the public and the government regarding how the government handles personal information. It was felt that the government had not been able to deliver adequate services with the data that it already has access to, and therefore could not be trusted to take forward new initiatives:

> *"I think the problem you have is that you've not done very well with the information you have so people feel if you've got even more, if you've got a DNA, if you've got national identification cards, then that just somehow makes you incredibly powerful and just as incompetent." (LHE London)*

Taking the idea of government incompetence further, there was also a feeling that the government are responsible for identity theft, and that their security systems can't be good enough if identity theft continues to happen:

> *"If you they get it through the internet then surely that means that the government and the powers that be haven't actually got that secure a hold on it, because if they did these identity thieves wouldn't be able to get that information." (LHE Cardiff)*

6.5 Government accountability

It was felt that the government did not take responsibility for data security lapses. It was stated that these types of incident are reported in the media, but then no individual, or department, is held accountable, and there are no repercussions:

> *"I was listening to what you were saying about the business of a memory stick that's left on a train, and it puzzles me because it seems there's no follow up, no one seems to be responsible." (LHE Cardiff)*
>
> *"No one owns up to a mistake these days either do they, personally, you know, if you're human. There's just too many people blaming computers." (LHE Manchester)*

There was a clear message from participants that if the government wishes to use the public's personal data, then it must take its responsibilities surrounding privacy and security seriously. It was felt that current practices may leave people feeling vulnerable:

> *"If you're going to have that information in the public arena then you as government have to take responsibility for protecting it as well. You can't have it both ways, you have access to all of that and then leave people vulnerable." (LHE London)*
>
> *"If something did go wrong I would want someone to be held accountable for the fact that my information has been misused or misplaced." (MHE Manchester)*
>
> *"And have people accountable for mistakes and errors instead of being oh naughty boy, off you go. It's not taken seriously enough. Everyone quotes, all companies, all big government quote data protection because it's a major, major issue. At the end of the day I don't know anybody who's been in trouble for data protection, loss of information, it needs to be taken more seriously and people need accountability…being dealt with accordingly if they make mistakes." (LHE Cardiff)*

It was commented that those who do make mistakes should be publicly punished as a deterrent:

> *"I want to see them punished." (LHE Cardiff)*
>
> *"Heavy penalties for people who violate the database." (MHE London)*

It appeared that participants felt uncomfortable with the way that their data was handled, and required accountability as a means of reassurance to alleviate their feelings of vulnerability.

6.6 The public's rights

Regarding personal data, the public's entitlements and rights were raised by the groups. It was suggested that the public would want to see their own data, or at least should be able to do this. Taking this idea further, it was also felt that the public has a right to view their own data:

> *"Absolutely everyone does have the right to check their own information." (MHE Manchester)*
>
> *"I should have access to my information." (LHE London)*

However, it was often stated that this should happen in order to check the accuracy of the data, rather than simply because it is their 'right' to view it.

> *"You are the people I'm trusting to look after that information and to do their job properly, well I equally have the right to kind of go oh excuse me, I'd like to look at that. No that's not my address or you've got that wrong." (LHE London)*
>
> *"I think it would put everybody's mind at rest. If you can actually see your data that's being held, not manipulate it in any way but you can, if you see something wrong you can then acknowledge that there is something wrong and can you check it." (MHE Manchester)*

However, once discussions turned to how the public could actually go about viewing their own data, it was acknowledged that this may not be feasible. Ideas about personal web pages were discussed, but it was realised that it would be difficult to make this secure, and may not be possible for every member of the population:

> *"But you're talking then about giving every member of the country a password aren't you? Do you know what I mean, it's not really feasible." (LHE Cardiff)*

6.7 Public control of public data

There was an underlying theme of control throughout the discussions. Participants were keen to know the details of how their data is held, for example, what security measures were in place for their data and how long it would be held for. It was also seen as important for the public to access their own information. This was discussed not only in the context of awareness of what data is held, but also to check for accuracy. There was some awareness of the Freedom of Information Act (FOI), but it was felt that the public should already be aware of who holds their data, what it is used for, and what benefits will result.

There was a feeling that the government is in control of the public's personal data, and as a consequence the public is left feeling vulnerable. There appeared to be a need to reclaim some control over their own data. The groups stated that they want the government to communicate with them and they want to be asked for permission for their data to be shared. The idea of being able to 'opt out' of government databases was also appealing to participants, for example it was mentioned that surveys are preferable to the idea of a central database because there is the option of not answering the question, or lying, on government surveys. However, for a central database, the control, i.e. withholding information, is taken away:

> *"You're saying we're getting all this information without even asking you, it's fine, don't worry. We're not inconveniencing you by getting all your information from somewhere else, whereas I might not want to give that." (LHE Manchester)*

> *"If you come round with the census I can easily lie to you, whereas, or not give you certain information whereas if you're just pulling it from other organisations then I don't have a choice in that." (LHE Manchester)*

It was also felt that once data is stored on any kind of database, the public's control of that data is relinquished:

> *"Once your data is stored on a database it's somewhat out of your control, you don't know exactly what it's going to be used for. I'm sure that quite often you're not asked permission for that and you're certainly not informed every time that your data is used." (MHE Manchester)*

Related to the lack of communication, there was also a sense of vulnerability. This was exacerbated by the perception that the government made decisions without consulting the public:

> *"They make the decisions for us and I don't think that's right. They make a lot of decisions that a lot of the public don't agree with, so we should be asked as well what we think about what's going on in the country." (LHE London)*

It was evident that there was an expectation that the public will be consulted by the government, for example to ask permission for their data to be used in certain ways:

> *"I think maybe you should run it by everybody first, so if you were to be pulling my data together for my record you'd send me something saying this is the information we're trying to get now, is there anything you don't want us to get?" (LHE Manchester)*

> *"I would want to know who was accessing. I would want to give my permission about who was accessing that." (MHE Cardiff)*

Some participants had had experience of government databases such as the NHS 'spine'. These participants recounted that their permission had been sought for this database, and would therefore expect the same protocol to be followed for other government databases:

> *"Some rights were won in the Houses of Commons or the House of Lords whereby you could be taken off the spine if you wanted to, and I decided to be taken off." (MHE London)*

7 Public perception of the security of Government data

As discussed earlier, it was evident that not all participants understood the purpose and use of statistics, and sometimes misinterpreted how they were used. The government was perceived to be incompetent and it was questioned whether it could be trusted to store the public's personal data. There was also a strong feeling that the government didn't communicate how it uses data and what it is used for with the public. All of these factors contributed to a sense of 'loss of control', and a feeling of vulnerability. This vulnerability was evident in the groups' concerns about the security of data held by government.

7.1 The growing issue of security

The groups raised strong concerns about the security of their personal data:

> *"I'd want the information to be secure, whoever's handling that must sort of do so in an appropriate manner so that not everybody can access it, only a select few." (LHE Manchester)*

Participants noted an increase in government security over the past few years. This was attributed to events such as terrorism or data security lapses. However, across all groups, concerns were raised about identity theft. Participants recounted personal experience or stories they had heard in the media. The idea of their data 'getting into the wrong hands' was thought to be a real threat and was repeatedly raised in the discussions:

> *"I wonder where them assassins got them passports from. Could have ours, you know." (LHE Manchester)*
>
> *"Somebody might hack it." (MHE London)*

Interestingly, there was an acceptance that the public themselves had a role to play in the increase of identity theft, and perhaps it couldn't entirely be blamed on the government. The amount of personal data displayed on social networking sites such as Facebook was noted:

> *"Sometimes we're our own worst enemy, like you said…Personal information you put about yourself on Facebook, half of it is enough to open an account somewhere." (LHE Cardiff)*
>
> *"It's amazing how freely we do actually give our information out." (LHE Cardiff)*

However, the public's lack of awareness was blamed on the government. It was suggested that children should be educated about data, its value, and the importance of protecting it.

Despite their concerns about the security of their data, there was acceptance that data cannot be kept 100% secure:

> *"The possibility is there so we cannot, whatever we say we cannot be 100% sure that it is secure." (LHE Manchester)*
>
> *"The reality is that there is no foolproof security for holding data." (MHE London)*

In addition to errors by computer systems, it was also noted that data would always be vulnerable to human error:

> *"The information is only as good as the person who inputs it." (MHE Cardiff)*
>
> *"It really comes back to whatever type of system you have, however good, however secure, however encrypted, it's the human element that is the weakness, always." (LHE Cardiff)*

Some concerns about data security were related to the distrust of government employees. It was felt that personal data was valuable and open to exploitation. There was thought to be a possibility that the public's data would be sold without their knowledge:

> *"If they are not of an honest nature then there's a lot of money to be made isn't there, by obtaining a couple of customers' details in one day and selling it on." (LHE Cardiff)*
>
> *"I think it's impossible to think there's going to be foolproof security measure to hold everyone's data and think it's going to be safe and people are not going to exploit it in some manner." (MHE London)*

Interestingly, participants who worked for the government were sometimes wary about divulging too much about their experiences with personal data, recognising their responsibility to confidentiality:

> *"I can't say much because I've signed the Official Secrets Act." (LHE Manchester)*

Those who worked for the government, and worked with personal data, noted that steps had been taken to improve the security of data. For example, it was explained that they had attended mandatory data protection training courses. However, security was described as a 'moving target' as technology is constantly changing and being updated:

> *"Another facet to it probably is the technology by which you save that data, and that is a moving target." (MHE London)*
>
> *"Keeping ahead of the hackers though isn't it, it's almost impossible." (MHE Cardiff)*

7.2 Distrust of Government motives

It was evident that there was a strong distrust of the government. When discussing sources of data, the idea of the government spying or covertly gaining information was mentioned. It was thought that the government was not completely honest about what data it collected and how the data was used, and it was felt that 'they know more than we think':

> *"I'm sure there's a hell of a lot of information that we don't know they've got and we will never find out they've got." (LHE Manchester)*

7.2.1 Selling personal data

In addition to the idea that individual government employees may sell the public's data, reference was also made to government departments selling this type of information as standard practice. This was not thought to be acceptable and was concerning for participants:

> *"I don't agree with the government passing information to commercial concerns basically. I mean I'm sure the government are making money out of selling that information which is our information." (LHE Manchester)*
>
> *"They've got my name and address from the DVLA, and how can the DVLA just give out my information like that." (LHE Manchester)*

Reference was made to the electoral register and how this could be sold to commercial organisations. Concern was expressed regarding the idea of commercial organisations accessing government databases:

> *"I'd be very wary about private companies being able to access government databases." (MHE Manchester)*

7.2.2 Suspicion of Government covert use of data

It was suspected that the public could be 'tracked' by the government, and that individuals could be monitored if the government chose to:

> *"Listening to your phone calls, which they do anyway. Every text message. Because it all goes through satellites, who owns the satellites, the government, so boom, everything you say or text is, in theory can be pulled up." (LHE Manchester)*

When discussing the idea of a central database, there was also suspicion that the full, and true, purpose of the database had not been disclosed by the focus group moderators. It was recognised that this database would be used for statistics, but there was concern that this was a 'cover' for another purpose:

> *"Of course you're saying that it's for statistics, but how do we know?" (LHE Manchester)*

7.2.3 Trust in Government motives

However, as well as the mistrust previously reported there was some indication of trust in the government. It was felt that the government would do what they can to keep data safe, although it was also suggested that this trust could be naïve:

> *"I'm quite happy for the government to hold personal information because I'm quite confident that the government will do all they can to keep that personal information safe." (LHE Manchester)*
>
> *"I can't really think of much or like many instances where I wouldn't be that happy between government agencies sharing information, because as far as I'd be aware, I don't know if it's naïve, you could trust the agencies." (MHE Manchester)*

There was also a suggestion of more trust in the government that in commercial organisations, but again recognised that this may be naïve:

> *"Somehow I stupidly feel more safe if somebody's employed by the government and their salary is paid by the government, if they leave it on a train I'm less offended than if a private company which happens to be working for the government for the current financial year loses it, because they are not government employees, the same checks have not been made on them and so on. But, you know, I may be living in a fool's paradise." (MHE London)*

This trust in government to use and share their personal information was sometimes linked to the idea that participants had 'nothing to hide'. However, this implied that the government would use personal data to 'monitor' the actions of individual members of the public:

> *"I would trust them with my information, I've got nothing to hide." (MHE Manchester)*
>
> *"I don't feel like I'm doing anything that I could be caught out for." (LHE Manchester)*
>
> *"I'd be happy, as I say, because I'm honest, law-abiding citizen they can hold whatever information they want about me." (LHE Manchester)*

Consequently, there was a concern that the central database could be used in this way, and may result in false implication. It was felt that the database could be 'used against' them:

> *"I personally wouldn't want such a database. I'd feel uncomfortable knowing that this one place held all my data, that at some point it could be used against me." (LHE Manchester)*

> *"I've never committed a crime but again, it could be used to implicate me." (LHE Manchester)*

It was suggested that the government needs to gain the public's trust that their data is being used appropriately and is kept securely:

> *"You have to gain the public's confidence in the fact that you have it secured, that it is solid." (LHE London)*

7.3 Security concerns about the central database

When discussing the concept of a central database, the major concern associated with this idea was security. Discussions about the database consistently returned to the issue of how secure the database would be, and how security of data would be kept:

> *"If there was a central, you know, a big massive central database, even though I'm a little uneasy but if it was going to happen…you'd want there to be something quite substantial…there needs to be adequate protection and if they can't, it's not something you can just go in and do just off the bat." (MHE Manchester)*
>
> *"The overriding issue for me is always going to be the security of it in one place and how you lock it down." (MHE Manchester)*
>
> *"Security is the main thing." (LHE London)*

7.3.1 Disclosure control

Across the groups, the most worrying prospect was that identifiable data would be released. Even when it was understood that the database would only be used for statistical purposes, there was concern that these statistics, even though anonymous, could somehow disclose personalised data. It was feared that members of the public would be identified on the database:

> *"We don't want it identifiable." (LHE Manchester)*
>
> *"As long as it's generalised…where it's a group of people who aren't going to be identified then that's fine for statistics and getting, you know, producing the services that they need to in certain parts of the country." (MHE Cardiff)*

7.3.2 Items of data acceptable for inclusion on a central database

Generally, the basic demographic information provided to participants as an example of what would be held on the database (name, address, sex and date of birth) was thought to be acceptable. The uncertainty of what else might be added to the database was thought to be concerning. There was variation in the type of information that participants were comfortable with, and support for the idea of the database was linked to what it would contain, to a certain extent.

A lack of understanding of the use of statistics meant that the groups did not always understand why certain information was necessary. Those participants who were less statistically aware tended to be concerned about their name being on the database. It was not understood why this was necessary:

> *"If the idea then is just for statistical purposes why have a name on it." (LHE Cardiff)*

> *"I'd be quite happy for you to have all the information about me but not, as long as my name wasn't there." (LHE Manchester)*
>
> *"Why do they need your name if it's just for statistics?" (MHE Cardiff)*

These participants tended to be more comfortable with a number, such as an NHS number, rather than their name:

> *"You need something to identify you as you, and it could be XQ775, it doesn't have to be your name." (MHE Cardiff)*
>
> *"You have a national health number, your passport number, that's only available to you as one person…you don't need the name because you've got those numbers." (MHE Cardiff)*

However, those with more statistical knowledge were more concerned about unique identifiers:

> *"*[discussing National Insurance number] *It's too personal, no I wouldn't want it there." (MHE London)*

Participants were not overly concerned with the detail of what should and shouldn't be kept on a central database, and felt that their support for different types of data depended on the reason why that information was needed. Which information was added to the database, and which government departments had access to it, was thought to be entirely dependent on why that information was needed:

> *"There must be a why; why do they need the information, how are they going to use it and who is going to use it." (LHE Cardiff)*
>
> *"It's the access of need." (MHE Cardiff)*

There was a suggestion that a change in the law should be required to add extra information to the database, and that who had access to it should be determined by law:

> *"a legal framework as to who has access to it" (MHE London)*

Participants tended to mention data that might be deemed more sensitive such as criminal records, medical records, political affiliation, bank details, and sexual identity as data that they would not want to be shared between government departments, or in the public domain. There was a difficulty in understanding how these types of data related to statistics:

> *"It depends what other information they wanted to get. At the end of the day if it was just general trivial stuff then it's not too bad, but if they…wanted to access criminal records and things like that, then I don't think it's relevant." (LHE Cardiff)*

Their concern about these more sensitive types of data again linked back to the concern about disclosure.

7.3.3 Security implications of public data on one database

As discussed previously, it was felt that regardless of what security was put in place for the database, it would be open to abuse. There was scepticism that the database could be kept securely, and biometrics were seen as the only way of keeping the database safe:

> *"The only real secure way would be to like have, you have to go in personally and have the iris scanned or a fingerprint or something like that." (LHE Manchester)*

There was particular concern about individuals being able to 'hack' into the database:

> *"That wouldn't stop computer hackers from accessing all the data." (MHE Manchester)*
>
> *"People can hack into it, people can abuse it." (MHE London)*

Consequently, a major concern centred around the idea of 'all your eggs in one basket'. There were two opposing views. On the one hand, it was felt that data may be safer in one place. Before the idea of a central database was explained to participants, it was suggested that a single database may be more secure and efficient. However, this was related to a misconception that a central database would reduce the need for other government databases. There was an expectation that once a central database had been created, the other separate databases would, and should, be deleted. Generally, it was believed that storing data about every member of the population on one database posed a greater security risk:

> *"At least if you had different systems, if one system was compromised then the damage would be limited. I think that's the main problem with a central database is the security." (MHE Manchester)*
>
> *"More problems with things going wrong on a massive scale." (LHE London)*
>
> *"If there were just one database and someone did get into it they would then have access to everything, whereas at the moment, whilst, yeah, lots of little databases may not be a good thing, if someone hacks into your record at the DWP they won't be able to see your medical history." (MHE Manchester)*

In addition to security, there were also concerns that the creation of a central database may not be feasible:

> *"It's so enormous is it feasible?" (LHE Cardiff)*

7.3.4 Levels of access

The idea of 'levels of access' was raised in the all of the discussions. It was suggested that access to certain information by government officials could be restricted based on what the individual viewing the database needed to know. The idea of restricting access to data appeared to be reassuring:

> *"I've got full access to one section of their records and I know that there's another section of their records but I can't see that because I'm not allowed to, it's nothing to do with my job." (MHE Manchester)*
>
> *"Certain people should only be allowed to access certain parts." (MHE Manchester)*
>
> *"It's almost as if this central record would have a number of pages allowing different other departments to have access to different pages rather than access to the whole thing." (MHE Cardiff)*

> *"If we were to have everything under one roof…each person's information should have kind of security degrees or something from A, B, C, D, you know, and I can access, DVLA can only access A and B meaning where you live, what your name is, National Insurance, things like that…let's say you're the police you need more levels of access, so you get C,D and E." (LHE London)*

It was also felt that different levels of access to the central database would reassure the public:

> *"Let's say that this agency can only access these many pieces of information from the main system, which would give some assurance to the people." (MHE London)*

When discussing which government departments should or should not have access to a central database, individual government departments were rarely singled out. However, as previously mentioned, there was a concern about open access to the database. The most important issue was felt to be relevance, i.e. that government departments should only be able to view the information that they need to see:

> *"Work and Pensions wouldn't be able to see your medical records because it's got nothing to do with them, that kind of thing, you know, people only be able to see the bits that are relevant to them." (MHE Manchester)*

> *"I don't see why anyone randomly in Swansea using my driving licence can go and look up my criminal record just because they happen to work for the government, that's not right." (LHE London)*

> *"Would you say that somebody say for example in Cardiff City Council would need to have all the medical records? No, it's not necessary." (LHE Cardiff)*

There was also insistence that the database would not be sold to commercial organisations:

> *"As long as there wasn't any kind of…I wouldn't want any kind of commercial selling, as long as you know there's nothing going to the commercial sector, everything's going to be used in the right manner." (MHE Manchester)*

The participants themselves recognised the value of clearly communicating to the public the exact details of how the database would be used in order to alleviate concerns about security:

> *"It's about as much care being put into telling people how it's secure and who has access to it." (LHE London)*

In summary, it appeared that there was acceptance of the idea of the central database in general, but this acceptance was based on the condition that security was appropriate:

> *"A good idea, but with reservations." (MHE Manchester)*

> *"It's a good idea to have everything in one place, provided there is security." (MHE London)*

The most important issue was that identifiable information was separated from the statistics, and this would be a key point to communicate to the public:

> *"As long as the National Insurance number or national health number or anything that was related to an identifiable person could be kept, could be encrypted or kept separately then if it were useful for statistical use…I'd be happy about it." (MHE London)*

Towards the end of the discussions, it appeared that participants had a stronger grasp of statistics and a greater understanding of how they are used, and the benefits of the database:

> *"It builds a picture of who really lives in Britain. I think that's quite a good idea." (MHE Manchester)*
>
> *"It perhaps helps them decide where they need to spend their money." (MHE Manchester)*

"It gives me more confidence in knowing that the government's going to actually have something to base their decisions on." (MHE Manchester)

7.3.5 Weighing benefits of the database against the risk

There were high, sometimes misguided, expectations of how the database could help the public. There was an expectation that the database would directly benefit their lives. For example, it was felt that the database might be an efficient way of keeping the public's contact details up to date, or might help to tackle crime. These findings are similar to those found in the quantitative testing:

> *"Say instead of me having to inform the local council that I've moved and the NHS that I've moved, everyone just to be able to go and inform the information people…tell them and then you know that your record's updated." (MHE Manchester)*
>
> *"Might help against fraud and identity theft." (MHE Manchester)*

Where participants were positive about the idea of a central database, this was sometimes due to a misunderstanding of the purpose. For example, it was assumed that the database would be used for administrative purposes:

> *"I kind of think it's a great idea having a central database but what if I get my new passport and it comes with my middle name spelt incorrectly." (MHE Manchester)*
>
> *"In terms of kind of like efficiency and all our information being in one place, it would be ideal and it would help kind of maybe police, then you wouldn't hear things like Somerset Police couldn't do anything with Greater Manchester Police." (MHE Manchester)*

However, the true purpose of the database, to be used for statistical purposes, was recognised and accepted by the groups:

> *"I think it may help to make like economy planning, assuming the government would like to build hospitals, could use as statistics to see where it is necessary." (MHE London)*
>
> *"If it was just that information was gathered from other organisations for statistical purposes no problem." (LHE Manchester)*

Nevertheless, despite recognition of the purpose, it was sometimes difficult for the groups to see how this would result in a personal benefit to them. As discussed previously, a personal benefit was thought to be important. Other reasons that were given for the purpose of a central database mainly focussed around efficiency, for example saving time and money:

> *"For ease of sharing information." (MHE Manchester)*
>
> *"Cost savings." (MHE Cardiff)*

> *"There's no denying it's more efficient to do it this way." (MHE London)*

Despite recognising these benefits, it was difficult for participants to see past the risks associated with the database, especially those concerning security. The influence of the media, in particular their coverage of other high profile databases, also meant that there was scepticism that the government would have the ability to create and manage the central database:

> *"I've just seen what a mess you've made of it so far. Giving you it all in one place, you'll just mess it up big time." (LHE London)*

7.3.6 Concerns for the future

The focus groups took place five or six weeks before the general election. It is possible that the political climate at that time influenced participants' views and biased their discussions on how the database could change in the future. There was a concern that changes in government could affect the purpose of a central database:

> *"The government changes. Ten years', fifteen years' time." (LHE Manchester)*
>
> *"I think that so long as we are living in a liberal democracy, then one has fewer worries, but one never knows who is going to be in government in 10, 15, 20 years' time and so therefore whatever decisions you make you perhaps need to err on the side of caution." (MHE London)*
>
> *"It starts off like that but in ten years' time oh my God, what will they, you know, they'll have every single thing on us." (LHE Cardiff)*

Following on from this idea, participants were wary about the possibility of such a database being misused by a future government. There was concern about how a database containing personal data about everyone in the country, especially data such as ethnic group and religion, could be used in a discriminatory way:

> *"An unsavoury, in my opinion, political party having all kinds of information on all of us and possibly having biases towards persons of different ethnic communities and therefore making life difficult for particular groups." (MHE London)*
>
> *"What if a more right wing party got in and started excluding people based on the information that's held in this database. It's not out of the realms of possibility. It's a slippery slope." (LHE Manchester)*
>
> *"If I was a member of some ethnic minorities I would be worried about that, thinking that in a time in the future given a political party might get in control that wants to discriminate against different ethnic minorities, has now got this list of where they all live." (MHE Cardiff)*

Related to this point, the groups discussed whether the database would be voluntary or compulsory. It was felt that it should be voluntary and that there should be an option to 'opt-out', but it was assumed that it would be compulsory:

> *"If people don't want to do it it'll just end up being compulsory won't it, at the end of the day. They'll just threaten you. You don't do it we're going to fine you." (LHE Manchester)*

The potential for the database to be used for malicious reasons was a worrying prospect for participants, and affected their support for the database:

> *"I'm worried that having one big database is bringing us one step closer to ID cards." (MHE Manchester)*
>
> *"And then all your human rights are being infringed before you blink." (LHE Manchester)*
>
> *"It's a powerful tool that could easily be misused, and I don't think it's worth the risk." (LHE Manchester)*

Conversely, another point of view was that the register could be beneficial for certain sectors of society in terms of targeting funding:

> *"Or you could target positive funding at that area, at that area of need." (MHE Cardiff)*

These two different views are founded in whether participants understood the statistical use of personal data, or had misconceptions about the individual level use of this type of information. These views are also related to the groups' understanding of the independence of the agency that would be responsible for a central database.

Regarding who should 'own' the database, there were some suggestions that it should be the police, or an entirely new government department should own it. However, it was also stated that the ONS should own it as it was recognised that the ONS is independent:

> *"I think it's the Department of Statistics that should have this." (MHE London)*
>
> *"As long as the Office for National Statistics is independent of government manipulation or other party manipulation I'm happier that a statistical department holds this information rather than social services or health." (MHE London)*

As previously mentioned participants did not immediately think about the statistical aspects when discussing a central database, however, an exception to this tendency was spontaneous mention of how a central database would enable an '*electronic census anytime you want*' . Generally, though the notion that a database may replace the need for a census evolved later during consideration of various details and queries concerning the database and its potential uses for statistical purposes. During this more detailed discussion, the advantages of the database, in terms of more frequent, up to date data, became clear:

> *"It's out of date by the time it's done, yeah." (MHE Manchester)*
>
> *"It's every 10 years isn't it you do a census and presumably if you could access information that gave you instantaneous answers as to what's happened to the population growth or people moving or stuff like that then fine." (LHE London)*

However, there was a need to know what would happen to the database in the future. For example, it was queried whether the database would take on the role of the census and become a public record at a later date.

> *"Presumably this statistical database will provide a historical document of a snapshot in time." (LHE Cardiff)*

8 Next steps - implications for a central population database

The purpose of this research is to explore in more detail the issues raised in the quantitative research, and subsequently feed these findings into a communications strategy. Taking these findings into account, it is suggested that the following issues are considered when formulating such a strategy.

8.1 Direct communication with the public

In all of the groups, it was felt that there was a lack of communication from the government to the public. There was felt to be a lack of transparency regarding what data is held about individuals, what this data is used for, who it is shared with, and how securely it is kept. It was evident that participants were not content with this lack of communication, and wanted the government to interact with them and inform them of its behaviours, actions and decisions. Additionally, there was awareness of the spin of the media, but it was felt that the government should find a way to communicate positive messages to the public. It was suggested by participants themselves that positive publicity for the government might increase the public's confidence in its ability to store and use the public's data.

8.2 Education of the public

In order for the public to fully understand the purpose of a central population database, and how it could benefit them, the public needs to understand what statistics are and how they are used to make decisions. In all groups, there was an interest in statistics and eagerness to learn how they can benefit their situation. There was uncertainty regarding how a central database could benefit them, and it was also thought that the risks, in particular the security risks, may outweigh the benefits. Consequently it was felt to be important that the benefits of the database are communicated to them. It was also suggested that this would increase acceptance of the database. Therefore, consideration needs to be given to how the government can educate the public about the wider purpose of the central database, and therefore help to gain the public's acceptance.

8.3 Management of public expectations

There were sometimes high, but misguided, expectations about how the central database could benefit participants as individuals. For example, it was felt that the register could be used to solve crimes or make applications for services more efficient (for example, so that the same information does not need to be provided to several different government departments). These high expectations would need to be managed carefully. It would be crucial to publicise the exact, true purpose of the database, i.e. to only be used for statistical purposes. For example, if it is not the purpose of the database to solve crime or make the provision of services more efficient, then this needs to carefully communicated. It would be necessary to explain and highlight the benefits of a central database, but balance these against unrealistic expectations. Again, this links back to communication and educating the public about statistics and their benefits.

8.4 Addressing concerns regarding future uncertainty

Another issue raised was the public's distrust of the government. There was a suspicion that the purpose of the central database may change in the future, perhaps with a change of government. A potential change in the purpose of the database was linked to malicious or negative purposes. There was also concern about what information may be added to the database, and in turn how this could affect its purpose. Again, the exact reasons for the creation of the database would need to be communicated to the public carefully and effectively, and concrete reassurance would need to be given about the purpose of the database, and how static that purpose is. The independence of the Office for National Statistics, as the ‘owner’ of the database, would also be an important message to communicate. There was also a need to know whether the database would take on the role of the census, and become a public record at a later date.

8.5 Control

It was evident that there was a sense of vulnerability regarding the fact that there was little awareness of how the public’s personal data is held and used. There was a need to reclaim some of that control; participants wanted to be consulted and feel involved in the decisions that the government takes. They also wanted to be asked for their permission for the use of their data. Although this research can be considered a consultation in itself, it was clear that there was an expectation that the public would be consulted regarding future decisions taken by the government.

8.6 Security

The security of public data was a major concern raised in all groups. Participants were keen to know exactly how their data was stored, and the security measures that were in place to keep it safe and avoid disclosure of their information. Their acceptance of the database was based on the condition that the security measures in place were appropriate.

When educating the public about the central database, it would be important to make clear that in order to compile and maintain the database, personal level information would need to be stored on it, but that this would not be included in the statistical outputs. Explaining that there are disclosure controls in place to prevent even anonymised records being identifiable would also be crucial.

8.7 Government accountability

A wider implication that has emerged from this research concerns the issue of government accountability. Participants felt strongly about government accountability. It was felt that government departments were not seen to take responsibility for lapses of data security discussed in the media, and this angered participants. It was stated that the government would need to be accountable for the central population database, and take full responsibility for its security. The implication for these concerns again comes down to communication with the public.

9 Conclusion

The report has illustrated that participants did not have a thorough understanding of how their personal data is used by the government, and they did not get their information about this data from the government itself. Their opinions and views of the government were based on their own knowledge and experience. Where there were gaps in their knowledge, it appeared that this was filled by negative communications from the media. These findings have strong implications for how communication with the general public is managed by the government, especially because the risks associated with data handling were a reoccurring theme throughout all the discussions about holding, sharing and using data.

It was strongly felt that the government did not communicate with the general public about what data it holds and how it uses it. It was suggested that an honest, transparent, communicative approach would increase the public’s confidence in the government and its ability to use the public’s data appropriately. The government was perceived to be incompetent, and this idea was reinforced by the failure of other government databases that had been reported in the media. It was also felt that the government did not take its responsibility for the security of the public’s data seriously. There was a need for accountability and repercussions for those who lose data. It was evident that there was a need to regain some control over their data. It was felt that it was their ‘right’ to view their own information, and there was an expectation that the government would ask the public’s permission to access their data.

The groups raised strong concerns about the security of their personal data. Reassurance about the security of the public’s data is key, as the groups’ acceptance of the database was dependent on the security of the database. It was feared that the use of the database would lead to disclosure of identifiable data. Different levels of access, dependent on what is needed from the database and who is using it, were thought to be important, and reassuring. There were sometimes high, misguided expectations of how a central database would be used, and how it could benefit the public directly. These expectations would need to be managed carefully. There was also a need for reassurance about the future of such a database, the concern being that a change in government may change the purpose of the database, resulting in it potentially being used for malicious reasons.

Appendix A: Beyond 2011 Public User Consultation Focus Groups Script

Introduction

Firstly, thank you to all of you for coming along to this focus group discussion this evening; we really value your help and your input.

I'm … and this is …, and we work for the Office for National Statistics or ONS as it is also known. ONS is responsible for carrying out lots of different surveys, as well as the census every ten years, and producing statistics on topics like the economy, health, unemployment and so on.

We've asked you to come along to this focus group this evening because the Office for National Statistics is thinking about possible changes to the way that it collects and manages personal information about the population, but before it does this it wants to seek the views of the general public. So, we are holding these focus groups in order to hear your thoughts and opinions on how the government handles personal information; what you think happens at the moment to all of the information that is held by the government about you, and what you'd like to happen to the information that is held about you. Plus we'd also like to hear your thoughts on some ideas that the Office for National Statistics has for the future.

There is no fire alarm test planned for this evening, so if the alarms do go off then we'll need to evacuate, all you need to do is follow myself and ….

The focus group will last for approximately one and a half hours, so we are aiming to finish at about 8pm.

I'd like to encourage everyone to participate in the discussion. Please feel free to voice your opinions; there are no right or wrong answers to anything that we discuss today. You might have the same or different views to other people in the group, and we want to hear them all, but please remember to respect the views of others, even if you feel differently. Because we want everyone to talk openly and honestly, I will ask you to maintain the confidentiality within the group; that is what is said here tonight stays between you as the participants.

It is very important that we try to not talk over one another, as this makes it difficult to hear everyone's views. It's also important that we talk one at a time so that the recorder can pick up what people are saying.

We will be recording the discussions that we have this evening, as it makes it much easier for us rather than trying to write down everything that you say. Everything that we talk about will be kept confidential, and when we report our findings we never identify any one by name. Once the report has been produced the recording will be deleted. Is that ok with everyone (if there is any objection ask for an explanation and try to reassure)?

START RECORDING

Please can I ask everybody to switch their mobile phone off, or turn it to 'silent', for the duration of the session, so that we don't have any interruptions?

To start with, it would be good if we could all introduce ourselves to the group and tell us your first name and something about yourself. I'll start and then we'll go round the table, so…

A) Awareness of data sharing (approx 25 mins)

The purpose of this stage in the focus group is to determine what participants currently think happens to their data that is held by the government.

Start the discussion off by asking respondents to tell us what they understand 'personal information' to mean in this context, and the same for the term 'government' (note – we want respondents to explore 'government' in terms of services and government departments, rather than government in terms of politics). The assistant moderator will note down the examples that respondents give on flip chart paper. The moderator should acknowledge that the assistant is doing this just so that we can remember what was discussed later on. This will be used as a reference later in the group.

The discussion needs to cover:

- Examples of personal information (e.g. name, dob, address, ethnicity, NI number, passport number, health info, etc)
- Examples of government departments that hold personal information (e.g. HMRC, NHS, DWP, Job Centres, Passport Service, etc)
- What kinds of information these government departments hold
- How the government gets this information
- What the government uses personal information for
- Whether government departments can share information with each other
- Whether there are any rules concerning what can be shared and what can't
- What are their feelings/thoughts about the idea of sharing information
- Benefits (e.g. reducing government costs) and concerns (e.g. privacy, data security) about sharing information
- What sources of information respondents have based their opinions on
- How confident are they that their description of the current situation is accurate

B) Preferences for data sharing (approx 25 mins)

Now we know what respondents *think* happens to their data, the purpose of this stage in the focus group is to determine how they would *prefer* their data to be handled.

To encourage the discussion to move on to this section, could explain that they have been discussing what they believe happens to their personal information, now I would like to hear their thoughts on how they would like their personal information to be treated. Start off by recapping that they've talked about the idea of government departments sharing people's personal information with each other, now talk about the reasons why government departments might want to do this.

The discussion needs to cover:

- Reasons why government wants to share information (e.g. statistics, to keep track of people, to tackle terrorism, to reduce government costs, to reduce identity/benefit fraud, etc)
- What type of information is ok to share, what isn't ok to share (remind respondents of flip chart list if necessary)
- Which government departments should be able to share information, which shouldn't (remind respondents of flip chart list if necessary)
- Respondents' reasons for their preferences
- Feelings/thoughts about sharing personal information between government departments (in relation to the specific examples they discuss)
- Benefits/concerns about sharing personal information between government departments (in relation to the specific examples they discuss)

- Do feelings/thoughts/benefits/concerns about information sharing change depending on how information will be used (e.g. for statistical or administrative purposes)

C) Views on a single population database (approx 30 mins)

We now know how respondents think their data is handled, and how they would prefer their data to be handled. The aim of the final part of the focus group is to explore their thoughts on the idea of a single population database.

To encourage the discussion to move on to this section, could say that they have talked about what they believe happens to their personal information, and how they would like it to be handled, but now I would like to hear their thoughts about some ideas that the government has about how it holds people's personal information. Start with scenario:

Now I'd like to explain an idea that the government has about how it holds people's personal information, and then I'd like to hear your thoughts about this idea. The idea is that the government could create one register which contains personal information about everyone in the UK. The plan is that one government department could speak to other government departments, ask them for information that they hold, and use this information to make one big register.

Then, the discussion needs to cover:

- Reasons why the government would want to create a single population register
- Respondents' level of support for a population register
- Feelings/thoughts about one central register
- Benefits/concerns about one central register
- What personal information is ok to go on the register, what information isn't (remind respondents of flip chart list if necessary)
- Which government departments should be able to contribute to the register, which shouldn't (remind respondents of flip chart list if necessary)
- Who should be allowed to use it and why
- Respondents' reasons for their views

Then introduce more specific scenario, which gives respondents more detail about the register:

Now, I'll give you a more specific example to think about. Imagine that the ONS wants to create a register of everyone who lives in the UK. The aim of the register is to help produce better statistics which will mean that money can be better allocated to places like schools and hospitals. The information on the register will not be used for any other purpose and will be kept under strict confidentiality rules. This register will start off containing people's name, address, sex and date of birth. Over time, other information will be added to it. The ONS would need to get people's name, address, sex and date of birth from other government departments. For example, they could create this register by looking at the NHS' patient register, by looking at people who receive benefits from DWP, and by looking at people who have a NI number from HMRC.

Then, the discussion needs to cover:

- Respondents' level of support for the register, in light of the specific information (e.g. the type of information that will definitely be on the register, how that information will be obtained and who from, that it will only be used for statistical purposes)
- What personal information is ok to go on the register, what information isn't (in light of the specific information) – if not already mentioned, probe around NI number, NHS patient number, health information, passport number, ethnicity, marital status, nationality, migration status, employment status, housing information

- Which government departments should be able to contribute to the register, which shouldn't (remind respondents of flip chart list if necessary) – prompt for HMRC, NHS, DWP, Job Centres, Passport Service if not already mentioned
- Who should be allowed to use this register and why
- Feelings/thoughts about this register
- Benefits/concerns about this register
- Burden – the potential for this register to replace/reduce questions on surveys
- Respondents' reasons for their views

Final 5 minutes
Assistant moderator to provide brief (couple of minutes) summary, then ask if anything has been missed.
Thank you for your participation. It's been a very interesting discussion and you've provided us with lots of valuable information which will be really useful to the project.

Glossary

Abbreviation	Meaning
DCMCS	Data Collection Methodology
LHE	Less highly educated
MHE	More highly educated

References

Ritchie J, Lewis J. (2003). ‘Qualitative Research Practice: A Guide for Social Science Students and Researchers’. SAGE publications.

Social Survey Division, Office for National Statistics (2009). ‘Data sharing between Government Departments: Report on public acceptability’. Published online: http://www.ons.gov.uk/about-statistics/methodology-and-quality/imps/beyond-2011/data-sharing-between-government-departments---report-on-public-acceptability.pdf