The future of privacy

Volume 2
Public trust and the use of private information

Perri 6
with
Kristen Lasky and Adrian Fletcher

DEMOS

DEMOS

Open access. Some rights reserved.

As the publisher of this work, Demos has an open access policy which enables anyone to access our content electronically without charge.

We want to encourage the circulation of our work as widely as possible without affecting the ownership of the copyright, which remains with the copyright holder.

Users are welcome to download, save, perform or distribute this work electronically or in any other format, including in foreign language translation without written permission subject to the conditions set out in the Demos open access licence which you can read here.

Please read and consider the full licence. The following are some of the conditions imposed by the licence:

- Demos and the author(s) are credited;
- The Demos website address (www.demos.co.uk) is published together with a copy of this policy statement in a prominent position;
- The text is not altered and is used in full (the use of extracts under existing fair usage rights is not affected by this condition);
- The work is not resold;
- A copy of the work or link to its use online is sent to the address below for our archive.

By downloading publications, you are confirming that you have read and accepted the terms of the Demos open access licence.

Copyright Department
Demos
Elizabeth House
39 York Road
London SE1 7NQ
United Kingdom

copyright@demos.co.uk

You are welcome to ask for permission to use this work for purposes other than those covered by the Demos open access licence.

creative commons

Demos gratefully acknowledges the work of Lawrence Lessig and Creative Commons which inspired our approach to copyright. The Demos circulation licence is adapted from the 'attribution/no derivatives/non-commercial' version of the Creative Commons licence.

To find out more about Creative Commons licences go to www.creativecommons.org

Demos

Demos is an independent think-tank committed to radical thinking on the long-term problems facing the UK and other advanced industrial societies.

It aims to develop ideas – both theoretical and practical – to help shape the politics of the twenty first century, and to improve the breadth and quality of political debate.

Demos publishes books and a regular journal and undertakes substantial empirical and policy oriented research projects. Demos is a registered charity.

In all its work Demos brings together people from a wide range of backgrounds in business, academia, government, the voluntary sector and the media to share and cross-fertilise ideas and experiences.

For further information and
subscription details please contact:

Demos
9 Bridewell Place
London EC4V 6AP

Telephone: 0171 353 4479
Facsimile: 0171 353 4481
email: mail@demos.co.uk
web site: mail@demos.co.uk

Other related publications by Demos:

On the Cards: Privacy, identity and trust in the age of smart technologies

Democracy in the Digital Age

Access Denied? Preventing information exclusion

NetState: Creating electronic government

First published in 1998

by Demos
9 Bridewell Place
London EC4V 6AP

Telephone: 0171 353 4479
Facsimile: 0171 353 4481
email: mail@demos.co.uk

ISBN 1 898309 49 3

Printed in Great Britain by Redwood Books
Design by Lindsay Nash

Contents

Appendices

List of figures

Data tables for Figures 14–29

Percentage tests on the key hypothesis: examples of cross-tabulations on consistent trusters for the particular organisations

Maximum likelihood test

Characteristics of experience and reputation based trusters, and institutionally based trusters: examples of regression analyses

High and low ranking trusters: examples of regression analyses

Preface and acknowledgements

This report is the companion to *The future of privacy, Volume 1* by Perri 6, also published by Demos. Volume 1 provides a detailed discussion of what will shape the future possibilities for securing privacy in a global society, the behaviour, thoughts, interests, preferences and contacts of each of whose members that is becoming steadily more systematically subject to digital recording. It develops some scenarios for the future of privacy over the next decade or so and makes some detailed policy recommendations.

The purpose of this volume is to examine in detail just one of the key shaping forces in the privacy debate – namely, the extent to which the public trusts organisations in the private and public sectors to handle personal information in ways that they consider respect their privacy.

This volume reports for the first time the findings of a survey of a representative sample of the population during early June 1997, interpreted in the light of a series of focus groups conducted in different parts of the country during March 1997, but it also draws on previous research to set these findings in context.

The report has been written by Perri 6, who directed the project, oversaw the design of the instrumentation for the focus groups and the survey and directed the specific data analyses conducted on the survey data, and selected the particular analyses for inclusion in this report. Adrian Fletcher conducted the focus groups and prepared a detailed report of findings, on which Chapter 2 is based and he worked

with Perri 6 on the design of the survey instrumentation. Kristen Lasky conducted statistical analyses of the survey data. Ben Jupp and George Lawson of Demos and Charles Raab of the University of Edinburgh assisted Adrian Fletcher in the moderation of a focus group. Additional research for Volume 1 which is drawn on here was conducted by Rachel Jupp and Danny Kruger. (There were many other research activities including extensive programmes of interviews and literature reviews and scenario building exercises for the whole programme of research on privacy, of which this book presents just one part: these are described in Volume 1).

We gratefully acknowledge the financial support of the Economic and Social Research Council (ESRC research project grant no R000221949).

We are grateful to Stephen Welch and Scott Wallace of MORI Omnibus for commenting on draft survey instruments, managing the administration of the questions during the MORI Omnibus survey, producing a report detailing summary statistics and percentages, supplying us with the raw data for our own analyses, and to Stephen Welch for detailed comments on an earlier draft of this report. Janet Dewes of MORI Field & Tab managed the recruitment of the participants in the focus groups according to our criteria and arranged venues for the group sessions to be held.

The project advisory group provided invaluable guidance, support and comment on draft instrumentation and interim reports. They were Anne Hinde of the Office of the Data Protection Registrar, Alan Hedges, Charles Raab of the University of Edinburgh and Melanie Howard of the Future Foundation.

A number of other people have provided important comments and suggestions, reservations, questions and encouragement including Francis Aldhouse, Geoff Mulgan, Ben Jupp, Tom Bentley, Mark Leonard, Orit Azaz and Sarah Tanburn.

None of these individuals can be held responsible for our opinions, errors or conclusions. Consistent with the principle of respecting privacy, we have taken care not to identify the sources of any of our focus group participants, survey respondents or expert interviewees.

Summary

This book is about what we, the British public, think about the ways in which large organisations in the public and private sectors handle information about us. Many business people and technologists hold the view that privacy is an irrelevance to customers, a cost burden on business and systems design, and probably in historical decline as a result of business and technological pressures. Only the sphere of government is believed to present privacy risks that business cannot.

The findings of the research reported in this book suggest very strongly that the British public does not share this view. Not that the public wants privacy above all else, or wants elaborate and bureaucratic machinery to protect privacy at the expense of other values. Rather, the public makes relatively sophisticated and discriminating judgements about the privacy risks that different kinds of organisations and their activities present. Understanding these complex judgements will be crucial for business strategists, government policy makers and designers of information and communication systems.

Recent surveys and qualitative work by other researchers suggest the following general picture of public attitudes. Privacy is important to the public but it is often a latent concern: the more people learn about information risks, the more concerned they become. Within the population it is now conventional to distinguish four groups:

- privacy fatalists, who believe that there is little that they or anyone else can do to ensure proper use of personal information
- privacy unconcerned, who are content that any person or organisation may collect information about them and see only benefits rather than risks in this
- privacy fundamentalists, who are very reluctant to provide personal information and believe that there are high risks that it will be used unfairly to disadvantage them
- privacy pragmatists, who are prepared to provide personal information to organisations in return for enhancements of service or other benefits.

Of these, the pragmatists form the largest group, although fatalistic attitudes are widespread. It may be that these are not fixed positions but a repertoire that most of us possess and from which we make choices in each context and case. While a majority of the population is aware, when prompted, of the existence of data protection laws and the Data Protection Registrar, many have fears about the costs, difficulty and efficacy of using these enforcement strategies.

Some kinds of information are more sensitive than others and – happily for many businesses – some of the most commercially valuable information is not widely regarded as sensitive. Financial details are among the most sensitive, followed by politics and religion, but newspaper reading and a number of other consumption activities are not regarded as sensitive by many people.

A large majority of the public trusts family doctors and NHS, followed by banks. Direct marketing companies do not score so poorly as the level of complaint about 'junk mail' might suggest. The least trusted with personal information are car manufacturers, newspapers and magazines, home shopping companies and cable television firms, suggesting that those making the most use of direct marketing into the home are among the least trusted. In the public sector, the Inland Revenue and the police attract much lower levels of trust than the NHS.

Before the present research, we knew very little about why these organisations are trusted or what exactly they are trusted to do or not to do with personal information. The aim of the qualitative work and the survey was to explore this question.

The main findings of the Demos survey, as interpreted using our qualitative work, are the following:

1. The existence of legal duties is prized by the largest majority of the public as the principle reason for trust, even though it is seen as difficult to enforce and use: reputation comes second, followed closely by staff reliability.
2. The public feels, with some regret, that along with personalised services comes a great deal of contact by mail or phone that is seen as unnecessary.
3. Citizens are as concerned with privacy risks concerning the private sector as they are with those concerning the public sector: there are quite reputable commercial bodies that, when we examine why people trust them and what they trust them to do, enjoy much more fragile and provisional trust than many councils or central government agencies.
4. The public is concerned about the levels of data sharing in the public sector.
5. One of the most important fears the public has about handling of personal data is that incorrect judgements will be made by inference from data held, leading to unjust treatment: this is probably a much greater concern now than simply worrying about how much is known about us.
6. Although many people regarded bank staff as reliable with personal information, surprisingly few people were prepared to say that having no problems with banks' handling of personal information was an important factor in trust. This suggests that even banks, which are among the most trusted bodies with security, accuracy and non-disclosure of personal information, do not enjoy full public confidence.

7. Supermarkets do not attract high levels of trust, suggesting that their information ethics for the use of data collected via their high profile loyalty card schemes have yet to convince the public.
8. Past experience of reliable performance, and a good reputation built up from the experience of others, are the reasons most likely to convince people to place high levels of trust in organisations to handle their personal information. This is much more important than the law (which most people felt was in practice all they had to rely on), specific warranties or public statements.
9. Ranked according to trust in personal information handling, the five types of organisations run as follows (starting with the most trusted): banks, central government agencies, local councils, phone companies, supermarkets.
10. In the case of local councils, there is some evidence that the people most likely to use their services are most likely to place high levels of trust in their personal information handling, but this could be the effect of a psychological process by which people persuade themselves that bodies they have to use are reliable.
11. Younger and more affluent people are slightly more likely to place high levels of trust in commercial organisations.
12. The best predictors of placing high levels of trust in an organisation's handling of personal information are: believing information to be kept securely; believing the staff to be reliable with information; believing that the organisation is law-abiding; using information only for the purposes notified and personalising services.
13. Older and better educated people are less likely to place high levels of trust in organisations to handle personal information properly, suggesting that increasing understanding encourages scepticism rather than confidence.

For market researchers trying to understand trust in their organisation the implications of these findings are:

- 'Privacy pragmatism' is easy to misinterpret: personalisation of service does not cancel out concern about privacy risks.
- When trust is understood correctly, 'fundamentalism' may be a smaller problem than it appears.
- But the 'unconcerned' may often turn out to be fatalists.
- The conventional segmentation is too coarse to be used on its own.

For business strategists trying to increase the public's confidence in their organisation's handling of personal information, the key questions to ask about the organisation's practices, procedures and strategy are the following:

Experience

- How can clients gain access to what is held about them?
- How can they see and feel the security, the commitment to accuracy, the minimisation of risks of unjust inference?
- How can they recognise that disclosure is not taking place?

Reputation

- How and where does word spread about good practice?
- How are scandals and mistakes responded to? What redress is offered?
- What public commitments to respect for privacy can the organisation make?

Reliable staff

- How are staff trained in handling personal information and accessing it when in front of clients?
- What codes of ethics, confidentiality and accountability to clients and what organisational procedures are staff expected publicly to sign up for?

In general, the public is more sophisticated and discriminating about the reasons they trust organisations and tasks which they entrust them to do than many professionals have believed. The widespread complacency in business and technology circles about privacy is misplaced. Public mistrust has long-run costs for organisations. In an age when personal information is the basic fuel of the information economy, privacy can never be a 'non-issue'.

Introduction

The views of the elite and the public

> Battles over privacy will be to the first decade of the new century what struggles over working conditions were in the second half of the nineteenth century. (Technology journalist, August 1997[1])
>
> Privacy is a non-issue. Consumers just don't seem to be interested in it. If there is an issue for business, then encryption technology will solve it. (Business journalist, August 1997)

Made within a few days of one another in telephone interviews during our research, these two remarks crystallise the extraordinary range of views held by experts on what the public thinks about privacy and what implications it could have. Indeed, we were interviewing them precisely because they are both experts. Such polarised views have been put to us throughout our research on privacy issues. Both cannot be right. In fact, in this introduction, we argue that they are both wrong, but nevertheless there is a germ of something very important in both views which can be synthesised and which the research reported here can help to illuminate.

Whether or not either of these experts are right, their views may well be typical of very different groups within the population as a whole.

Certainly, this polarity between alarm and complacency – to describe each position in the words of its opponents – about privacy is widespread in the expert communities in business, technology, government and social movement circles which concern themselves with privacy.

In at least one respect, the claim that privacy is a non-issue seems to have been comprehensively disproved during the period which we have been researching it. Throughout the years since 1996, when we began this research, the broadsheet newspapers have regularly carried stories on the front pages or in the home news sections about press intrusiveness and the question of regulation, the public disclosure of the names of convicted paedophiles, the use of genetic information in life insurance and the pervasiveness of closed circuit television cameras in shopping areas and residential estates.

Meanwhile, the business and international pages of the same newspapers have been reporting both the previous Conservative and now the Labour government's proposals on the regulation of cryptography, the Labour government's data protection reforms and President Clinton's initiative to have privacy concerns taken up in the course of negotiations at the World Trade Organisation to generate greater international electronic trade. Back in 1995, the Conservative government's proposals for identity cards created some acrimonious arguments over privacy and civil liberties. And in just one week in February 1998, the main stories in the British broadsheets were preoccupied, apart from international crises, with press privacy debates, including alleged ministerial misdemeanours, splits in the Cabinet on press privacy regulation, government amendments brought forward to the legislation on the European Convention to entrench the role of the Press Complaints Commission and the Department of Trade and Industry's new cryptography proposals.

In what are sometimes called 'specialist' communities, but which, taken together, involve millions of people, privacy is one of the central topics of concern. Internet users, a growing proportion of the population, probably put up more web pages, run more electronic discussions and send more protest e-mail about privacy than almost any other subject. In health care, the debates between the medical professionals,

the government and the insurers about the privacy of patient records are the subject of three major enquiries in Britain alone, and of recent legislation and proposed legislation in the United States. Debates about road pricing using smart cards which are read remotely from overhead gantries, about caller identification in telephone calling, about direct marketing from junk mail to cold calling, about the use of census data and other research, about the rights of law enforcement agencies in liberal democracies, about the implications of the coming of 'information warfare' in military strategy, about the basis of evidence on which social workers take children into care – all turn out to be about aspects of privacy.

The communities that care very passionately and actively on any side of these debates may be scattered and each of these communities may be relatively small. But taken together, they span so many of the daily concerns of millions that privacy surely cannot be a non-issue.

Certainly, if we take a longer time frame, privacy is a relatively new concern among the publics of Western societies. Most data protection laws, and most of the demand for them, date from the post-war era, culminating in a spate of legislation from the mid-1970s onwards. Certainly, the experts we cite at the beginning of this chapter are very well aware of the history, for it frames the ideological debates that lie behind claims of rights to privacy and the corresponding denials. If your general outlook is that the 1970s were the high water mark of regulation and that, from the mid-1980s, Western societies have made a decisive break with regulation, then you are more likely to see privacy as an atavistic demand for regulation which should to be resisted. If on the other hand, you see this history as the steady advance in business and government alike of new techniques for collecting and manipulating information about individuals, then you are more likely to see privacy as more fragile now than ever before and therefore of rising importance.

However, as these simple polarised views about regulation have begun to lose their credibility in the 1990s, so the balance of expert opinions about privacy has probably moved closer to the balance of public opinion. The *comprehensively* complacent and the alarmed today form relatively small proportions of both expert and public opinion.

The majority in both groups is pragmatically prepared to experiment with a little more or a little less privacy in different spheres of life.

So there are groups whom we might call *locally* alarmed and complacent about, say, cryptography or press intrusion, but who might take different positions about another privacy issue, depending on their interests, understanding, priorities, culture and situation. While a generation ago, such practices in managing one's opinions were often denounced as inconsistent and lacking in ideological fibre, today philosophers and intellectuals are more tolerant of the idea that one can legitimately take a different view of what is just or fair in different fields.[2]

For the majority, then, privacy is very important sometimes, but most people will make different trade-offs in what they regard as different circumstances. This enables us to re-read the comments of the two experts in a way that makes the conflict between them less polarised and more interesting.

In the second half of the nineteenth century, if one could speak of any single theme dominating politics and social life, it would have to be the conflicts that arose between employer and employee in the work place, and between organised capital and labour. Today, if we can speak of any single defining characteristic of our societies, it would not be unreasonable to stress the centrality of the collection and manipulation of personal information.[3] Databases of personal information in various forms are among the most important tools in these processes.[4] In the late nineteenth and early twentieth century, trade union activists and hard-liners in favour of redistribution and regulation were probably a minority of the population and most people made trade-offs with their employers as best they might. While the few who imagined the socialist state have occupied a disproportionate amount of space in the history books, the mass of the population might have hoped that technological advance and economic growth might ease the process of making one's trade-offs and reduce the necessity for conflict.

So it is with privacy concerns today. While a small proportion of activists for and against privacy legislation make headlines, most people hope that technological development and greater wealth will make the decisions they make daily about what information to disclose

either easier to bear or easier to implement securely. In part, both our experts cited above are right. Where they are probably wrong is either in imagining that privacy will lead to persistent and major social cleavage and conflict in the way that labour's conflicts with capital did, or in thinking that because this will not happen, privacy is of no importance. There will be not often be revolts on the streets about privacy but neither does it make sense to say that, because there will be little or no uproar, privacy is irrelevant.

The evidence we present in this volume about the shape of public opinion and the distribution of hard-liners, the complacent and the pragmatically but irregularly concerned, is all cross-sectional. That is to say, it describes a particular point in time. However, we know enough to be able to pick out certain trends and to make a convincing case about others.

One thing that does emerge clearly is that privacy is not going to become a non-issue. Another is that it is important to try to map the shades of grey and the fine judgements that people make. People do not make simple black and white choices to trust or not to trust organisations to use personal information about them, and then either grant them carte blanche or else avoid them altogether. Instead, most people trust some organisations to do or not do particular things but not for others, and their reasons vary. As a result, our behaviour will differ, not simply by using a service or not using it, but in the ways in which we use a service, what we reveal and what we do not, and on what terms we are prepared to reveal information about ourselves.

From our qualitative research, it is also clear that most people do, at least implicitly, make judgements about what scope they have to preserve their privacy and what effect each choice they make will have. Certainly, the faith we place in data protection laws, business ethics and the power of reputation is tempered with a sharp understanding of what is possible. But people are not powerless, at the mercy of commercial and governmental forces over which they have no control. There are things that one can do, in response to risks to one's privacy, to protect oneself, to make a sensible trade-off or to seek redress and, crucially, to handle oneself effectively in transactions where one is

expected to reveal a great deal of personal information. Awareness of these strategic choices is unevenly distributed across the population. However, it is clear from our research that the discrimination with which many people make decisions is finer than has emerged from some previous research.

And that, finally, is why public opinion on privacy matters. The legitimacy of what business and government do with what they know about us is not unquestioned and it rests on a series of trade-offs that we all make. The two expert views with which we began can both draw some support from the data. One points out that the glass is half empty, the other that it is half full. The point, as we document in some more detail in the second part of this volume, is that trust depends on what exactly organisations do and what reasons they can offer for being trusted. Organisations that do not appreciate the risks they run with public opinion will suffer, not necessarily in dramatic ways but in ways that will hurt sooner or later.

Structure of this volume

Part One of this volume sets out the background to our research.

Chapter 1 summarises the basis of previous research on which we have built. We begin by summarising key findings from the qualitative work and tracking surveys commissioned by the Office of the Data Protection Registrar during the 1980s and 1990s on public awareness of privacy risks and of the possibility of recourse to the law. We also pick out some of the principal findings from Alan Hedges' detailed qualitative study of public faith in confidentiality on behalf of the Department of Social Security, and from the qualitative work undertaken by Christine Hine, Steve Woolgar and others at Brunel University. We then compare the findings of the 1995 Henley Centre for Forecasting survey for the Dataculture report, the 1997 Future Foundation survey for the Direct Marketing Association and Informix for their report, *The new information trade.*

In Chapter 2, we set out the ways in which we built on these sources in the selection criteria for our focus groups and then summarise some

of the principal findings from our group sessions, using quotations as appropriate.

Chapter 3 presents the design principles for the survey. The approach is grounded in work on the concept of trust that Perri 6 began in 1994[5] and has used in other studies, such as one on the determinants of trust in a certain category of professionals.[6]

Part Two summarises the main findings of the survey. In Chapter 4, we present an overview of the principal findings.

Chapter 5 is concerned with the relationship between the questions, 'Why does someone trust an organisation with personal information?', or reasons, and 'What exactly does the person trust the organisation to do or not do with that information?', or tasks.

Chapter 6 sets out the findings of the survey on the relative rankings that people give each of the types of organisations on which the questions focused their attention, and explores the reasons why people rank organisations as they do.

In each of these data chapters, we present first the simple percentages before moving on to more complex analyses that attempt to explore socio-demographic characteristics of particular groups, and finally to multivariate analyses that seek, in the statistical sense, to explain why people report the views they do. More details on the data are provided for those interested in Appendix 3. As space does not permit us to print a comprehensive set of tables of all the analyses, we have selected some of the most striking and interesting ones to illustrate points made in the body of the text.

Chapter 7 concludes the report with some more extended data interpretation on the questions of how important privacy is to the British public and what exactly is important. We discuss the meaning of trust in this context, identifying some of the key drivers of change for the foreseeable future and, finally, drawing out some of the most important implications of these findings for strategists in business and government organisations.

This report should be read as a companion to Volume 1, where the role of public opinion is set in the wider context of the other forces operating in this field and which makes detailed policy recommendations.

Part 1
Background

1 Previous research

In this chapter, we summarise some of the most important findings from previous research on what the British public thinks, fears, worries about and has confidence in, in the field of privacy. This is vital because we have designed our research specifically to add to existing knowledge, to fill in gaps in the inheritance of material and to open up new territories for debate.

The chapter begins with a brief description of the main sources of data. The body of knowledge that can be drawn from them is then presented summarily, organised around the following themes: the priority the public attaches to privacy; the risks to privacy that the public perceive and worry about; public awareness of various different strategies for coping, protection and redress; the different degrees of sensitivity of different kinds of personal information and people's views about the trade-offs they make when they sacrifice privacy for some enhancement of service; the public's ranking of organisations that use personal data; and finally, the ways in which researchers have succeeded in segmenting the population by their different degrees or kinds of commitments to privacy.

The data sources

The findings from previous surveys, summarised below, are treated thematically rather than survey by survey, in order to build up the

picture of what is known. However, it is important to introduce the data sources on which we will principally draw. For simplicity's sake, each data source is given an abbreviation.

Track: The Office of the Data Protection Registrar commissions an annual tracking survey, findings from which are summarised in the Registrar's annual report.[7] The research includes a survey of businesses as well as of the general public. Every year, the public survey draws a representative sample of the population aged sixteen and over of about 1000 people for face-to-face interviews. The survey looks for awareness, both prompted and unprompted, of the existence and the content of data protection legislation, and the relative priority of privacy against other major social issues. The tracking survey also provides some information about public confidence in different kinds of public and private sector bodies' handling of personal information. Track data are taken from the *Thirteenth annual report of the Data Protection Registrar,* which runs up to 1996.

Dataculture:[8] In 1995, the Henley Centre for Forecasting conducted the Dataculture research jointly with the Direct Marketing Association and some of its leading members. This comprised qualitative focus groups with consumers, a face-to-face questionnaire survey of a representative sample of 1000 adults and a combination of depth interviews and surveys of businesses. The qualitative work and survey provide information on the relative rankings of types of information felt to be 'personal' or 'very personal' and what people are prepared to divulge in return for what kinds of improvements in service, the methods by which people are willing to provide information, awareness of different kinds of organisations' collection of information and happiness to provide information to them, concern about certain kinds of privacy risk and confidence that the law is complied with. A selection of these findings were used in a previous Demos study.[9]

NewInfoTrade:[10] In 1996, the Future Foundation conducted research which led to the 1997 publication, jointly with the Direct Marketing Association and Informix, *The new information trade.* The sampling

methodology for the Henley Dataculture research was repeated, although quite new questions were asked and new kinds of analyses conducted. NewInfoTrade developed the segmentation of the public suggested by Professor Alan Westin, the leading US theorist on privacy, in his analysis of a series of surveys conducted by the Louis Harris-Equifax organisation. That segmentation divides the population into privacy fundamentalists, privacy pragmatists and the unconcerned.[11] The Future Foundation analysed their data using a factor-cluster analysis to suggest a division of the pragmatists by greater presumption of confidence in the public and private sectors. Questions were asked about individual treatment offered and sought in return for the provision of personal information, awareness of data collections, views on so-called loyalty schemes, understanding of smart card technologies and data collection roles, views on electronic purse applications, degree of concern about data sharing, awareness of the legislation, preferred means of securing subject access and views on proposed national identity cards.

DMACensus:[12] Each year, the Direct Marketing Association produces its *Census,* which is in fact a compendium of research by the DMA Research Centre, commissioned research and data from other sources, now up to 1996. While much of the research is concerned with business attitudes and behaviour or else draws on Dataculture or NewInfoTrade, findings from the DMIS Direct Mail Trends survey of consumers are reported. This includes questions on awareness of consumer protection schemes, opt-out boxes, as well as data from other surveys on attitudes to 'junk' mail, contentment to access different services electronically and also some data on complaints about direct marketing practices.

Brunel:[13] Professor Steve Woolgar and his colleagues, Dr Christine Hine and Juliet Eve, at the Centre for Research into Innovation, Culture and Technology at Brunel University conducted a small-scale qualitative study during 1996 using snowball sampling techniques to recruit twenty six individuals for semi-structured depth interviews, quasi-ethnographic observation, use of a small number of shoppers' diaries and a series of small focus groups with between four and eight people,

using newspaper headlines as triggers for discussion. The focus groups were conducted with students, library staff, retail staff, a mother and baby group and a group of retired people. The aim of the Brunel research was to explore the experience of shopping and in particular people's feelings about privacy in such transactions. They also sought to understand people's feelings on the prospects for privacy in the context of electronic shopping and to explore how future trends, particularly in electronic shopping, might effect consumers' feelings and experience.

Hedges:[14] The Department of Social Security commissioned Alan Hedges to conduct a programme of qualitative research during November and December 1996, which involved eight focus group discussions with a total participant list of 69 people from 68 households in sixteen interview sessions, and eight unstructured depth interviews using only a loose topic guide and stimulus materials, in four areas of the country. The aim was to explore people's perceptions and beliefs about confidentiality practices with personal information held by DSS agencies, their views on what should happen and how different practices in respect of confidentiality might affect propensity to claim benefits.

Kable:[15] Of somewhat less direct use for our present purposes, but providing some additional background information, is a survey commissioned by Bull Information Systems from the public sector information technology consultancy, Kable, using BMRB during late February and early March 1997 to administer a questionnaire to a representative sample of 1000 people aged fifteen and over. The questions were mainly concerned with contentment with and willingness to use different technological media for interactions with government agencies such as payment, including the telephone, smart cards, a personal computer for Internet contact, paper mail or face-to-face contact. The data include some general findings on trust and distrust in public agencies, technologies and security of information.

POE:[16] This was a qualitative study undertaken in 1996–97 by Patterson, O'Malley and Evans of the Universities of Glamorgan, Cardiff and Bristol respectively, using six focus groups supplemented

with questionnaires administered to focus group participants in Windsor, Bristol and Cardiff stratified by age and social class. The study was concerned in particular with perceptions of privacy issues in connection with direct marketing and loyalty schemes. The key variables for analysis were perceptions of being in control of personal information, knowledge of database marketing practices and capacities, the sensitivity of certain kinds of information, the relevance of offers made in direct mail, views on organisations engaged in database marketing, intrusiveness, and confidentiality and accuracy.

Taken together these sources enable us to build an overview of the state of our understanding of public attitudes to privacy, prior to presenting the Demos research.

The priority of privacy

In very general terms, at least, when prompted to think about privacy as a set of risks that individuals face, the British public does think that its protection is very important, and more people seem to be taking this view. MORI's monthly unprompted question about the issues that people think are the most important for the nation does not yield a high rating for privacy. However, Track, using a prompted question that is more about what individuals are concerned about for themselves than for the nation, reports a statistically significant rise, between 1996 and 1997, from 63 per cent to 70 per cent of people agreeing that privacy is very important. The same study found an average ranking of privacy as joint third with unemployment, after crime prevention and improving educational standards (these other concerns are always among the top five in the MORI findings on issues of concern facing the nation). This represents an increment of one place over early 1990s results. However, privacy has consistently ranked above freedom of speech, inflation and equal rights for women or minorities as a public concern.

Hedges' qualitative study, by contrast, found that privacy concerns were a background worry, usually displaced by crime, unemployment and getting benefit entitlements, and brought to mind mainly in the context of receipt of junk mail and difficulties with a credit rating.

Privacy risks

The key privacy risks can be classified as follows:

- *injustice*, or the risk that, by collecting personal data or by linking two or more sets of personal information that were originally collected for very different purposes, incorrect inferences may be drawn and, in consequence, unjust decisions made about entitlement to service or treatment
- *collection of data without the consent of the subject* in contexts where there is no obvious reason (such as the need to levy mandatory taxation or subject firms to mandatory regulation) to set aside the need for consent
- *loss of transparency*, or the risk that personal information will be disclosed, exchanged and used in decisions about treatment or access to resources and services, where one does not know of the existence, content, accuracy or authority for collection and use of that information
- *function creep*, or the risk that data, having been collected for one purpose, will be used for other purposes, to which the subjects have not consented
- *excessive or unjustified surveillance*, or the capacity of business or government agencies to trace and profile one's behaviour, attitudes, communications, speech, networks and so on, when those organisations have neither a valid need nor a valid right to do so – such as being a police officer with a well-founded suspicion that one is involved in a crime or a loss adjuster assessing liability for damage where a claim has been made
- *loss of anonymity*, or the capacity of business or government agencies to connect information about behaviour or attitudes to one's true identity, when those organisations have no valid need or right to know one's true identity to carry out their legitimate activities
- *unnecessary or unjustified disclosure or disclosure without consent*, or the risk that organisations holding personal

information about one will disclose it to other agencies, either without one's consent or where consent is not actually required, in situations where it is neither necessary nor perhaps even appropriate, and perhaps where the other agency would use the information for quite a different purpose from that for which it was collected

- *reversal of the presumption of innocence*, or, where data matching is conducted in order to detect or minimise crime, non-entitlement, fraud, moral hazard or adverse selection, the risk that systems for handling personal data can readily become a means of using 'red alert characteristics' of individuals – ethnicity, use of cash where credit card would be expected, national origin, place of residence and the like– as the basis for 'categorical suspicion'; in other words, service or entitlement is denied, suspended or otherwise impaired on the basis of suspicion of abuse which is based on inferences that are very often incorrect from behaviour that can be undertaken quite innocently; this can have the effect of reversing the presumption of innocence until guilt is proven, leaving individuals in the position of having to prove a negative in order to secure entitlement or to avoid adverse treatment
- *loss of access to the means of protecting oneself from these risks*, such as the right to acquire and use strong cryptography and other security procedures, at least partially to protect confidentiality.

We can use this classification in exploring different public perceptions of different risks, and we shall return to this taxonomy when we come to explore the concept of tasks of trust in the presentation of the survey data.

Levels of general concern about the quantity and use of personal information held about individuals rose from 68 per cent in 1996 to 72 per cent in 1997, down from a high of 78 per cent in 1994 (Track).

Hedges found that the main risks which concerned people were a) a violation of confidentiality by disclosures in a climate of what is perceived to be an ever greater flow of data and b) a shift in the balance of power between individuals and large organisations that hold and use personal data. He argued that people want a kind of box to be built around the particular transaction for the purpose of which data is collected, and for it to remain within the box unless it could be shown that someone outside the box needed to know. In that case, only that which was absolutely necessary should be disclosed, the scale should be limited, controlled by appropriate procedures, notified to the data subject and, in the case of sensitive information, cleared with that subject. Most participants recognised some conflict between efficiency and confidentiality and were prepared to see some trade-offs, but they would not want to see efficiency considerations generally trump those of confidentiality. General fishing expeditions, unprompted by any particular transaction or evidence of an individual case of fraud, were regarded with particular abhorrence. Reliability concerns about the extent to which information was accurate and up-to-date were widely raised.

In particular, Hedges found strong concern that the DSS should not share information with commercial bodies or charities. People thought information should be shared with the police or the Inland Revenue only in the rarest cases of clear evidence of criminal misbehaviour, and with councils only in respect of linkages with Housing Benefit entitlements. Many would want selective controls on sharing even among DSS agencies, particularly in respect of the Child Support Agency. The circumstances under which he found more support than opposition for data sharing were to protect children at risk, confirm a National Insurance number, to help the MOD to find service personnel who have gone AWOL, to help the parents of a seventeen year old runaway girl to find her and rescue her from London's Kings Cross area, to track fine defaulters, to alert the police about a drug dealer and to alert someone that they were the beneficiary of a will. However, Hedges also found a widespread belief that all government databases are already somehow linked.

Similar perceptions emerge from POE, which found that, while people wanted control over the disclosure of information, many felt that automatic data collection and re-sale were now very widespread and that some effort would be required to remove oneself or any particular detail from a database.

Dataculture found that 54 per cent took the view that giving personal information to companies is a necessary evil, which rose to nearly 60 per cent among 45 to 74 year olds and in socioeconomic class D, but fell as low as 41 per cent among eighteen to 24 year olds. Eighty three per cent saw the provision of personal information to banks and other financial services companies as something in which they had no choice if they wanted a service at all. Significiant majorities in all age groups, rising to four fifths among 45 to 59 year olds and ABC1s, agreed that the even if they did not provide information, companies would find out information about them without their knowledge. Eighty five per cent recognised the telephone directory as a source and 72 per cent knew that the electoral register was available to companies; only 27 per cent understood that guarantee cards were a source, although 40 per cent acknowledged the role of buying consumer lists.

Dataculture studied four categories of risk: exclusion from services, inaccuracy of records, passing on information and fears associated with technology. Older people, people on low incomes and with low occupational status are most likely to dislike being profiled and 'pigeon-holed'. Thirty nine per cent were worried that providing personal information to a company could affect the way they would be treated and, in this case, younger people were more likely to be concerned than older people. Eighty nine per cent were concerned about inaccuracy. In qualitative work, however, correct spelling of name and address appeared particularly important, suggesting that respect and courtesy are almost as important in this regard as risks of unfairness in providing services. Seventy one per cent considered selling customer lists to be unethical and 87 per cent believed that companies should not be permitted to disclose information to other companies, although 40 per cent knew that it was a major source of personal information. The most common risk perceived from disclosure was unsolicited junk mail.

It is clearly very difficult to interpret measures of public concerns about unjust inference, because questions can be leading, because people are likely to think any adverse treatment of themselves to be unjust and because the greater salience of the risk may lead people to exaggerate its probability. However, Dataculture did ask people about whether they feared adverse treatment (which might reflect either fair or unfair decisions) from information held about them. Figure 1 below shows that the variation in the perception by age or by class is not very great.

NewInfoTrade found that 62 per cent would not be happy if companies joined together to share information, while 23 per cent would be prepared to consider this on a case-by-case basis.

NewInfoTrade asked people's views on a national identity card scheme and found 63 per cent content, 18 per cent resigned to it as an inevitable evil, 15 per cent not happy and 4 per cent unsure. Older people were more likely to be content. Those opposed were not necessarily

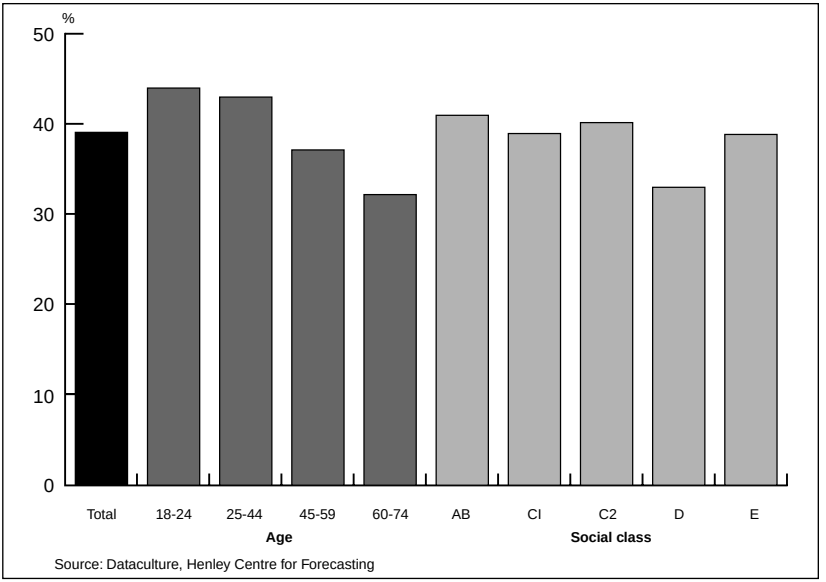

Figure 1 Fear of adverse treatment resulting from personal information held.

fundamentalists on privacy issues in general. The main benefits perceived were to do with law enforcement – cutting crime, helping the police, reducing fraud. A MORI survey in 1995 found a full 75 per cent content with an identity card scheme. However, Kable found that only 1 per cent would choose to use an identity card to identify themselves rather than any other currently available mechanism. But if there were to be such a scheme, Kable found 29 per cent would like it to be a smart card.

Kable asked people what would make them resistant to dealing with government electronically. Taste for traditional technologies and lack of access to new ones were the most important reasons, but 21 per cent reported a distrust of government and just 1 per cent pointed to concerns about data security.

DMACensus cites a Brann/Henley Centre survey on charities' loyalty schemes which finds that while most people are unhappy about disclosure even by charities, nevertheless younger people are happier for charities to pass on details than other kinds of organisations, at least to other charities.

Strategies for coping, protection and redress

Track found that two thirds of the population was aware, on prompting or semi-prompting, of the existence of the Data Protection Act 1984; this was pushed up slightly to 72 per cent immediately after an advertising campaign run by the Office of the Data Protection Registrar. Awareness among ABC1s of the existence of the Registrar is over 50 per cent and awareness of the Act reaches 84 per cent among ABs and 82 per cent among 45 to 64 year olds. Figure 2 shows the trends over time.

This is broadly in line with Dataculture, which found 60 per cent aware of the Act in 1995. Drawing on the DMIS Direct Mail Trends Survey, NewInfoTrade reported that awareness of the Act plateaued in 1993 after rising steadily and dipped by 1995.

Unprompted understanding of the Act's provisions is much more limited. Track found that 22 per cent were able to say that it protects rights about what information can be kept about individuals. Awareness

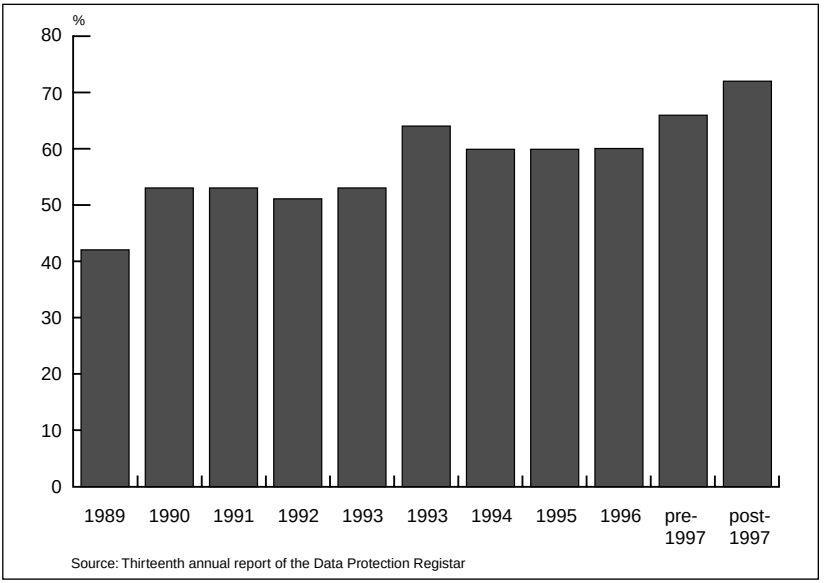

Figure 2 Semi-prompted and unprompted awareness of either the Data Protection Act or the Registrar.

of subject access rights has increased from 14 per cent in 1996 to 21 per cent in 1997. Thirteen per cent mentioned confidentiality (duties not to disclose to third parties) and just 5 per cent were aware of firms' duties to register. When prompted, 69 per cent were aware of subject access or rights to correct errors and 50 per cent of duties not to disclose, all increases on the previous year. Over 60 per cent believed there was something they could do about computer mistakes.

Dataculture paints a more pessimistic picture of understanding. Fifty three per cent did not know who was responsible for regulation, 15 per cent managed to come up with 'the government', 13 per cent thought no one was, while just 11 per cent managed, without prompting, to mention the Data Protection Act, although 49 per cent could do so on prompting.

The survey found that most consumers believe that significant proportions of companies do not comply with the legislation. Estimates of

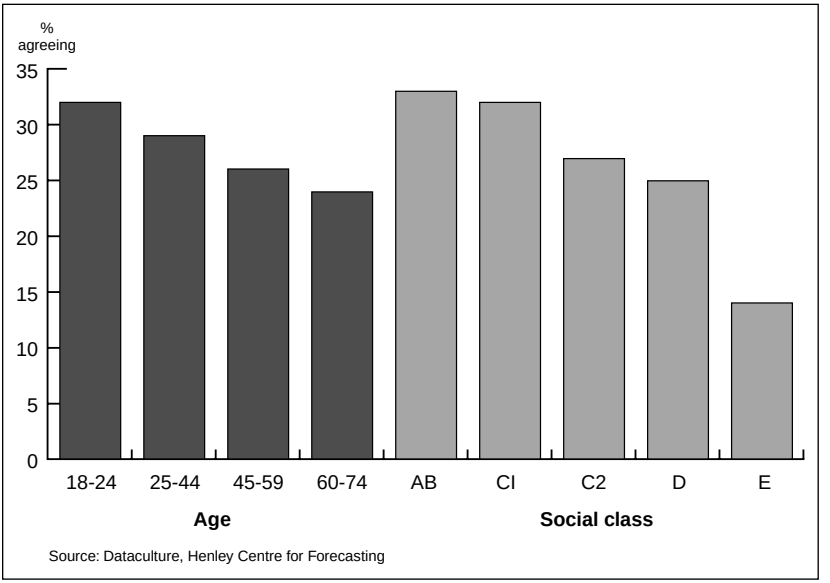

Figure 3 Confidence in compliance with data protection law.

the proportion of companies complying ranged from 1 per cent thinking all did, through 27 per cent thinking most did, 32 per cent thinking some did, 23 per cent believing very few did and 4 per cent believing that none of them do. Figure 3 shows the breakdown by age and class.

Hedges found knowledge of the Act to be patchy and poor, and many had doubts about the likelihood of effective exercise of rights of subject access.

Brunel found that few of their interviewees mentioned the legislation; still fewer understood its provisions or felt that it protected their interests.

POE did not ask about the legislation; it did ask about awareness of opting out, which was found to be common but something in which often rather little faith was placed as an effective guarantee of removal of an entry or prevention of unsolicited direct mail. Some participants reported providing false information on occasions as a strategy for

avoiding dataveillance, although they acknowledged that this might create problems in subsequent transactions.

NewInfoTrade found that 95 per cent of the sample thought that consumers would need new protections as companies collected ever more personal information and 90 per cent wanted this to take the form of new tougher legislation.

Dataculture provides some information on awareness of ordinary coping strategies. Three quarters of the sample were aware of opt-out boxes on questionnaires and coupons, although this was markedly higher among ABC1s. An earlier Henley report, *Teleculture 2000,*[17] found 90 per cent in 1994 and 1995 wanting the opportunity to opt out from receiving any cold calling (DMACensus).

NewInfoTrade asked people about their interest in the idea of using independent data access companies to find out what is held about them, as proposed in an earlier Demos book on privacy,[18] and over 50 per cent said they would be prepared to pay £5 for the privilege, marginally more preferring this to be delivered by post than by telephone.

The DMIS Direct Mail Trends Survey (DMACensus) found rising awareness of consumer protection schemes reaching a plateau of 40 per cent in 1993 and 1995 for mail preference services.

DMACensus also cites a BT Telemarketing survey conducted by BMRB in 1996 which found that 58 per cent of consumers claimed to be complaining more nowadays, citing a variety of reasons ranging from rising to falling standards of service, greater confidence, rising expectations and greater ease of making complaints.

Sensitivity of personal information and trading-off privacy with service

Track reports that savings information is the most sensitive, with 75 per cent concerned or very concerned about it, followed by earnings, medical history and credit rating.

By contrast, Dataculture found in 1995 that 61 per cent of consumers were in principle willing to provide personal details to a company in return for better service, up from 48 per cent in 1994, and 55

per cent were happy for a company they trusted to keep personal information about them on computer, up from 31 per cent in 1994. Forty four per cent of women and 29 per cent of men enjoyed participating in loyalty schemes, and the most keen were the 25 to 34 year old age group (42 per cent) and 35 to 44 year olds (41 per cent), with higher socio-economic groups significantly more interested than those in socio-economic group E. However, the offer of a loyalty scheme rarely made people think more highly of a company. About half the sample had, in the last year, provided personal information to a company by some means or other, with the 25 to 44 year old age group significantly more likely to have done so, and the over 60 year olds less likely to have done. Seventy per cent said that they were happier to provide information to organisations of which they were regular customers.

Dataculture qualitative research suggested that the key characteristics of an acceptable direct marketing communication were being targeted their needs, relevance, coming from a known company and adding value. A Royal Mail survey in 1995, reported in DMACensus, found that 69 per cent reported relevance as the most important reason for welcoming letters from companies offering services.

In return for providing personal information, two thirds wanted better service and two thirds of young people and two fifths of retired people wanted discounts and promotions; only between a fifth and a quarter wanted information and products designed for them individually.

The Dataculture qualitative research also yielded a hierarchy of personal information from the not very personal to the highly personal, which was supplemented by a quantitative data broadly confirming the same picture, expressed in terms of percentage of the sample willing to provide each category of information if requested. Nearly 90 per cent were prepared to give a name, postcode and address, nearly 80 per cent their marital status and over 70 per cent their TV viewing habits, hobbies and interests, age and car ownership. Savings, income and other financial details, work telephone number, value of house and politics were considered much more personal, as were (in the qualitative research) medical history and education. The survey also found that 60 per cent were prepared to give more information if their record

remained anonymous. Men typically thought TV viewing, newspaper readership and religion more sensitive, while for women age, car ownership, weight and telephone numbers were more sensitive. Those over 60 were less likely to be willing to provide information on request, with 20 per cent of this group reporting themselves unwilling even to give their name. Hedges' qualitative research confirms this general ranking of sensitivity but adds that, in large quantities, apparently trivial information can become sensitive. Figure 4 summarises these findings.

In a more positive vein, NewInfoTrade asked people what would make them trust a company with personal information. Around four fifths of the sample chose being treated with respect, being told what the company would do with the information, being open and honest and having a reputation or quality service. Membership of a trade association, keeping information within a department or communicating with them regularly scored far lower.

Dataculture found that only 17 per cent of their sample wanted personalised services in exchange for information: most wanted better general service or discounts. Like Dataculture, NewInfoTrade also asked in more detail exactly what service enhancements people – or at least, pragmatists – expected in return for providing personal information. The most popular enhancements were individual treatment, free delivery, recognition and discounts, all picked out by more than 80 per cent of the sample. The next most popular group were advance warning, tailored products, free telephone services and a simple thanks for their custom. Air miles and home shopping attracted only minorities, although at more than 40 per cent, these are substantial minorities. However, rather few people reported that they were getting the individual treatment they wanted and only banks were cited by more than a third of the sample as providing it.

However, the survey also found that 60 per cent of the sample did not realise that smart cards record data about the holder as they use them, with lack of appreciation highest among women, older people and socioeconomic groups DE, at about 70 per cent. A majority of the sample were unhappy for companies to collect smart card transactions data, despite the fact that a majority were also generally pragmatists.

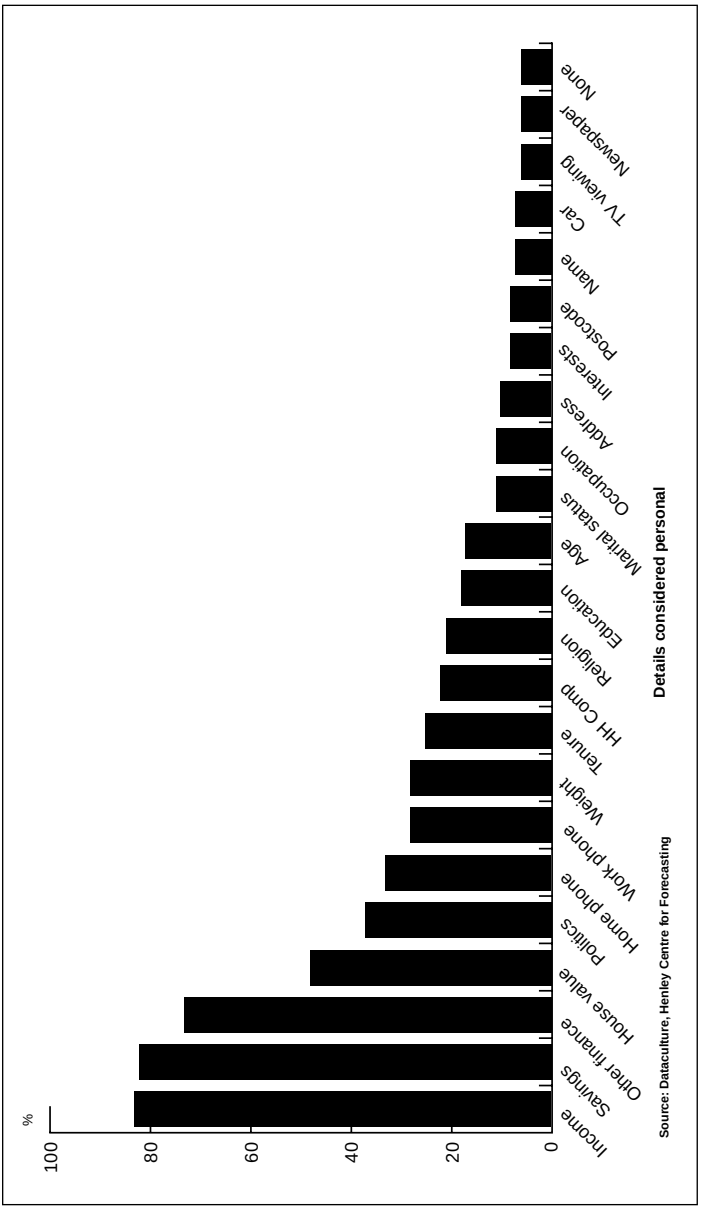

Figure 4 What is considered 'extremely personal' information?

POE found a hierarchy of sensitivity broadly similar to that which emerges from NewInfoTrade and Dataculture: financial information was most sensitive, phone number slightly less (but women being more concerned about this than men) with name, address and, interestingly, household size and composition relatively insensitive.

Kable asked people about their views on public sector smart cards and found that 80 per cent of the sample agreed that they could be useful, while only 5 per cent could see little or no use for them.

Ranking organisations that use personal data

POE found that the general reputation of companies seeking or using personal information mattered in many people's decisions on whether to provide personal information and, if they did provide it, when, how and what type. The reliability of junior staff also emerged as a key factor.

Track reports that mail order companies are the least trusted (53 per cent report themselves as having little or no trust, up from 49 per cent in 1996), followed by credit reference agencies (42 per cent) and shops and stores (33 per cent).

Dataculture used a different way of classifying businesses. The survey found that 46 per cent did not like direct marketing – which, their qualitative work suggests, people associate with junk mail and cold calling – from automotive companies, 34 per cent disliked it from consumer goods companies and 25 per cent from information technology, other high technology and telecommunications companies, while travel and leisure companies encountered the lowest levels of resistance at 15 per cent.

Dataculture also asked people which types of organisations they were aware held data on them and, of those organisations, which ones they were happy to provide personal information to; it then subtracted the one from the other to give a simple index of privacy concern by type of organisation. The organisations that few people were aware held data on them were food manufacturers, supermarkets (18 per cent), newspapers and magazines (19 per cent), clothing retailers (21 per cent), leisure and travel companies (26 per cent) and hi-fi and computer companies

(26 per cent). However, 56 per cent were happy to provide information to supermarkets, while only 31 per cent were happy to provide it to newspapers and magazines. The biggest gap between awareness and contentment was for government and local authorities combined (−33 per cent), banks and building societies (−20 per cent) and utility companies (−12 per cent), although it should be said that absolute levels of happiness to provide information for these organisations were relatively high at 56 per cent for government, 74 per cent (the highest of all) for banks and building societies, and 65 per cent for utility companies. These findings are summarised in Figure 5 overleaf.

NewInfoTrade asked people whether they trusted types of organisations a lot or a little. Building societies and banks scored positive trust with well over 80 per cent of the sample, with charities, telephone companies, insurance companies, utilities, supermarkets and credit card companies finding some trust among about four fifths. Lowest scores were for car dealers and manufacturers, magazines, cables companies and home shopping companies, none of which crossed the 60 per cent threshold. In general, the more contact people have with an organisation, the more they seem likely to trust it. There are, probably, two processes going on here. On the one hand, people choose to have more contact with organisations once they trust them. On the other, if one has to have extensive contact with an organisation, distrusting it is a painful business and making oneself trust it may reduce what psychologists call the 'cognitive dissonance' of such a conflict between emotion and behaviour.

NewInfoTrade reported rising take-up of loyalty card schemes, in particular for the supermarkets, especially among younger and upper socioeconomic group households, who are the target high value customers. Fifty per cent of the sample reported holding some kind of loyalty card.

Measuring public confidence in government data handling by the different agencies within the public sector is rarely undertaken, partly because so few public bodies have much 'brand recognition' with the public. Track reported some data for the period 1989–92, which was reproduced in the 1996 Demos book, *On the cards: privacy, identity*

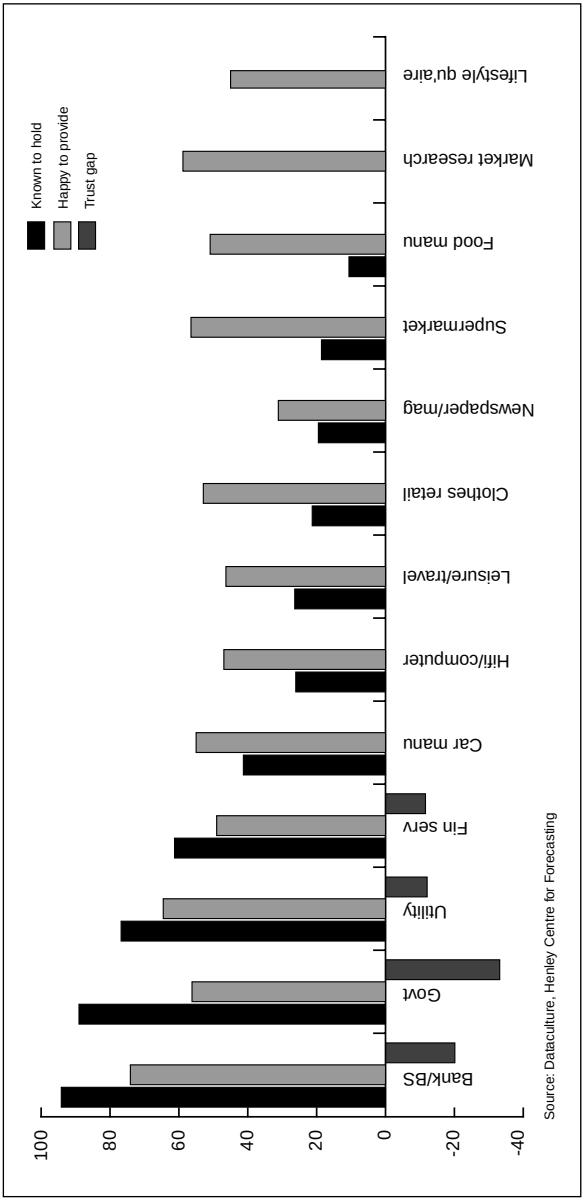

Figure 5 Who holds personal information and to whom are we happy to provide it?

and trust in the age of smart technologies.[19] Those surveys showed that doctors and the NHS generally usually found over 90 per cent of the sample prepared to trust them with personal information, while the police attracted just over 70 per cent of the samples, schools and colleges about 66 per cent and the DSS just over 60 per cent.

Hedges found that the DSS and its agencies attracted rather low levels of confidence and some participants felt that they collect more information than is necessary, often verbally in physical office settings which lack privacy, and that they perform poorly in explaining what is done with the information collected or the rights that claimants have to see and correct their records.

NewInfoTrade provides a more detailed breakdown. GPs remain top of the league, with the post office and then the health service not far behind in the ninetieth percentile. Interestingly, the police score much higher on this survey than Track found, with just over 80 per cent. The DSS and local government score the lowest at just over 60 per cent, with local councils scoring the smallest proportion of those who trusted them 'a lot' at just over 20 per cent.

This is broadly in line with MORI omnibus survey data on which individuals in particular roles are trusted to tell the truth. GPs are consistently at the top of the league, followed by teachers, with business people and politicians somewhere near the bottom, just below journalists.

Segmenting the population's commitments to privacy

POE found that, in their small scale qualitative study, privacy concerns were relatively evenly distributed across the age and class strata on which they focused.

Dataculture, using a similar method to that adopted by Equifax (described above), segmented the population into 8 per cent who are unconcerned about the collection and use of personal information about them, 9 per cent privacy fundamentalists who are unwilling to provide personal information even in return for service enhancement, 3 per cent who simply do not participate in the 'dataculture', and a massive 80 per cent pragmatists who will make trade-offs on a case-by-case

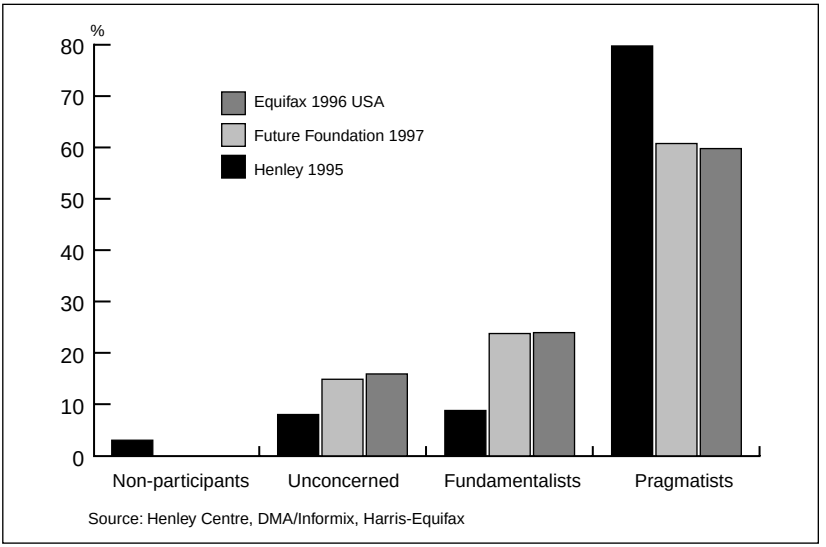

Figure 6 The conventional segmentation.

basis as to whether the service or enhancement of service offered is worth the information requested. This can usefully be compared with the US data and with other surveys, as Figure 6 overleaf shows.

NewInfoTrade took this analysis a step further, using a factor-cluster analysis, which revised the conventional segmentation by dividing privacy pragmatists into those who are more disposed to place their trust in public bodies and those more disposed to private companies, and provided some demographic profiles of the segments.

That survey found that 11 per cent appeared to trust no one but their GP and were especially distrustful of credit card and insurance companies and, contrary to what might be suggested by Dataculture, were more likely to be young. Thirty four per cent, typically older people and those from lower socioeconomic groups, were very trusting of both sectors. Twenty five per cent placed more trust in public agencies than commercial companies, although within the commercial sector

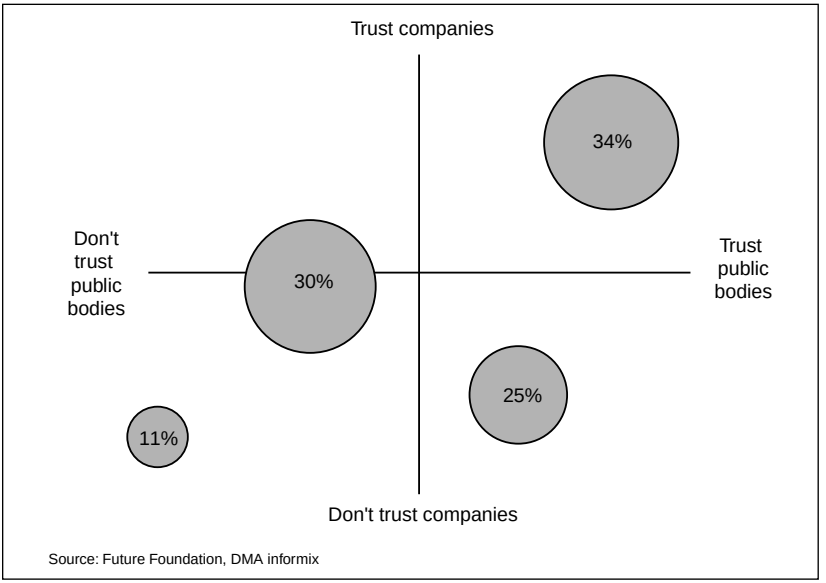

Figure 7 A revised segmentation.

they have slightly more faith in utilities than other types of company and they are relatively trusting of building societies, traditionally seen as less profit-oriented. They are more likely to be ABC1, aged 35 to 54, male and have children. Thirty per cent were ambivalent about commercial companies but significantly distrustful of public agencies; they were slightly more likely to be female and younger. Figure 7 summarises the results of their factor-cluster analysis.

Working with the conventional threefold Westin Equifax classification of unconcerned, pragmatists and fundamentalists, NewInfoTrade produced a different breakdown from that offered by Dataculture: only 61 per cent came out as pragmatists, while 15 per cent were unconcerned and fully 24 per cent were fundamentalists.

The Brunel research takes a more nuanced approach to segmentation. The authors argue that individuals generally take different stances in different situations; very few people can meaningfully be described

Element	Characteristics
Balance	willing to make trade-offs; resigned trust
Defensive	give minimum info; control flow; question organisations' motives
Big brother	find use of PI threat; feel powerless; refuse to provide
Techno	see self as technologically aware, capable, understanding, rational

Figure 8 Not segments but a repertoire of behaviours.

as fundamentalist, unconcerned or even pragmatic in all shopping situations. Therefore, they prefer to distinguish repertoires of stylised types of response to privacy-related situations in shopping.

They distinguish four clusters of repertoires. 'Balance' is a cluster which is willing to make trade-offs, balancing gains and risks, and trusts in a resigned way to providing personal information as necessary to participate in the consumer society. 'Defensive' is a repertoire in which shoppers give the minimum information, are very concerned about where the information will go, question the motives of the organisation and have specific views about the legitimacy or otherwise of particular possible uses. 'Big brother' finds use of personal information threatening and is threatened by new technology and fears ever greater surveillance, but feels powerless or hostile and may refuse to cooperate or even provide false or misleading information. The 'techno' repertoire describes awareness and confidence with technology for electronic shopping and payment and one's ability to make informed risk assessments and decisions, and sees no inherently greater risk to security or privacy from electronic payments than from conventional payment systems. Figure 8 above summarises the Brunel view of the repertoire.

The emerging picture of British public attitudes

The general picture that emerges from this body of research on public attitudes in Britain is of a population that is genuinely concerned and anxious about the fate of privacy and the handling of personal

information, but among whom confidence in one's own ability to protect oneself is unevenly distributed between a generally more consumerist and private sector oriented group of younger people in their twenties and thirties and a much more suspicious older population.

A degree of fatalism about the inevitability of privacy violations can be detected, especially in the qualitative research, but clearly most people are not equally resigned about all the kinds of risks to privacy. In general, people are more resigned to the collection and maintenance of large banks of data than they are to the idea of casual or simple commercial disclosure of information to suit the convenience of large organisations. Awareness of risks, particularly in the newly emerging fields of loyalty schemes and smart card technologies, is growing from a low base, but there are wide differences between people in levels of awareness.

People report quite consistently a hierarchy of the kinds of information they regard as more personal and sensitive than others. While some people may have general dispositions to trust public or private organisations on the simple basis of their organisational form or sector, most do not. Thus, while GPs and the NHS score highly, local councils score poorly in the various trust leagues. Likewise, the differences within the private sector between trust in banks at the top end and trust in double glazing companies, car dealers and mail order firms at the bottom are much greater than the differences between sectors. The presence of accountability to the public through the ballot box or the profit motive is not, for most people, the crucial factor in making their trust decisions.

Those who are prepared to make their decision on the pragmatic basis of providing information when the service offer is worth the loss of privacy want a great deal more individual service than they are getting. While, when prompted, a majority say they are aware of the existence of the Data Protection Act and some of the principal rights that it enshrines, many are sceptical about its value, its ease of enforcement and the willingness of many organisations to comply with it. While many people see no alternative to legislative regulation that would be as effective in protecting their privacy and feel that it should indeed be

strengthened, most people seem to make a fairly sober assessment of the capacity of the law to discipline commerce and government in the information age.

What remains to be understood

On reviewing this evidence, it is clear that policy makers considering how to move forward in data protection, business strategists concerned with the legitimacy with customers of their operations and regulators, such as the Data Protection Registrar, all need to know much more about what lies behind these public attitudes in Britain.

In particular, we know very little from these various pieces of research about the forces that shape the decision to trust or not to trust, or where there is no decision because there is little choice but to use the agency's services, the feeling of trust or distrust. In short, we need to know, firstly, more about why people trust organisations (reasons) and what exactly they trust them to do or to refrain from doing (tasks).

Secondly, we also need to know more about the relationship between the risks that people perceive and the specific privacy-related tasks that people trust or do not trust organisations to carry out with their personal information. Thirdly, we need to learn more about the relationships between the reasons for which people do or do not trust organisations and the tasks they entrust to them.

Finally, when we have learned more about reasons and tasks, we should be able to understand better the ranking of trust between different kinds of organisations. At the moment, we know what does not drive the ranking – namely, sector – and only a little about what does. Personal face-to-face encounter, regular contact, esteem and belief in the presence of some code of professional ethics all seem to matter in the case of GPs and the post office but we know very little beyond this.

We designed our research specifically to build upon the body of knowledge summarised in this chapter and to supplement it by exploring these four key gaps in our knowledge.

2 Findings from the focus groups

This chapter presents the principal findings from our qualitative work, which took the form of focus groups. Having explained the purposes of this research and the methods used, we then present some of the key substantive findings on what triggers heightened awareness of privacy risks, awareness of strategies for dealing with these risks, the extent of fatalism or confidence in the possibilities of using these strategies to secure privacy, the kinds of reasons that people offer for trusting organisations to respect their privacy and handle personal data in an acceptable manner and, finally, their attitudes to different kinds of organisations.

The purpose of the qualitative work

For this programme of research, it was important to use both qualitative and quantitative research methods.[19] The qualitative work was undertaken for three purposes.

Firstly, the results are of interest in their own right. They provide a richness and depth of experience and language that quantitative statistical analyses of data gathered on a restricted set of possible responses to preset questions cannot.

Secondly, we wanted to use the findings of the qualitative work to help us design and phrase the questions for the survey. In this regard, the material gathered was of enormous use in helping us to design the survey instruments that appear in Appendix 2.

Thirdly, we wanted to use the findings to help us interpret the meaning and in some cases qualify and nuance the significance of the quantitative survey data, which, when read too simply and straightforwardly, may be misleading. We conducted our focus groups before the survey because we ranked the second purpose above the third.

Methods

Four focus groups were held, each with between eight and eleven persons, during March 1997. The focus groups were held in Stockport near Manchester, West Wickham in Kent, Newcastle-upon-Tyne and Bristol, to provide a reasonable geographical spread of participants. The participants were recruited for us by MORI Field & Tab. All focus groups were moderated by at least one researcher; three were moderated by two.

As selection criteria for participants, we tried to use a variant of Westin's now canonical segmentation developed by the Future Foundation in NewInfoTrade:

- those who generally trust most organisations to handle information about them properly ('unconcerned')
- those who generally do not trust most organisations to handle information about them properly ('privacy fundamentalists')
- those who trust some organisations but not others and who trust private organisations (firms, companies, voluntary bodies) more than public ones (government bodies) or are neutral ('pro-commercial pragmatists')
- those who trust some organisations but not others and who trust public organisations (government bodies) more than private ones or are neutral ('pro-government pragmatists').

Rather than to try and get a spread of these types in each region, we sought to recruit one group type within a region.

Although there was no great difficulty in finding participants, the recruiters reported that the sectoral distinction was not clear to many

people. In addition, the groups, once recruited, turned out not entirely to reflect the selection criteria. In particular, the 'unconcerned' group turned out, on probing during the session, to be more fatalistic than unconcerned. And there were many common themes. While this alone cannot suffice to cast doubt on the robustness of the segmentation, it does confirm findings from some qualitative research conducted for the Office of the Data Protection Registrar that, in general, the more people are made aware of, or reflect on, what they know of the risks to their privacy, the more concerned they become.[20]

The group sessions covered attitudes both to privacy and information issues in general, and to nine specific organisations or types of organisations: banks, supermarkets, local councils, electricity companies, the Inland Revenue, the Department of Social Security, the police, telephone companies and GPs. Appendix 1 contains the topic guide for the sessions.

What raises privacy concerns

The main way in which privacy issues impinge on people is through junk mail and telephone calls. Most people expressed some degree of annoyance at this. A few people said that it was interesting to receive offers and you could always turn them down, but the general view was unfavourable. People said that they would go out and look for a product if they wanted one, that they felt pressured, that the mailers were trying to impose choices on them and that the mail was a waste of paper and trees.

> 'I got a water bill the other day and inside it was like the Sunday supplements – loads and loads of leaflets for insurance, double glazing, cushion covers – there was about half a dozen. I took the bill out. I thought, what is going on with this interchange of information? What a waste of paper'.

Many people thought that, once information was on any computer system, it was possible for anyone to 'hack into' it. Many people had

also been surprised that companies could identify them over the telephone when they gave their postcode and some other piece of information (such as house number).

> 'There's always somebody who can hack into your computer. You hear about it all the time. I wouldn't have thought anything was safe on a computer'.
>
> 'I gave this lady my name and postcode. She told me where I lived. Even the number on the door'.
>
> 'With all these computers, anybody can just hack in and find out anything. You just give someone your postcode and they know who you are.'

Most people could not think of any particular bad experiences regarding information disclosure. But some had interesting stories.

> 'Last Christmas I wanted to get another mobile telephone. They go through a credit rating agency. The answer came back, a big no, and I was very embarrassed. And I went through the motions of sending off a pound for the information, and I never got a reply. I went to my local shop and my credit was OK. I was angry, but there was just an answer-phone with an address, and in the end I wrote off and never heard anything. I never fully followed it up. I could have taken it a lot further, but we'd moved on by then and it wasn't important.'
>
> 'I had lots of telephone calls, all asking for the same wrong name. And this chap said, 'It's your fault this happened, you must have got some kind of card. Have you got a card?' I put the telephone down on him. It's not as if he said, 'I'll take the information off, very sorry to disturb you.' It was a very arrogant attitude.'

'My son had problems living in London, and I think he went a bit over with the bank, and we had a stop and we didn't know why, because we've always paid all our bills. It was all rectified, but it was a bit of a shock.'

'I had a problem with the Health Service and the school nurse. There was something my daughter had said and they wanted an investigation. It didn't turn out to be anything. But some time later I applied for a fostering job, and they knew all about it and that was the first thing she asked me. She said, 'It's on your records.' I'm going for a teaching course in September. Will it affect that? Will it affect everything for ever?'

'I telephoned up Marks and Spencer to see about a loan – just enquired – and, the day after next, we had something through from the bank saying. 'Do you want to borrow any money? 'We couldn't believe it. It could have been coincidence, but we didn't think so.'

'We've got cable telephones and we've had our number changed three times. Someone within the cable network was selling the telephone numbers. We're ex-directory. This individual was actually selling our number to other people. And it happened twice with different people.'

There were some concerns about the possibility of information going abroad.

'I heard something thoroughly disturbing on the radio about how the NHS processes appointments. It's all computerised, but apparently there's so much that they're shipping it out to India for processing. I was a bit rattled. I've nothing against the Indians, but it's 8,000 miles away. There may not be the controls over there.'

'Now London Electricity's gone public, they've been bought up by some Americans. That I don't like. If it's English, and it's British, I know it sounds really naff, but that's fine. But when they start saying these Americans are going to buy it. I don't really want some person in the States knowing my details.'

'It's more worrying that the data's going abroad because I feel I'm less aware of what that data might be used for than I would be in this country. I feel I'm more aware in this country of the implications of certain people knowing certain data.'

'I suppose that perhaps with Europe going to be a federal state, there's going to be an enormous computer somewhere with a lot of data on it.''Horrendous thought, isn't it.''Why? What might happen?''It just conjures up lack of individuality, lack of freedom.'

Many participants were concerned about the inferences that could be drawn from data.

'With a credit card, there's an awful lot of information that's taken down about you and at the touch of a button they can cross-reference you with anyone else.'

'My brother could be a missionary to Colombia, and I could call him once a month to speak to him, and then some little bright spark says 'Ooh!' I could get a lot of hassle I wouldn't deserve. I wouldn't want that sort of monitoring. I think it's an invasion of privacy.'

'I have three children, and I went through a phase when over three weeks I was at casualty with all three of them. The hospital telephoned my health visitor and luckily she knew me, otherwise I really felt as if I was going to be done for child

abuse. I thought, to someone looking at my record, it looks terrible. If I'd been a single parent, living in Inner London, with no money, I think I would have been in trouble.'

'If you're applying for a teaching job, they go through all the records. I think it's a bit more than if you've interfered with children. Do parents want their children to be taught by someone who drunk-drove into a bus queue twenty years ago? Is this person fit to be a teacher? I'm not saying whether it should come into it or not, but I think it does for local authorities. If somebody used to be a drug dealer – not necessarily to children – twenty years ago, are they sufficiently reformed now to be trusted with children and the future moral welfare of the nation? That's the view of some parents'.

'In America, they don't want paedophiles moving in next door to houses where children live. It could turn into a witch-hunt. Some of these people are evil and they'll keep doing it, but some are genuinely sorry and rehabilitated, but they won't be left alone for the rest of their lives.'

Awareness of coping strategies

Most groups had some awareness of the Data Protection Act and/or the Mailing Preference Service, but few had tried to use them. Only a very few people had sought to exercise any information rights, always in connection with credit referencing. People generally did not know what their rights were nor how to exercise them.

'I should imagine it's a hard thing to do and would cost you a lot of money.'

'I don't think it would cost you money, but I think it's very hard to do and doesn't particularly get you anywhere.'

'I'd like to see some flyer with the information telling you how to complain and who to, because nobody here knows how to go about it.'

'I don't think you've got many rights. They've got what they've got and you can't do anything about it.'

'I think it's gradually changing now. You can demand to see your record and they can't say no. Once upon a time they could stop you. That's law now.'

Most people were prepared to fill in forms, even if they found them intrusive, but some had refused on some occasions.

'If you want the credit card, you just fill the form in, because if you don't, you won't get it.'

'Many years ago, I don't know if you remember the Marshall Ward catalogue? That came with this form that wanted [to know about] my grandmother, how old she was, and everything else, and I thought 'Blow this' and tore it up. I remember that distinctly. It went back to my grandparents.'

'I went to B&Q wanting to buy a kitchen on HP. They asked me all sorts of questions which I didn't think were applicable. But at the end of the day I wanted to buy the kitchen and I wanted to do the HP through them.'

'There's not a lot you can do about it, really, is there? You want benefit, you've got to give them the information. There's so many people claiming benefit who aren't entitled to it.'

'I leave them blank. You just say it's got nowt to do with them and leave it blank. They won't come back to you, and if they do you can ask why they need it.'

Fatalism versus confidence and competence

Sometimes, attitudes were resigned or fatalistic rather than trusting. Some participants tended to believe there was nothing they could do to protect their privacy. By the end of their session, the supposedly 'unconcerned' group seemed to be getting a little annoyed that we were persisting with a subject they had decided there was nothing to be done about.

'I think, really, on the whole, everybody knows everything about everybody now. There's not a lot you can do about it.'

'Every piece of information you've put down somewhere, in your life, has been gathered and it will be used and people will be able to buy it. There may be certain things that maybe under Charters that you can't get over, but basically people can get everything they want to know about you.'

'It just gives them the ability, the information, to get in touch with you. I don't think it does you any good. I don't see how it can do you any good.'

'You're just a number. That's just life these days.'

Reasons for trust

However, not everyone was fatalistic and, of those who were, some at least were not consistently so. A number of people thought that the risk of loss of reputation in a competitive market would be a discipline on organisations.

'If blanks weren't secure, they'd lose business. If one of them was notorious for not respecting confidentiality, the other three would gain business.'

'As a big company, BT have got a lot to lose if it became public that information exchange was going on and people lost confidence in them, especially now that they're open to competition.'

Confidence in the individual staff of organisations varied considerably, with those in banks being highly rated and those in local councils less so. Staff who were regarded as 'professional' commanded confidence, even when (as with the Inland Revenue) they were not liked. Opinions about the police varied widely.

'Banking is a confidential profession. A clerk in the Town Hall might not have the same amount of discretion.'

'I trust the Inland Revenue implicitly, though I don't like to say that – they've chipped away at my money over the years.'

'I worked for a doctor for sixteen years and I know that the secretaries are reliable. You have to be, or you'd be out on your ear.'

'The charter and the Hippocratic oath are very important to doctors.'

'I trust the police because they're the police.'

'A policeman, an ordinary human being, is open to corruption. And they've got access to all sorts of information and would be willing to sell it to someone who was willing to pay for it.'

'There are so many people who work for DSS – information must leak.'

Attitudes to particular organisations

Banks were felt to be secure organisations, with generally trustworthy staff. It was felt that they had much to lose in terms of reputation if they failed to handle personal data properly. There was however some concern at the exchange of financial information within the bank for marketing purposes. It was strongly felt that they should keep the information they held within the bank, though few people doubted that they did so. Different banks were not perceived as being very different from

one another, thought some people would be more worried about non-UK banks. Some participants took a fatalistic view that they had to rely on banks whatever they might think of them.

Supermarkets have only recently begun to hold information on individuals. For people who hold 'loyalty cards', this information includes data on all transactions where the card was used. In discussion, the groups reached a correct understanding of what information was held but participants' initial levels of understanding varied a good deal. Some believed they had only provided their name and address on their application form and so the supermarket only held that information. Generally, people felt that information about their shopping was not very sensitive and not something to worry about. There was general scepticism about supermarkets' diversification into banking services.

Local councils were perceived as having quite a lot of information on some people, especially those receiving social services. The fact that councils sell electoral roll data was not known to all participants and rather shocked some. Some doubts were expressed about the reliability of councils as organisations and of their staff as individuals. There was ambiguity in people's attitudes about the sharing of information between council departments for child protection and the sharing of information with the DSS for benefit purposes.

Electricity companies were not seen as holding any particularly sensitive or confidential information. One participant was aware that her electricity company was now in US ownership and worried about what that might mean for her personal information. Participants were not generally worried at the possibility that their electricity companies might try to sell them other services, such as gas.

The Inland Revenue was perceived as holding a great deal of information but also as handling it securely. They did not seem to be liked as an organisation but participants saw them as likely to hold information confidentially. A recent scandal about an Inland Revenue employee had affected some respondents' confidence. Again, there was some fatalism: some participants felt that there was nothing they could do.

The Department of Social Security was perceived as knowing a great deal about certain people. Participants had only limited confidence in

the organisation and its staff; they were felt to make too many errors and sometimes to behave dishonestly. Some people who had claimed benefits had come away with a negative impression of the DSS. There was some feeling that it was necessary to use information to combat fraud, coupled with a fear that the use of wrong information might lead to wrong decisions.

Telephone companies (mostly BT) were seen by some participants as similar to electricity companies in that the information about usage that they held would not be very sensitive or interesting, unless perhaps it included calls to sex services. A minority of participants were much more sensitive about information on who they called, which they regarded as very personal. Some feared that their call data might be analysed for political or commercial ends, others were concerned with the possible effect of itemised bills within the family. Confidence in the telephone company was generally high but some participants were aware that telephones were sometimes tapped and were distrustful as a consequence.

The police were perceived by some participants as holding information only on people with criminal records and by others as holding data on a very wide range of people. Confidence in the police varied from the very low to the very high. At the top end of the scale was implicit trust in the police simply because they were the police. At the bottom end, a number of participants felt that individual officers might sell information. People with relatives who had direct experience of the police service seemed to have more concerns about the quantity of information held and the possibility that it might be 'hacked'.

GPs were perceived as highly trustworthy, even though the information they held was considered very sensitive and participants were keen that they should not disclose it. Professional ethics and the Hippocratic oath were frequently mentioned. There seemed to be a similar level of trust in hospital doctors. The only concerns mentioned (and these rarely) were to do with the reliability of GPs' staff and general concerns about the security of computers. Some comments reflected trust that doctors genuinely sought to do the best for their patients; a few expressed a fatalistic view that one had no choice but to trust one's doctor.

Conclusions

A number of issues emerge from these qualitative findings. Privacy was an important concern for most people but often a latent one. Often it was only when probed about the issues that people began to think through the risks they might face and to recognise that they had concerns about those risks. It would be useful to know what situations outside the artificial climate of the moderated group discussion have the effect of triggering the movement of these latent concerns into consciousness and reflection.

There is clearly a relationship between one's confidence in one's own ability to negotiate a way through the transactions that face one with these almost unavoidable large organisations and one's trust in them to handle the information they hold about one in ways that respect privacy or one's fatalism about the prospect of securing privacy against some risk. In general, as we would expect, younger people had more confidence in their ability to understand the risks associated with a situation where they must provide some information for service and to find some appropriate coping strategies.

The high trust in GPs suggests two only partially competing hypotheses that will be important in understanding the dynamics of trust. It might be that trust in the personal information handling of GPs flows simply from the generally high esteem in which doctors are held. Rather than high esteem being a view arrived at on the basis of prior trust in them to carry out a variety of tasks and eschew other things regarded as sins, it may be that the causal relationship for many people is the reverse. Alternatively, it may be that doctors are trusted to handle personal information on the basis of the public belief in the value of the professional ethic and duty of care owed to each individual client or patient, combined with face-to-face contact with a named individual practitioner in control of her or his own organisation, which is missing in the case of transactions involving larger organisations. We shall return in the final chapter to the relationship between esteem and trust.

3 Design of the survey

In this final chapter of the first part of this report, we explain the strategic principles and the tactical decisions that went into the design of the survey questions. Most reports of this kind do not need to devote such space to this issue, as the survey questions are not discrete entities related only by a common interest in privacy but focused on distinct aspects. In this case, however, the questions are closely related to one another and tightly linked as a part of a programme to test some theoretically grounded hypotheses about the nature of trust in organisations handling personal information.

Understanding trust

The aim of the survey was to understand why people trust organisations and what they trust them to do. For this purpose, we drew on some earlier theoretical work.[21] Trust is an 'agency relationship'. That means that typically we trust people or organisations for given reasons to carry out particular tasks. Therefore, trust is quite distinct from esteem, in which no tasks are required, and from respect, where even clear and distinct reasons may be absent. It is an empirical question whether someone will only trust the people or organisations that they hold in high esteem or respect and vice versa, and if so, and whether esteem comes first or trust comes first.

We classify the reasons why anyone might trust anyone ('reasons'), and what they might trust them to do ('tasks'), in the following way. We begin with reasons.

First, we might trust on the basis of past *experience* of dealing with the person or organisation in that they have been proven reliable. Second, we might trust on the basis that the person or organisation has a *reputation,* in either of two ways. We might take evidence of that reputation as a kind of reference, trusting on the basis of the reported experience of others. Or we might infer that the person or organisation will value that reputation and behave in a trustworthy way in order not to damage it.

Third, we might trust on the basis of *characteristics* – for example, because we share the same nationality or the same local roots as the person or organisation, or in some cases, simply the same sex, we might decide that they are trustworthy. Alternatively, if we believe someone to be reliable on the basis of an eyeball-to-eyeball judgement, we are ascribing a characteristic that is, for us, a reason for trust. In some cases, this may be a special kind of reputation based trust, if we think that reputation in the community of shared identity is valued. Alternatively, if we think that the person or organisation may feel some sense of obligation to us because of that shared identity or some other characteristic, the role of the community of identity is more to do with moral scope of duty.

Fourth, we might trust on the basis of various *institutional* factors. *Generic institutional factors* include the availability of legal redress in the event of default, while *specific institutional factors* include the warranties and guarantees or other 'hostages' that the person or organisation may offer us.

Broadly, we then classify the tasks as follows. First, the *minimal* or merely *prudential* level of trust whereby we trust a person or organisation whose statements of intent that they make toward us can be believed. Promises, threats and other indications of intention to do or not do a certain thing can be believed, whether or not they are welcome.

Second, we may trust the person or organisation to carry out the *contract* that we have with them – explicitly or implicitly by virtue of

some legal rule or duty – and, presumably, to do so to the threshold level of *competence* required, explicitly or implicitly – by the terms of contract.

Third, we may trust the person or organisation to exercise *goodwill.* That is, we trust them to put our interests first and use their discretion in the agency relationship to promote our interests. If the terms of the contract turn out not to be in our interest, then one who exercises goodwill trust-worthiness will set them aside. If they are in our interests, they may do a little more for us than the contract requires.

There is a fourth category of trust, which we might call *absolute* or *moral* trust, in which we no longer trust the person to do anything in particular, but trust them, *tout court.* Organisations are not normally eligible for this category and it will be ignored henceforth.

Cross-tabulating these categories yields the following matrix:

Tasks:	**Reasons:**	**Minimal (prudence)**	**Contract and competence**	**Goodwill**
Experience				
Reputation				
Characteristics				
Institutions				

Figure 9 The dimensions of trust: reasons and tasks.

In some situations, if we trust at all, we will not trust for just one reason but a combination of reasons. Moreover, if we have reached goodwill trust, then implicitly we have already achieved contract trust, and likewise one cannot place contractual trust without first placing minimal trust. Therefore, we should think of any particular trust relationship as being represented not by occupying a cell in the matrix but rather by an area of the matrix covered.

In general, movements like ink spreading over blotting paper to the right are movements in the direction of greater trust, while shrinking of the inked area to the left represents falling trust, perhaps the consequences of some betrayal. It is not necessarily the case that having

forfeited our goodwill trust, the person or organisation will retreat all the way to the left hand border of the matrix or even back to prudential trust: they may still be trust-worthy under contract, provided we retain reasons for trust that lead us to think that breaking a contract would:

- be so out of character that even the negative experience of failure to provide goodwill does not lead us to imagine that they would do so
- damage a valued reputation
- break some duty owed by virtue of particular characteristics
- run risks by way of some institution such as contract law or a prior specific warranty.

Our previous research[22] led us to frame the following key hypothesis:

- People who place 'goodwill trust' in a person or organisation will be more likely to do so on the basis of experience than on the basis of institutional factors.

A culture of active, self-confident consumerism, in which individuals view themselves as powerful purchasers in a market, placing provisional trust in an organisation on the basis of evidence, expecting transparency, concrete assurances and some means of redress, will be one in which experience based reasons are more important than institutional ones. There are two kinds of consumerism. In a *consumerism of exit*, a provider that does not behave in a trustworthy fashion will be forsaken in favour of the next who might. In a *consumerism of voice,* people remain with the provider (perhaps because the absence of any alternative to choose) actively complain, seek redress and make demands. In the data that we obtained, we can also glean something about whether, if so, among which groups such types of consumerism are to be found in respect of the handling of personal information.

The survey design reflects this theoretically grounded classification of reasons and tasks. We listed the privacy risks that we had identified

from our review of the privacy literature and, from our qualitative research, framed a description of behaviour that would not present an individual with that risk and classified those behaviours using the taxonomy of tasks. Then, using the same method, we derived a grouping using this system of the main reasons offered for trusting organisations to respect privacy of personal information.

The questions were designed to elicit from individuals the key tasks and reasons they associated with five priority types of organisations, using a technique that we have used in previous research on trust.

Classifying the reasons and tasks around privacy risks

Privacy can usefully be thought of as a claim that individuals should – at least up to a point – be protected against certain kinds of risks.[23] Following the classification developed in Volume 1 and summarised above, we can identify tasks corresponding to each of the reasons. We classified the reasons and tasks as follows (Figures 10 and 11).

Although the grouping of reasons follows straightforwardly from the meaning, there is some scope for argument about the classification of the tasks, and we hesitated for some time over some of them. A heroically maximalist view of the legislation (that is, the 1984 Data Protection Act and the 1995 European Directive which will be implemented in 1998 legislation) would lead one to pack all of those we have regarded as 'goodwill' (except tailoring services to one's particular

Type	Reasons
Experience	People don't often have problems
Reputation	Damage to reputation
Characteristics	Reliable staff
	Because they're British [local]
Institutions	Legal duty
	Written agreements
	Public commitment

Figure 10 The taxonomy of reasons for trusting organisations with personal information.

Type	Tasks
Minimal (prudence)	Use only for purposes notified
Contract and competence	Keep secure
	Don't disclose sensitive without permission
	Keep accurate and up-to-date
	Don't hold for longer than need to
Goodwill	Don't mail or telephone unnecessarily
	Use to provide services to my particular needs
	Don't hold more than need to
	Don't use to make judgements that might be right or wrong
	Don't collect from other places without telling me

Figure 11 The taxonomy of tasks for entrusting organisations with personal information.

needs) into the implicit 'contract' to be carried out competently. However, we have followed what seemed to be more accepted 'common sense' in many organisations that certain practices are regarded as more fundamental. Some of the goodwill tasks, while mentioned in the principles of the legislation, are provided for there in such general terms that it would be hard to enforce them against many data users because they involve fine judgements of necessity and strictness of implication. By contrast, the tasks included in the category of contractual trust are ones for which there exists some more straightforward principle by which one can determine whether or not they have been carried out.

Survey design principles, tactical issues and priorities

Terms

We have eschewed the use of the word 'trust' in the design of questions. It seems to have different resonances for different people and because it has been so widely used in political campaigning, newspaper comment and other writing, it may have become slightly intimidating for some people. Therefore, we have substituted the word 'confidence'.

Likewise, we have preferred 'personal information' to 'personal data', since 'data' is a legal term of art that may not be recognised by everyone and mentioning it might count as leading a respondent to think of the Data Protection legislation.

No 'do you trust?' question

Part of the point of using the classification of reasons and tasks is that we recognise that trust in an organisation is not controlled by a simple switch, which is either on or off. On the other hand, it is not a continuously differentiable variable in a single dimension either. One either reaches the minimal threshold in order to trust or one doesn't, and after that increases are in phases.

We decided not to ask people the crude question of whether they trust an organisation at all the before asking them in detail about reasons and tasks. Firstly, this might have proven to be misleading because, having reflected on reasons and tasks, they might come to a different answer. Secondly, the answer they might give to such a question might confine their later answers on reasons and tasks.

The future of privacy

On the other hand, asking whether they trusted at all after a battery of questions about reasons and tasks would be pointless. If they did not even score minimal trust, we know that they do not trust and, likewise, if they score no reasons at all then we can draw the same conclusion. Moreover, if we obtained an answer to such a coarse question asked after we had more detailed information which was inconsistent with the detailed task and reason answers, we should have to rely on the more detailed information in any case.

Positive versus negative questions

Questions about trust can be framed either assuming trust and asking 'why?' and 'to do what?', or assuming mistrust, and asking 'why not trust? and 'because you fear what?'. However, because our framework

of reasons and tasks enables us to elicit nuances of trust that the simple 'do you trust?' questions do not, it would have been wrong to frame the questions on the basis of suspicion. Therefore, we chose the positive formulation. This, too, has costs. One might imagine that the issue could be solved by asking people first whether they trusted and then asking 'if not, why not?' and 'if so, why?' questions. However, as we have seen, this would run other methodological risks and in any case would have been very expensive, because it would have required almost twice as many questions.

Segmentation

While it would have been interesting and useful to explore further the segmentation of the population developed by Westin and refined by the Future Foundation and to compare the segments by their reason and choices, with our limited resources we decided that this was not the key priority. However, we introduced some ranking questions which do enable us to make some comments about the idea of a sectoral preference difference among pragmatists. In addition, we can examine our respondents who would accept no proffered reasons or tasks and compare their profile with that of the privacy fundamentalists identified by the Future Foundation.

Sector or organisation ranking

We wanted to explore the differences in the types of reason and task for trust that different organisations attracted. We set priorities, limited by the survey budget, which reflected a reasonable spread of organisations that would be generally recognised by the public and which presented different kinds of privacy risk. We settled on local councils, banks, central government departments, supermarkets and telephone companies. To guide those whose knowledge, particularly of the public sector, is limited, we provided examples of the kinds of institutions we meant them to think about in all questions. While this does produce a more thought through answer, this seemed more valuable for our purposes than the immediate and unreflective reaction.

We considered whether to ask separately about particular agencies such as the Inland Revenue, the police and the Benefits Agency. We decided against this, on several grounds. Attitudes to the police are more likely than to other organisations to be ones for which esteem drives trust rather than the other away around, and the police excite extremes of deference and hostility. Not everyone deals with the Inland Revenue or the Benefits Agency directly and frequently.

We decided on two key tasks on which to seek ranking, which are situated at opposite ends of the trust matrix: one was a matter of prudence (only using information for purposes they say they will) and the other a matter of goodwill, which emerged from the focus groups as of particular concern (not drawing inferences about you that might be right or wrong).

Rating, ranking and priority factor selection questions

For this survey, on the basis of previous experience of survey design work on reasons and tasks for trust,[24] we decided that the best way to get useful responses was to opt for *priority factor selection* questions. In this format, we ask people to choose from a showcard the two or three factors that they consider to be most important for the principal variable in the question.

This avoids the well-known problem with rating questions, that many people will rank a great many factors as 'very important' or 'important', leaving the analyst with no clear idea of how people would want trade-offs to be made in the event that different considerations came into conflict.[25]

It also avoids the problem of arbitrariness in ranking questions in the middle ranks where one has more than, say, six factors. While meaningful information can be gleaned from the top and bottom two ranked factors, the ranking in the middle may be often be forced by the question design, rather than reflecting any real prioritisation.

The risk with priority factor selection questions is that some respondents (other than, of course, those who choose 'none' and 'don't know) will not take up their full quota of three responses, which

makes for slightly qualified analysis. However, on balance, this seemed to be a risk worth accepting.

Rating questions could also have been asked about the felt level of trust – high, neutral, low – placed in each type of organisation. However, there are such questions in other surveys, it would have added significantly to costs and the categories cannot be very finely discriminated. Therefore, because we had chosen a small set of organisations, it seemed worth using that group for ranking questions and concentrating analytic effort on the top and bottom two of the resulting groups.

Response set

There can be a problem known as 'response set' in surveys of this kind. Because questions take exactly similar forms for different organisations, respondents, particularly those who are less educated, may simply race down the questions automatically choosing the same answers to each question. The risk can never be wholly eliminated in any survey which seeks strictly comparable information on any series of variables. It is reduced in this survey by the face-to-face administration of questions and, in the case of these particular questions, the sample was divided into two halves and the order of questions reversed for one half.

One way to test for response set is to examine whether there is a more than explicably probable consistency in the data set. As we shall see in later chapters, there is sufficient variation and even a high degree of independence in the answers gained to suggest that response set is not a major problem with these data. Moreover, those people whose answers are repetitive do not display the sociodemographic profile normally associated with high risks of response set. Appendix 2 provides the questionnaire.

Method

The survey was commissioned from MORI as part of the MORI Omnibus survey between 6 and 9 June 1997. The sample was of 2,018 adults selected across 172 constituency-based sampling points chosen

to be a representative sample of the whole country by region, class, voting patterns and other variables. Interviewers select respondents using a ten-cell quota provided to them. The data is then weighted for social class, standard region, unemployment within region, cars in household and age within sex, to adjust for any discrepancies in the coverage of individual sampling points and to ensure representativeness. Face-to-face interviews were carried out by MORI Field & Tab in respondents' own homes, with the interviewer coding answers. Data entry and analysis were carried out by Numbers Data Processing Ltd. All percentages given in the figures here have been rounded up to the nearest integer.

Part 2
Survey findings

4 Overview

In this chapter, we present some of the 'top line' results, in simple percentage form, and give some preliminary reflections on their significance in the light of the qualitative research. However, there are a number of points on which the 'top line' results are misleading and the more sophisticated analyses presented in later chapters give a more accurate and naunced view.

Reasons

Figure 12 presents the percentages of sample choosing each reason for each type of organisation.

These data on reasons need to be read with some caution. For example, most people chose the presence of the legal requirements as a key reason for trusting organisations. Yet, in our qualitative work, and indeed that of in Hedges and the Brunel team, the law appears to attract rather little confidence: those focus group participants who knew much about it thought it would be difficult and expensive to enforce and none of them knew anyone who had done so.

It could be that these findings tap into a powerful stream of British culture which holds the coercive power that is associated with the law to be the most powerful reason for believing that a principle will be complied with, *only if* the law can be enforced. That is, the data represent a conditional statement combined with a general faith in the 'strong tools' of governance over the 'weak' ones of moral obligation.

Organisation: Reason:	Locals councils	Central government	Banks	Super-markets	Phone companies
Law requires	63	67	62	41	55
Damage to reputation	38	33	47	47	47
Written agreement	34	35	39	22	30
Public commitment	19	17	17	21	21
Reliable staff	17	20	26	16	16
Don't know of problems	15	10	9	15	13
British/local	5	5	2	3	4
None of these	7	7	5	8	6
Don't know	5	5	4	10	6

Figure 12 Reasons for trusting organisations with personal information, by organisation (%).

Similarly, probably rather few people actually possess a copy of any written agreement from these organisations concerning personal data handling, although most will have written policies that can be seen on request for current accounts, tax or benefit accounts, loyalty card schemes, telephone subscription and billing accounts. Perhaps we should read those data as referring to the idea that such things probably exist or that, if they do exist, they probably have some weight.

It is interesting that the absence of experienced or known problems was so low for all the organisations about which we asked people. This reinforces the finding from previous research that concern about personal data handling is often latent rather than at the forefront of people's minds. As we saw in our qualitative work, however, when prompted people find that they often can think of problems.

Some of the difference between organisations in respect of the reasons for trust are relatively straightforward to understand. For example, the greater numbers of people who regard reputation as important in the commercial sector reflects a clear understanding that executive government is less vulnerable from damage to its reputation,

because people have fewer choices to go elsewhere for the services that it offers.

Interestingly, banks appear to occupy an intermediate position between telephone companies and supermarkets on the importance of law as a reason for trust in their personal data handling. They attract more faith in their staff than other organisations, yet fewer people said that they knew of no one who had problems with banks than with other organisations.

Supermarkets are an outlier in this group of organisations, for several reasons. Only supermarkets deviate from the rank ordering of numbers of people picking particular reasons. Reputation, rather than law, seems to be regarded as the principal factor that disciplines their data handling. Certainly, fewer of the public picked the law as a key factor for trust in the supermarket sector than for other organisations. Again, an offer of a written agreement about data handling by supermarkets was convincing to far fewer people than for other kinds of organisation. Slightly more people chose 'don't know' and 'none of these reasons' about the supermarkets than about other organisations. This may reflect ignorance about the purpose of loyalty card schemes but, in some people, it may reflect a measure of uncertainty and doubt about the uses to which the personal data collected in such schemes is being or might be put. However, the relatively competitive score of people who did not know of anyone having problems suggests that the worry is based more on what might be possible or intended than about what is actually being done.

Although the importance of British identity of organisations as a factor making people more confident about their data handling was mentioned in the focus groups, the survey suggests that this factor has very little weight.

Turning to the sociodemographic differences, those aged over 55, those in socioeconomic classes C2, D and E and non-workers tend to place their trust in the law slightly less often and are also a bit more likely to pick 'don't know' or 'none' on the tasks (see the next chapter on those who always pick 'none'). This may suggest either ignorance about data handling, comparatively lower levels of faith in the law or a more general low confidence that

personal data is handled well. However, voting intention does not distinguish significantly between people on the reasons for trust.

People in Wales, Scotland, Greater London and the North West were slightly less likely have faith in the law. Wales also contains more people who choose 'none of these reasons', and people in Wales are consistently less trusting. As many as 17 per cent of East Anglians chose 'none' for central government bodies.

Tasks

Figure 13 presents the 'top line' findings on the things that the British public trusts organisations to do or to abstain from doing. A number of points are worth noting at this aggregate level. Banks attract significantly more public confidence in their data security than other organisations do: this was the only organisation that attracted more than 40 per cent of the sample to pick any one task.

The commercial sector generally attracted more confidence in its ability and willingness to tailor services to the needs of particular

Organisation: / *Reason:*	*Locals councils*	*Central government*	*Banks*	*Supermarkets*	*Phone companies*
Don't mail or telephone unnecessarily	30	25	19	23	22
Keep secure	29	35	43	19	28
Don't disclose without my permission	26	24	32	16	23
Use to provide services to my needs	24	19	27	28	28
Don't hold more than need	18	13	14	19	17
Keep accurate	16	18	27	12	20
Don't make judgements	14	13	9	11	9
Don't collect with telling me	13	11	13	12	12
Tell me what use for	12	12	14	13	12
Don't hold longer than need	7	7	5	8	7
None of these	8	8	6	10	8
Don't know	7	12	6	15	11

Figure 13 Tasks with personal information entrusted to organisations, by organisation (%).

individuals, and central government agencies the least. However, conversely, the commercial group attracted less confidence than the public sector in refraining from unnecessary mail and telephone contact. With the exception of banks, confidence in the security of personal data held by commercial companies was a factor for fewer people than for that held by the public sector.

As with reasons, supermarkets attracted more people to say 'don't know' and 'none of these', suggesting that this sector does face a challenge to convince the public of the quality of its personal data handling. In particular, supermarkets scored poorly on non-disclosure and accuracy of personal information. By contrast, banks scored more highly on these dimensions than any other organisation.

Central government agencies emerge from these data with some evidence of a tarnished reputation by comparison with other kinds of agency, mainly – as we might expect – on non-disclosure and tailoring services to individuals. It was clear from the qualitative work that many people believe that central government agencies already share data extensively; perhaps, also, some awareness has filtered down of recent anti-fraud measures to permit more data matching across the public sector. Interestingly, however, central government bodies score competitively on accuracy and several other tasks.

In general, the very low numbers having confidence that information is not collected about them without their knowledge or that it is used for purposes of which they are made aware suggests that there is a real problem of low confidence in Britain about some of the basic elements of data handling by large organisations.

Rankings

Figure 14 opposite gives the mean scores on the ranking questions for using information only for the stated purpose and for not making judgements that might be right or wrong.

The rank order of the mean scores is the same. While it may be reassuring that the mean scores are not very low for any organisation, none are very high either.

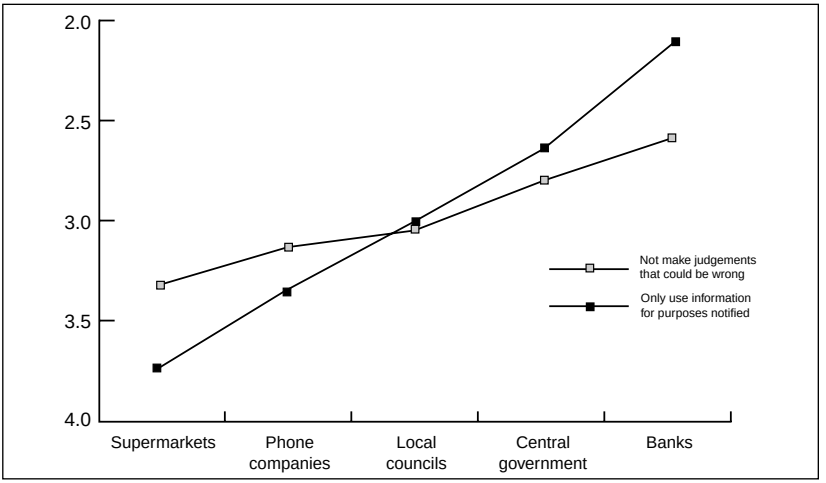

Figure 14 Average rankings for the organisations by minimal trust and goodwill trust.

As we would expect from the findings on the more specific questions on reasons and tasks, banks are the most trusted and supermarkets the least, with local government consistently occupying the mid-point.

However, the spread is statistically significantly greater on the prudential trust question than on the goodwill trust question, but the pivotal point of local councils is much the same. The weaker average ranking on prudential trust for telephone companies and supermarkets seems to be a reinforcing indicator of the provisional and fragile character of public trust in their personal information handling.

5 Reasons and tasks

The types of reason and tasks

Figure 15 opposite gives a breakdown, using just the rows of the trust matrix and the classification of reasons presented above, of the percentage of the sample choosing each type of reason, by organisation. To construct Figures 15 and 16, we combined statements on reasons and tasks using the categories set out in Chapter 3.

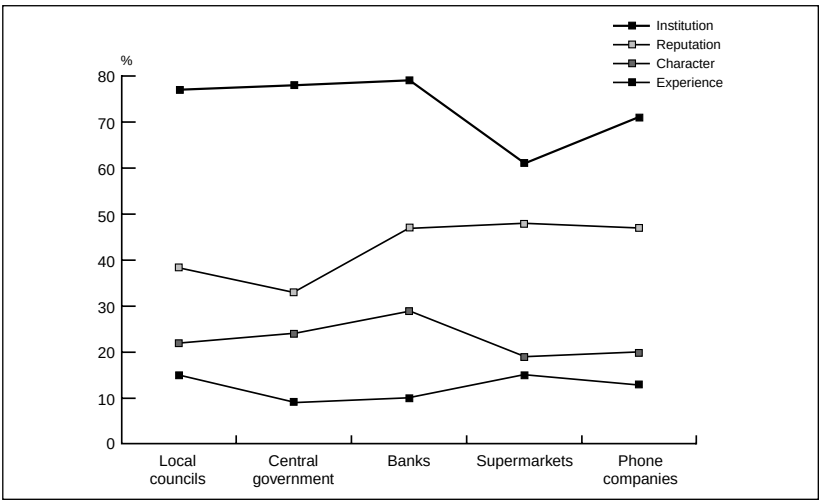

Figure 15 Percentage of sample selecting each type of reason for trust, by organisation.

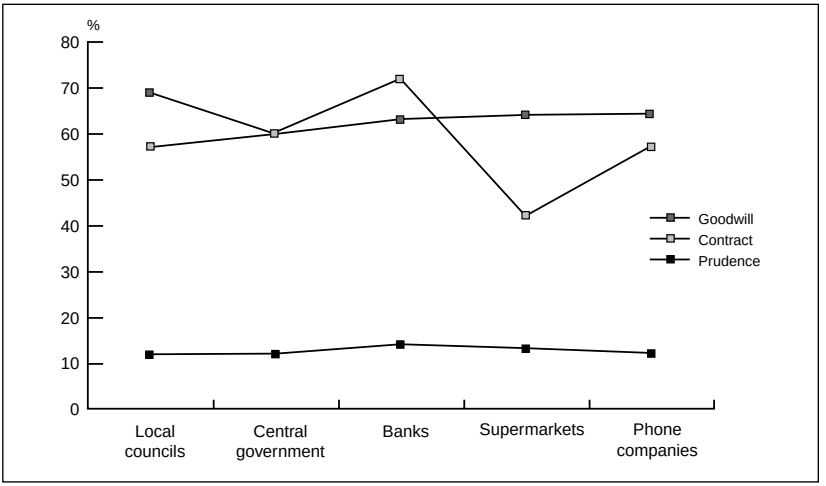

Figure 16 Percentage of sample selecting each type of task to entrust, by organisation.

As we already know, institutional reasons–of which the principal one is faith in the law – dominate and reputation matters more for commercial bodies. Figure 16 gives the same kind of breakdown for the tasks.

The low proportion choosing prudential trust partly reflects the fact that only one statement was offered under this category.

Despite the relatively high levels of confidence that seemed to emerge for banks from the top line data, it is worth noting that they attracted more contractual than goodwill trust, whereas – as we might now expect from the fact that the two are often in antithetical positions – supermarkets attracted the reverse, although the levels of goodwill trust that each attracted are not statistically significantly different.

Understanding the relationship between reasons and tasks: building the trust matrix

Having explored reasons and tasks separately, it is now necessary to bring them together in order to test the key hypothesis that people

who place goodwill trust in a person or organisation will be more likely to do so on the basis of experience than on the basis of institutional factors.

In this section, we build up the trust matrix set out in its theoretical form in Chapter 3 in a complete statistical form for reasons and tasks for trust in personal information handling, in three different tests, using correlations, cross-tabulations of percentages and fitted probabilities.

A median correlation test

The first test of the key hypothesis is one using median correlations between tasks and reasons. In this test, we cross-correlated each reason for each type of organisation with each task for that organisation and then selected the median correlations from the series within each type of reason to create a correlation for all the organisations. This is shown in Figure 17.

The median correlations bear out the key hypothesis quite markedly. The easiest way to see this is to concentrate on the extreme

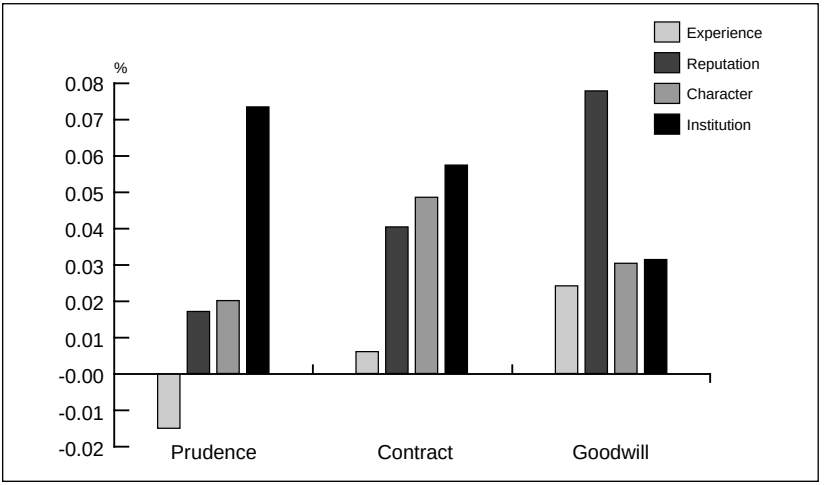

Figure 17 Median correlations of each task and reason type for all organisations

corners of the figure, where institutional and experience based reasons are related with prudential or goodwill trust. Institutional reasons for trust are most strongly correlated, at the median, with prudential or minimal trust and less so with goodwill trust, while experience based trust is slightly negatively correlated with prudential trust and most strongly with contractual and goodwill levels. Taking experience and reputation together (because reputation is in the long run determined by the experience of many people), the effect is even more markedly to link positively these reasons with goodwill trust.

A percentage test for consistent trusters

A statistically simpler but graphically more powerful way to see the link between reasons and tasks is cross-tabulation of percentages of the sample selecting types of reason, broken down by the tasks entrusted for all organisations (Figure 18) and, vice versa, types of task to entrust broken down by reason (Figure 19).

In constructing these bar charts, we try to define the standard for inclusion in the reason and task group rigorously according to the principle that we want to capture those who consistently chose a type of reason or task. However, very few people only chose one type of reason or task (for example, since there was only one prudential trust task to choose from and respondents were asked to choose their top two or three, very few people chose just that one).

Figure 18 considers all reasons selected by those who chose at least two tasks of each type for all organisations, except in the case or prudential trust, where only one task was offered.

Figure 19 considers all tasks selected by those who consistently chose a certain type of reason for all organisations. Consistent experience and reputation based trusters always chose statements from those categories. Consistent character based trusters were defined as those who chose both character statements and, similarly, consistent institutionally based trusters were defined as those who chose all three institutional statements for all organisations.

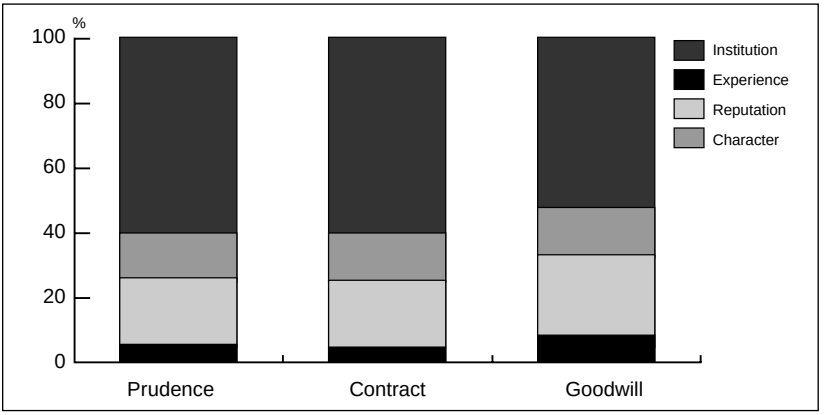

Figure 18 Percentages of the sample consistently selecting types of reason to trust, by task entrusted.

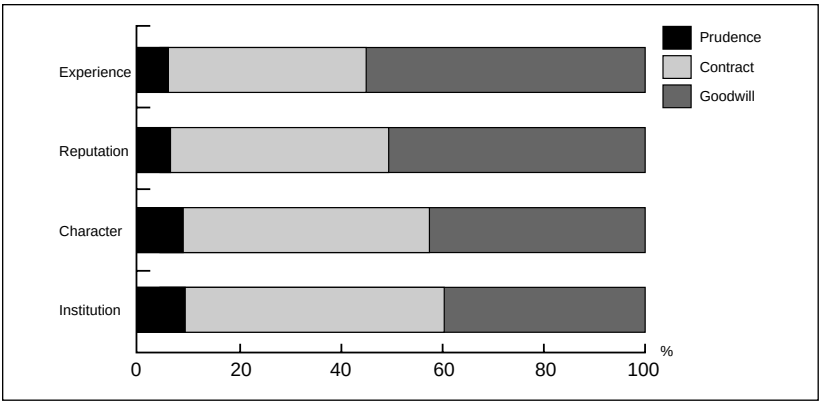

Figure 19 Percentage of the sample consistently selecting types of task to entrust, by reason to trust.

It is clear, most obviously when looking at Figure 19 of tasks by reasons, that experience based trust is more likely to be associated with goodwill trust, and institution and characteristic types of reason most likely to be associated with prudential or contractual trust. Although

the relationship appears less dramatic in Figure 18 of reasons by tasks, the same association holds.

In the second section of Appendix 3, Figures 47 to 51 give a selection of analyses of this type for the specific organisations. Figure 47 showing tasks by reasons for central government highlights a particularly strong association between institutional reasons and contractual trust and weak relationship with goodwill trust. However, exactly the same relationship is found, in slightly varying degrees of strength, for all the organisations. The differences which are in almost every case statistically significant are those between experience and institutionally based reasons, and between prudential and goodwill trust. Taking reputation and experience together, and taking characteristics and institutional reasons together reinforces the significance. The relationship is not so strong that we might put it down to response set, but it is consistently observed.

A fitted probability test

Another way to test the key hypothesis is to examine the probability that a person, having chosen principally or only a certain kind of task, will also choose principally or only a certain kind of reason.

We estimated four logit models using fitted probabilities. The aim was to estimate the probability that a person:

- if they chose an experience or reputation reason, would pick only good-will tasks, and conversely
- if they chose an institutional reason, would pick only prudential or contractual tasks.

The test involves estimating fitted probabilities, which are calculated from the maximum likelihoods estimates of the model. A fitted probability is an interpretative tool that estimates the probability, within a multivariate model, that the dependent variable has a certain value, when the independent variables have been fixed at certain values. For this test, we picked the median values for socioeconomic variables and then chose different combinations of the task variables to construct a table of fitted probabilities.[26]

For each hypothesis, two models were estimated for each of the types of organisation, using both reason and task data and the key social, economic and demographic variables of age, income, race, sex and social class. The estimation of models worked 'backwards' from tasks entrusted to reasons for trust: that is to say, where goodwill tasks were chosen, the fitted probability of also choosing experience or reputation variables was estimated, and where prudential or contractual tasks were chosen, the fitted probability of also choosing institutional reasons was estimated.

Indeed, in general and with some qualifications, the hypotheses are borne out in this test as well. We take the case of the median or typical respondent to the survey, who was 44 years old, white, female, earning between £13,500 and £15,499, and in the social class C2.

Firstly, if she chose one prudential and two of the contractual and competence tasks, then on average, she is 18 per cent more likely also to choose at least two of the institutional reasons for trust than if she chose three goodwill tasks.

Secondly, if she chooses three goodwill tasks, then on average she is five times more likely also to choose both experience and reputation reasons than if she chose the one prudential and two of the contractual and competence tasks.

The models estimated for the first part of the hypothesis (that institutionally based trusters will be likely to choose contractual or competence tasks) fitted the data better. Since three fourths of the sample chose at least one institutional reason, this is not surprising: it is much harder to find models to fit the small group that choose only experience and reputation based reasons. The averaged predicted probability of choosing only experience and reputation tasks for any individual respondent is only just above 6 per cent.

Age, income and occasionally class proved statistically significant factors. The older a respondent and their higher social class, the more likely they are to trust for experience and reputation reasons, and the less likely they are to rely on institutional reasons. However, income is an offsetting factor against social class: as it rises, the tendency to trust for institutional reasons rather than experience and reputation is reinforced.

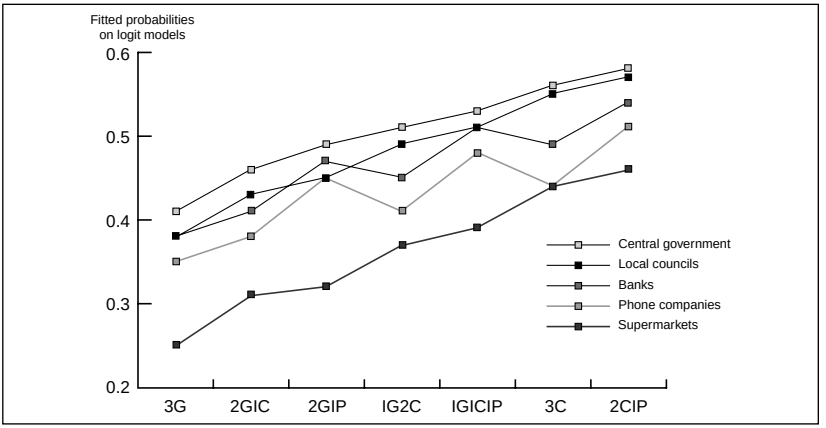

Figure 20 Fitted probabilities that the median respondent will choose at least two of the institutional reasons for trusting each organisation to handle personal information, by choice of task.

The fitted probabilities from the model that fitted the data better are given in Figure 20 above (more details on the logit models are given in the third section of Appendix 3). That the hypothesis is borne out for most organisations can be seen by observing that, in general and with some exceptions, the probabilities rise as one moves away from a choice of three goodwill tasks (3G) and towards a combination of prudential and contractual tasks (2C1P).

We can conclude, therefore, that the key hypothesis is correct. Experience based trust is much more robust than institutionally based trust, in the sense that it is statistically more likely to be associated with goodwill trust and, conversely, institutionally based trust is statistically more likely to be associated with prudential or contractual trust.

Characteristics of people who trust for particular types of reason

In this section, we focus on what our data tell us about the people who base their trust decisions principally on certain kinds of reason.

Because characteristic reasons were chosen by so few people for any organisation, we ignore them in this analysis.

Therefore, we take together people who consistently chose both experience and reputation based reasons for trust in each organisation, and contrast them with people who consistently chose at least two institutionally based reasons for each organisation. That is, we are looking here at 'consistent reason trusters', not at 'zealots' who never pick any other kind of reason at all (of whom there are very few for each type of reason). Binary variables were constructed to indicate whether an individual was or was not an experience or reputation based truster (1 or 0) and whether the individual was or was not an institutionally based truster (1 or 0).

We then conducted analyses to determine by which characteristics, both demographic and attitudinal, these positions on reasons for trust were most strongly statistically 'explained', controlling for the effect of all the variables. Analyses were conducted to estimate two sets of models for each organisation, one set for the dependent variable of consistently choosing experience reasons for trust and the other for the dependent variable of consistently choosing institutional reasons for trust. The fourth section of Appendix 3 provides examples of some of the logistic regressions on which these findings are based.

Figure 21 overleaf provides a basic summary of the differences that were statistically significant using the Chi-squared test.

As we would expect from the findings on the relationship between reasons and tasks, institutionally based trust is strongly associated with prudence and the types of contractual tasks entrusted. Moreover, the multivariate analysis confirms the findings from the percentages that older and more lower class people are more likely to trust on the basis of experience, while these are less likely to be characteristics of institutionally based trusters.

Rethinking the idea of a privacy fundamentalist

There are some people – we have already referred to them as 'zealots' – who choose only one kind of reason for every organisation and never

Organisation	*Local councils*	*Central government*	*Banks*	*Supermarkets*	*Telephone companies*
Experience and reputation based trusters	Don't mail or telephone unnecessarily	Don't use information to make judgements	Don't mail or telephone unnecessarily	Don't mail or telephone unnecessarily	Don't hold more that need to Don't mail or telephone unnecessarily Don't use information to make judgements Provide services to meet my needs (more likely to be older)
Institutionally based trusters	Tell me what they use information for (prudence) Don't disclose sensitive information without permission (less likely to be lower class)	Don't disclose sensitive information without permission Keep information secure Keep information accurate and up-to-date	Don't disclose sensitive information without permission Don't hold more that need to Keep information secure Keep information accurate and up-to-date (less likely to be older)	Tell me what they use information for (prudence)	Tell me what they use information for (prudence) Don't disclose sensitive information without permission Keep information accurate and up-to-date Provide services to meet my needs

Figure 21 Characteristics of people trusting on the basis of different types of reasons by organisation.

choose any other kind. Their numbers are small. However, there is a kind of zealot in which we are especially interested, namely those who, offered a list of reasons and of tasks, pick 'none'.

Someone who recognises none of the reasons than we offered for trust, is presumably – since we are confident that our list of reasons is, on the basis of our qualitative work, reasonably complete – someone who does not trust at all. And someone who picks 'none' for all organisations is presumably someone who would be called a 'privacy fundamentalist', using the Westin-Future Foundation segmentation. Equally, someone who picked no tasks to trust any organisation for, is also presumably a privacy fundamentalist. So, with our data, we can distinguish these two types – namely, reason fundamentalists and task fundamentalists.

Now, of course, this is a rather different and tighter definition that the Harris-Equifax and Future Foundation ones. Harris-Equifax use questions such as 'how concerned are you about privacy?' combined with a battery of questions about views on the seriousness of particular risks. The Future Foundation used questions of the form 'I am happy to provide information to …?' and offered scales of agreement, together with similarly structured questions about rewards expected for the provision of information. Both those surveys found that about 25 per cent came out as fundamentalists on their definition.

Defining a privacy fundamentalist in the way that we can produces, we believe, a more thought-out response, because the respondent has been confronted with a set of reasons and tasks on a showcard and asked to think about how much each weighs with her or him. The more thought-out response may, of course, not be the same as the response that the individual would give in the high street or in the government office. However, with the opportunity for this kind of reflection, dramatically fewer people report themselves to be reason or task fundamentalists than report themselves to be fundamentalists on the Harris-Equifax or Future Foundation definitions. Indeed, of our sample of 2,018, there were just 32 reason fundamentalists (weighted number; that is, 2 per cent) and 54 task fundamentalists (we ghted number; that is, 3 per cent). Of course, it does not follow that one definition is right and another wrong, but it does suggest that we need to

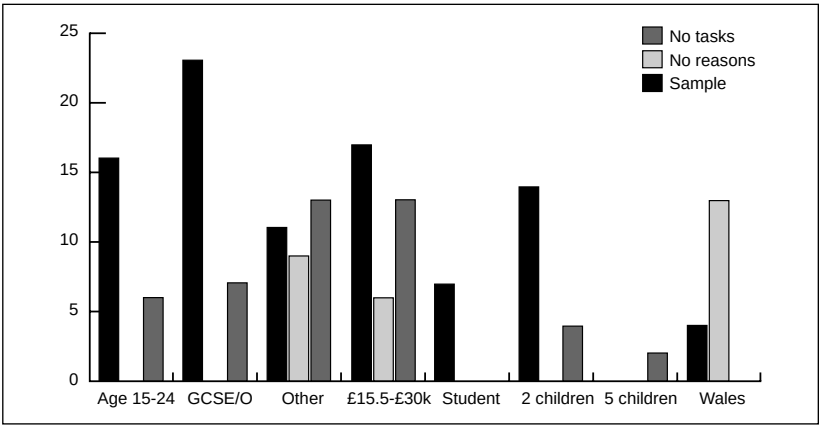

Figure 22 How reason and task fundamentalists differ from the population as a whole.

use a number of different ways of measuring privacy fundamentalism before making confident statements about its scale and its demographic profile.

What, then do we know about privacy fundamentalists in Britain? The Future Foundation found a cluster of people who were generally untrusting except for their GP and were likely to be in the younger half of the population, in the 25 to 44 age bracket. To compare with these findings, we broke down our tiny group of fundamentalists by simple percentages in the main sociodemographic categories and then compared the breakdown with the sociodemographic profile sample as a whole, to identify those percentages that were statistically significantly different. Figure 22 lists the percentages that were statistically significantly different.

The profile of our reason and task fundamentalists then is rather different from the Future Foundation's NewInfo Trade privacy fundamentalists in that they are actually less likely to be in the youngest cohorts aged between fifteen and 24. As we knew from the earlier review of demographics, they are more likely to live in Wales. They are more heavily concentrated among single people and among those with

Reason	*Absolute weighted numbers*	*Over-represented*	*Under-represented*
Law requires	507	Income: over £15,500 Socioeconomic class B, C1 Full time work Education: first degree	Age: over 65 Education: no formal qualifications Income: under £7500 Socioeconomic class: D,E Age: over 65
Damage to reputation	273	Age: 35-44 Income: £15,500-£29,900 Part time work Age: 35-44	Education: no formal qualifications Age: over 65
Written agreement	198	Income: £15,500 + Socioeconomic class B Full time work Education: first degree	Education: no formal qualifications Income: under £7500
Public commitment	68	Income: 15,500-£29,999 Full time work	Housewives
Task			
Don't disclose information without my permission	138	Age: 45-54	Age: 15-25 Students Children: none
Use to provide services to my needs	104	Sex: female Education: first degree	Age: over 65 Sex: male

Figure 23 How reason and task zealots differ from the population as a whole.

non-standard education who have achieved middling levels of income. Naturally, with such a small absolute number of people, it is unwise to place great weight on these demographic profiles. However, they do suggest that privacy fundamentalists may be under-represented in the younger, more metropolitan, highly educated segments.

Other kinds of zealot

Other kinds of zealot means those who choose a reason or a task consistently for all organisations. While the absolute numbers of zealots are very low (with the exception, as we would expect from the top line findings, of zealots for legal obligation), it is worth briefly noting some of their social characteristics. Figure 23 summarises the statistically significant differences from the sample as a whole, but only for those reasons and tasks where there are such significant differences.

In general, the zealots about particular reasons and tasks are middle aged, middle income groups, in work, with reasonably good education. Gender is significant only in the tailoring of services to personal needs, with women being significantly more likely to have confidence in this for all organisations.

The fact that the absolute numbers of zealots are very low and that the profile of those over-epresented among these groups is not those who are poorly educated provides substantial reassurance that the meaningfulness of the data as a whole is not damaged by the problem of response set.

6 High and low ranking trust

Constructing the categories

In this chapter, we explore in more detail the information that can be gleaned about who ranks which organisations high and low in the prudence task and the goodwill task about avoiding inferences that could be unjust, how they differ in their sociodemographic characteristics and the reasons and tasks for which they place trust in organisations.

We begin by constructing our dependent variables. We shall call them 'high ranking trust' and 'low ranking trust'. A respondent has high ranking trust in an organisation if they ranked that organisation either first or second in both questions. Conversely, they have low ranking trust in an organisation if they ranked that organisation fourth or fifth (last) in both questions. Clearly, this is not a completely general measure of high trust, because it combines just the prudence task and one goodwill task. However, it provides a rough proxy for trust in an organisations' ability to handle personal information properly. Therefore organisations of each of these kinds will be interested to know more about those people who are high and low ranking trusters in them, because this will tell them a good deal about their potential willing clientéele and those who are most likely to be resistant clients, in terms of personal information handling.

Figure 24 gives the percentage of the total sample that they represent and Figure 25 gives the percentage difference between the two. The percentage difference is a very crude measure of the relative distance in trust in each organisation in this group of five types.

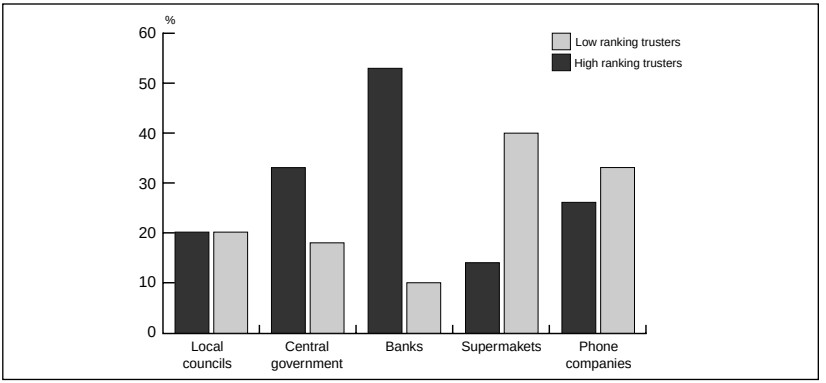

Figure 24 High and low ranking trusters in the organisations.

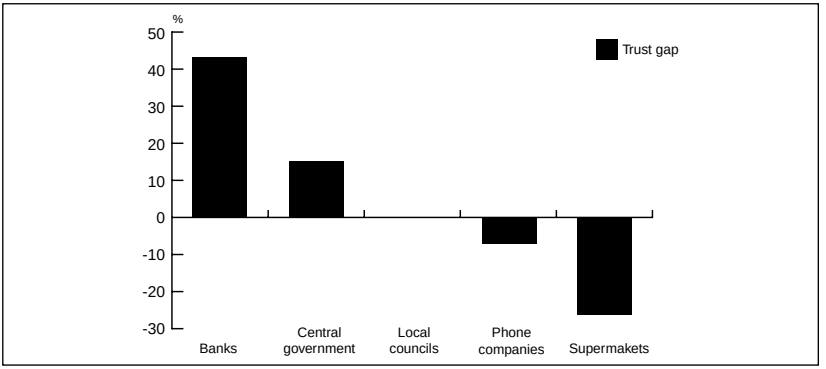

Figure 25 Gap between the percentage of high and low ranking trusters.

Figure 25 simply confirms the top line' findings on rankings, that local councils occupy an intermediate position between the extremes of very low trust in supermarkets and very high trust in banks.

Part of the interest of these data is that they show a rather different picture from that offered in the Henley Centre's *Dataculture* report, which used a gap analysis (see Figure 5 above), or a deduction between the percentage of the sample believing the organisations to hold data on them and the percentage that was happy to provide those organisations

with personal data as a proxy for high and low trust. The Henley finding was that the greatest gap (that is, negative indicator) was for the public sector combined, the second greatest gap was for banks, while supermarkets performed relatively well: telephone companies were not disaggregated from other utilities, which showed a modest gap.

On balance, we believe that our indicator has some merits over the Henley one and the very different ranking that it produces may be more valid and reliable. Firstly, the gap between knowledge of the holding of personal information and happiness about providing it is at best a very indirect indicator of trust. It is extremely sensitive to differences in people's awareness of data being collected For example, the very large gap indicated by the Henley data for government may simply reflect the widespread public understanding that government engages in a variety of data collections rather than generalized distrust.

Secondly, the Henley questions used in the gap analysis do not deal directly with the questions of data handling and are entirely lacking in information about people's views on specific tasks or privacy risks. By contrast, our ranking questions were asked after all the information on reasons and tasks had been collected and focused on a prudence and a goodwill task respectively. Thus, respondents had been prompted to give some thought to their views, and the rankings do focus on specific tasks. Moreover, the ranking of organisations that we secure in these data is consistent with those obtained by the Office of the Data Protection Registrar in the its eighth report.[27] In that 1989–92 survey, banks scored well, 'shops and stores' rather badly and a variety of public sector agencies rather well, using a deductior of the percentage dissatisfied that the organisations could be trusted to use personal data in a responsible way from those satisfied.

Reasons and tasks for high ranking trusters

First, we need to know about the high and low ranking trusters from the ranking questions, what kinds of reasons and tasks they chose on those questions. Figures 26 (on page 92) and 27 (on page 93) provide this information.

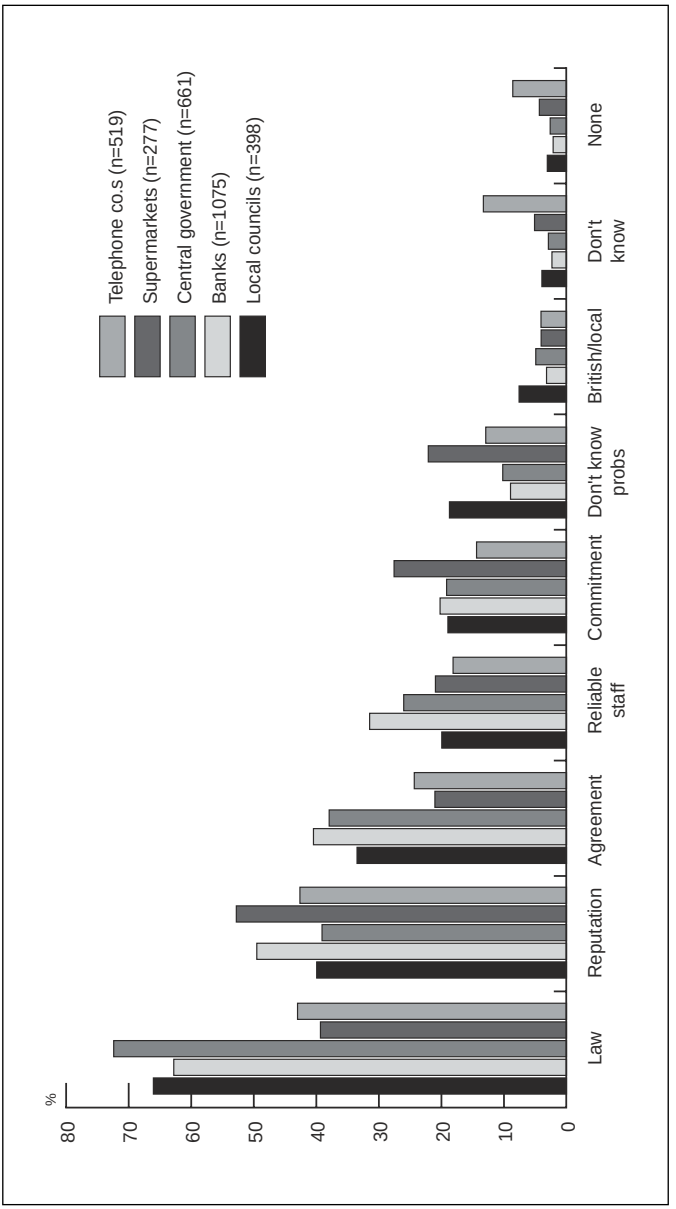

Figure 26 High ranking trusters' reasons for trust, by organisation.

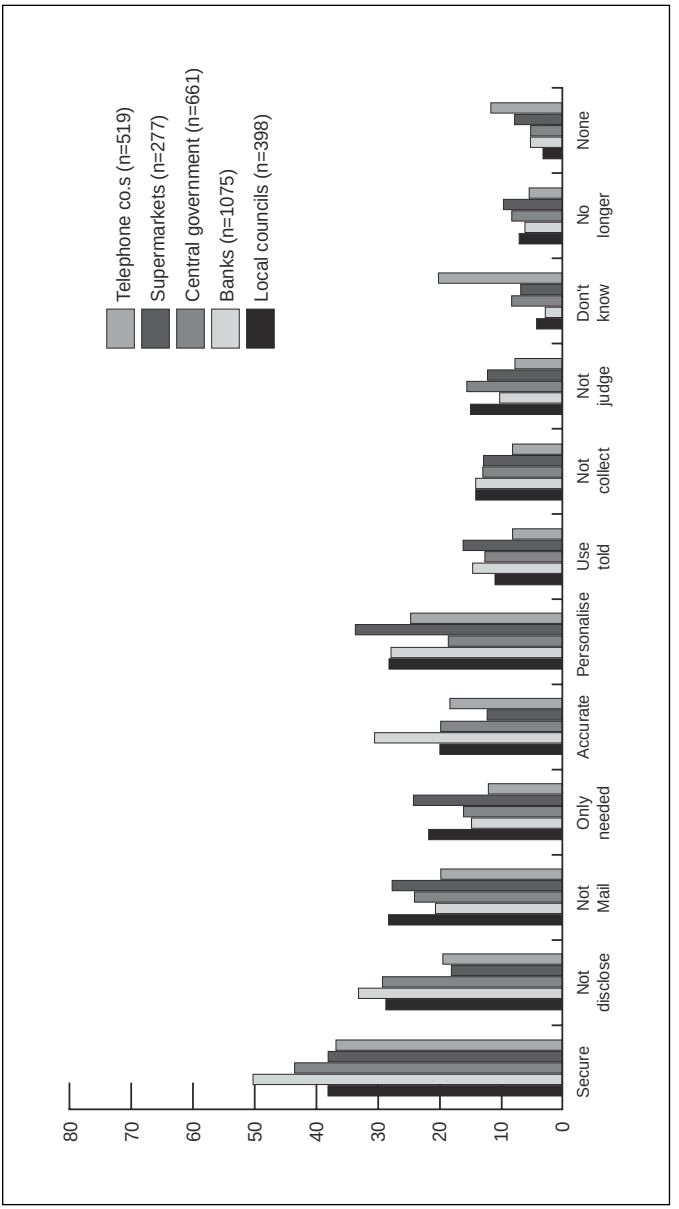

Figure 27 High ranking trusters' tasks entrusted, by organisation.

Taking the reason and task profiles of high ranking trusters together and comparing them with the reason and task profiles of the sample as a whole, which were given in the 'top line' results in Chapter 4 (Figures 12 and 13), it is clear that the high-ranking trusters are similar to the sample as a whole. With the exception of one organisation, the high ranking trusters show the same (that is, differences are not statistically significant) or slightly greater more likelihood of choosing most reasons and tasks than the whole sample.

That exception is the telephone companies. For them, high ranking trusters are between one and five percentage points less likely than the sample as a whole to choose each task and the reputation legal duty, written agreement and public commitment reasons. It is not clear to us how to explain this. The differences are not huge and not in all cases statistically significant. However, the consistency of the finding across all tasks and on the reasons that are most important for the population as a whole and the fact that this occurs only for telephone companies suggests that high ranking trust in telephone companies may be less solidly grounded than high ranking trust in other kinds of organisations.

Reasons and tasks for low ranking trusters

In order to understand the implications for the organisations under scrutiny, we need to compare the high and low ranking trusters. For if they turn out to place their trust for quite different reasons or entrust quite different tasks, this will tell strategists in these organisations something of importance.

Figures 28 (on page 95) and 29 (on page 96) give the breakdown of the low ranking trusters by reason and tasks respectively.

Comparing high and low ranking trusters with each other and with the whole sample, a number of differences emerge. All the following differences between the high and low ranking trusters in each organisation are significant at the 5 per cent level.

High ranking trusters in local councils have significantly higher faith in the reliability of council staff and in the reputation effect for local authorities than do low ranking trusters in these organisations.

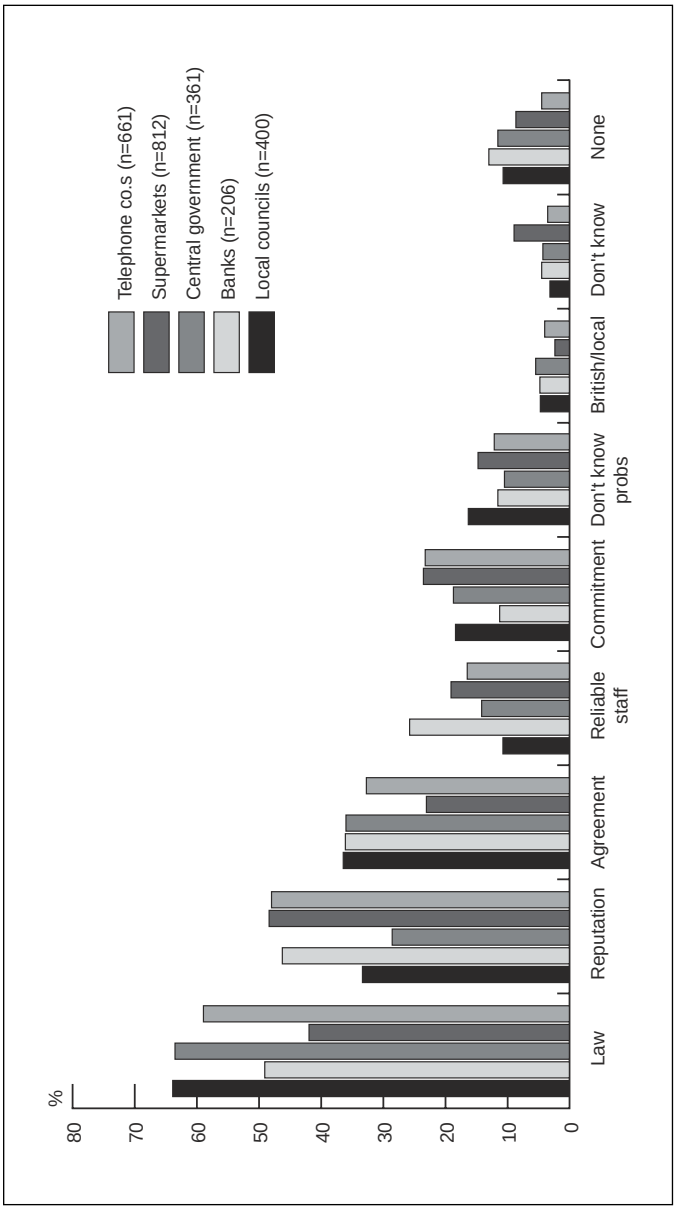

Figure 28 Low ranking trusters' reasons for trust, by organisation.

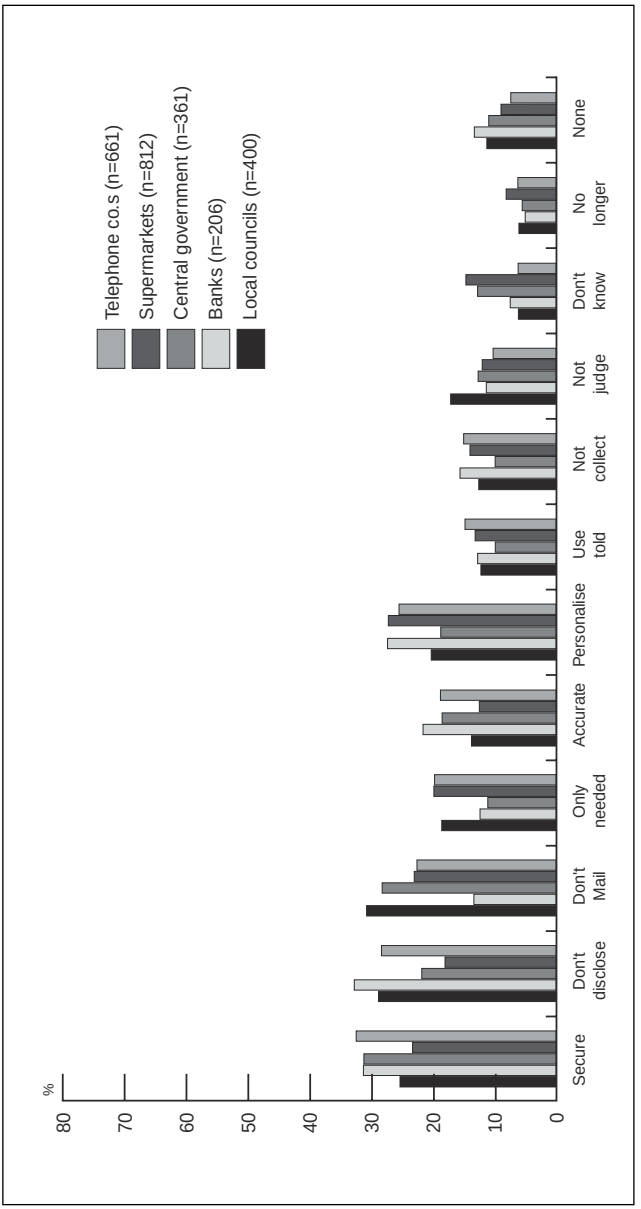

Figure 29 Low ranking trusters' tasks entrusted, by organisation.

On the other hand, slightly fewer high ranking trusters in councils put their faith in written agreements than did low ranking trusters. On tasks, high ranking trusters were more likely to stress their confidence in security, accuracy and tailoring services to personal needs than were low ranking trusters.

In respect of reasons, central government occupies a position somewhere between banks and local authorities, for high ranking trusters differed from low ranking ones in their faith in the law and reputation effects and in staff reliability. On tasks, high ranking trusters respected central government agencies' capacity not to disclose without permission, keep data secure and not keep more data than necessary more than low ranking ones did.

By contrast, high ranking trusters in banks differed from low ranking trusters principally in that they placed significantly more faith in institutional reasons for trust. High ranking trusters in banks were more likely than low ranking trusters to place confidence in banks' security, accuracy and avoidance of unnecessary mail and telephone calls.

High ranking trusters in supermarkets are more likely than low ranking trusters to choose experience reasons and to stress personalized services.

Just as high ranking trusters in telephone companies seemed, paradoxically, to be less trusting of them than the sample as a whole, so the low ranking trusters for telephone companies seem to have higher trust in most reasons and tasks entrusted to them than the sample as a whole. In particular, low ranking trusters in telephone companies had greater faith for institutional reasons than did high ranking trusters. Again, on tasks, low ranking trusters in telephone companies were more likely to have confidence in the companies to tell them what use is made of information, not to collect from elsewhere or disclose without permission, keep data secure and not to keep more than necessary. Perhaps this simply reflects a belief that, when reasons for trust and trust in the handling of particular task are generally weak, there is only the law to rely upon.

As we would expect, for most organisations, low ranking trusters are more likely to choose 'none' of the reasons and 'none' of the tasks

offered than high ranking trusters or the sample as a whole. However, consistent with the finding that high and low ranking trusters in telephone companies behave in ways that are hard to understand, actually more high ranking trusters in telephone companies chose 'none' of the reasons and 'none' of the tasks.

The demographic profile of high and low ranking trusters for the organisations

Figure 30 summarises the principal sociodemographic characteristics that are over– and under–represented in the high and low ranking trust groups for each kind of organisation.

Taken as whole, these findings could be read as suggesting that in some measure people have contact with the organisations they first trust or that people tend to place trust in organisations when they have a great deal to do with them, perhaps because they feel they have to (psychological

Organisation	*Over-represented in high ranking trust*	*Under-represented in low ranking trust*	*Under-represented in high ranking trust*	*Over-represented in low ranking trust*
Local councils	Socioeconomic class E Income: less than £7500 Unemployed	Age: 75 and over	Income: £15,500-£29,999	
Central government		Region: north	Age: 15-24 Students	Region: south
Banks	Age: 55-64 Socioeconomic class C2 Retired		Education: degree or higher	Education: masters or doctoral deg. Unemployed
Supermarkets	Age: 15-34 Region: south	Students Region: south, esp. London	Region: north, East Midlands	Region: north, East Midlands
Phone companies	Region: Wales	Age: 15-34 Students		

Figure 30 How high and low ranking trusters differ from the population as a whole.

theorists might suggest that the reduction of cognitive dissonance would explain this): no doubt the two processes reinforce one another. For example, the clientéle of local council service is disproportionately elderly and poor, and these appear to be the people who are more likely to be high ranking trusters and less likely to be low-ranking. Again, the most active day-to-day users of the face-to-face services of retail banks are, in practice, the lower middle class and older people: the poor tend not to use banks much and the rich tend to have other ways of handling their resources. Interestingly, however, as education level rises, people seem to have less faith in banks data handling. Supermarkets, like much of the high street retail economy, are most trusted by the most confident, actively consumerist group in society, which tends to be found most among young people and those living in the south of the country. However, as we shall see, this explanation is not without problems.

High and low ranking trusters: a multivariate test

All these results on high and low ranking trusters have used simple percentages. Because of the importance of understanding high and low ranking Trust, it seemed worth checking the bivariate comparisons and differences by using a multivariate analysis that would control for the effects of the variables upon each other, in order to be able to describe the profiles of these groups with greater accuracy.

Therefore, we constructed binary variables indicating whether or not an individual exhibited high ranking trust (1 or 0) for each organisation and whether or not an individual exhibited low ranking trust (1 or 0) for each organisation. We then conducted a series of logistic regressions in which the following list of controlling and explanatory variables of high and low ranking trust:

- all the attitudinal variables on reasons and tasks for the relevant organisation (but not for any other organisations and not the rankings of organisations), and
- the sociodemographic variables of age as a continuous variable and income by brackets, degree level education, sex and socioeconomic class.

The fifth section of Appendix 3 provides examples of some of the logistic regressions on which these findings are based.

Figure 31 below provides a basic summary of the differences that were statistically significant at the 5 per cent level using the Chi-squared test.

In general, for the organisations that are in any case more highly trusted – namely, banks, central government agencies and local councils – the most powerful predictors of high ranking trust are believing in the reliability of staff and that the organisation keeps

Organisation	*High ranking trust more likely*	*Low ranking trust less likely*	*Low ranking trust more likely*	*High ranking trust less likely*
Local councils	Keep secure Lower socio-economic class Higher education	Reliable staff Older	Resaons: none	Tasks: none Tasks: don't know Higher income
Central government	Reliable staff Keep secure Not hold more than need Older	Reliable staff Older		Reasons: none Reaons: dont' know
Banks	Reliable staff Keep secure Class C2	Keep secure	Reasons: none Tasks: none Higher education	Dont' know of problems Higher education
Supermarkets	Male		Keep secure	Tasks: don't know Older
Phone companies	Reliable staff	Service to meet my needs Tasks: don't know	Older	Public commitment Legal duty Tasks: don't know

Figure 31 Reason, task and sociodemographic factors making high and low ranking trust in each organisation more and less likely.

information secure, while for the commercial organisations, as the Future Foundation research suggests, tailoring services to meet people's individual needs is important, but supermarkets are still not convincing people that they are doing this yet.

By contrast, for low ranking trust, sociodemographic factors are more important (since choosing 'none' for reasons and tasks is, presumably, logically related to low ranking trust rather than being a plausible causal explanation for it). In general, for the widely trusted organisations, low ranking trust seems to become more likely as education and income rise, while for the less trusted commercial organisations, older aged groups are more likely to show low ranking trust.

7 Understanding and using public trust

In this concluding chapter, we offer an interpretation of these findings. Firstly, we return to the questions with which we began – how important is privacy to the public and what exactly is important? Secondly, we consider some more sceptical hypotheses about the importance of trust. Thirdly, we consider whether our cross-sectional data suggest any ways in which these attitudes might change in the foreseeable future. Finally, we examine the implications for the strategies of business and government agencies.

Interpreting the findings

With these data, we are able to enrich greatly our understanding from previous research on public trust in the ability and willingness of organisations to respect privacy.

What privacy risks does the public feel concerned about?

We can now offer a much better answer than previous surveys of the British public have been able to, to the question with which we began – namely, just how important is privacy to the public at large?

We found as we used our qualitative findings to design the survey that the best way to tackle this question is to distinguish between different kinds of privacy risks and examine public concern about them.

The general finding is clearly supported that some risks are much more important to people than others. Our survey enables us to reject comprehensively the idea that the public is lacking in discrimination about the risks that people face (tasks) or about the kinds of factors that make for trustworthiness among organisations that handle personal data. It is clear from our qualitative work that the public is not in every case well informed about the type and range of privacy risks that the handling of personal data by different kinds of organisations presents. But, as a people become more aware of these risks, in many cases, they care more about the issues raised and are well able to discriminate between the risks that worry them and the risks that do not.

From the survey findings and from our focus groups, it is clear that among the privacy risks that most people recognise and understand is *Pestering* – that is, unnecessary mail and calls. But a simple practice of restraint in pestering is not sufficient to reassure the public that personal data is being handled properly. If we examine the tasks that reassured high ranking trusters, we find that this group is most likely to stress keeping information secure. By way of confirmation of the importance of this, the most trusted organisations were banks and the single task that attracted the largest group of the sample as a whole for any organisation was keeping information secure for the banks (43 per cent), while for the least trusted organisations – namely, supermarkets – only 18 per cent of the sample stressed confidence in their performance of this task. It seems reasonable therefore to conclude that information security is very high on the public's list of privacy risks of concern.

Other risks that seem to be high on the public's list of priorities are disclosure of sensitive information without permission and accuracy of information.

Although the survey does not suggest that it is the single greatest concern of the public, there is a steady current of concern about the making of inferences about individuals which go beyond the strict implication of the information before organisations and which may lead to unjust decisions about entitlement or treatment. We had great difficulty in framing a description of task that would avoid this risk, which would not lead respondents to choose it. We are concerned with

what, in Volume 1, we call 'unjust inferences'. Had we put the issue to the sample in those terms, it would no doubt have seemed sufficiently alarming to have attracted many more to pick it. Probably, the wording we finally chose is so anodyne that the results understate the levels of public concern here. Our qualitative work, for example, suggests strongly that people are concerned about decisions of entitlement and treatment being made on the basis of inferences from informations.

It was for this reason that we decided to use this as the 'goodwill trust task' on which to seek ranking information about organisations. Our analysis of high ranking trust in an organisation suggests that in the minds of many of the public, there is the straightforward and entirely reasonable proposition that the only real safeguards against unjust inference and restricted use are the ethics of the staff and the formal procedures for data handling.

We know from previous surveys, and in particular from the work of the Future Foundation, that a majority of the population are willing to trade some personal information for some enhancement of service. The survey shows clearly that this is an important factor for a significant proportion, both for the sample as a whole and for those who place high ranking trust in organisations. Moreover, it is clear that when privacy fundamentalism is measured as accepting none of the main conventional reasons for trusting any organisation, and trusting no organisation to carry out any task that would minimise the main privacy risks, then there are very few privacy fundamentalists indeed.

But this finding needs to be set in the context of the survey as a whole. The mistake that many of the more complacent business and technology analysts make when they point to information of this kind is that they assume that privacy pragmatists can be treated as if they were unconcerned or at least bought off with some enhancements of service.

Our survey shows that this is simply not the case. The organisations that have made the greatest strides to offer the most personalization of service are the telephone companies, through such schemes as BT's 'Friends and family' and the supermarkets, through the targeted special offers based on information about purchases collected from till

receipts through individuals' loyalty cards. The public understands that they have made strides in this direction: these organisations score more highly than others on the task of designing service to meet individual's particular needs.

Yet our survey also shows that supermarkets are the least trusted and, while telephone companies achieve a slightly better mean ranking on both ranking questions, the analysis of the high and low ranking trusters in telephone companies strongly suggests that trust in these organisations is not robust. Personalisation of service to individuals' particular needs does not cancel out or override concerns about other kinds of privacy risk.

Why does or would the public trust organisations to respect privacy?

In general, it was clear from the qualitative work that public trust in organisations' ability and willingness to handle personal data with respect for privacy is not strong. While the survey reports larger numbers choosing legal duties as the main reason for confidence, it does not follow that they have much confidence in the enforceability of or voluntary compliance with the law, or that many people feel much confidence in their own ability to use it. Rather, our qualitative work and these data suggest that the finding reflects the lack of any great confidence in anything else.

Moreover, we have been able to confirm the hypothesis that goodwill trust is statistically more likely on the basis of experience, despite the relatively smaller proportion of the sample who do their trust in this way. This suggests that organisations should design their strategy for trust management on the basis of offering their clients the chance to see for themselves that their personal information is well used, thus putting their reputations on the line.

While the bare survey data do not suggest that staff reliability is a particularly important reason, the analysis of the high ranking trusters gives it an importance that the coarse aggregate data do not reveal. The results suggest that high levels of trust will be secured in many organisations

only when they can offer the public clear reasons to think their staff reliable.

Trust, esteem, contact and resignation

The skeptics and the complacent about trust sometimes argue the following propositions:

- people trust organisations to do particular things not so much on the basis of a rational assessment of whether they think the organisation is willing and able to do the particular task but on the basis of whether in general they have high esteem for the organisation.
- people will come to trust any organisation they must deal with because the cognitive dissonance of placing oneself in the hands of an organisation that one does not trust is simply too great a psychological strain for most people
- people are more resigned and fatalistic than trusting because they know that real power now rests with organisations, not with them, and so it is not very important whether or not they trust.

Each of these propositions has some support from our qualitative and quantitative work and none can be dismissed out of hand. For example, the high trust in banks seems to reflect other survey data on general esteem for banks, just as the Data Protection Registrar's tracking survey found that people had high trust in personal handling by their GP and this seems to correlate with high general esteem for GPs.

Our sociodemographic profile of high ranking trusters in local authorities, banks and supermarkets seems very similar to the profile of those who use them most, in some cases (at least in the case of local councils) because they have to. And in the focus groups, we did hear evidence of a widespread resignation, confirmed in such surveys as the Harris-Equifax annual consumer privacy study of the US population, that people are fatalistic about their chances of gaining control over the use of personal information about them.

However, none of these statements is wholly borne out and, even if they capture some element of public opinion, none represents the whole truth. First, it is not clear how to make these three statements consistent with each other, unless the claim in each is restricted to some distinct segment of the population. Those who are fatalistic or resigned about the power of an organisation presumably cannot logically place it in very high esteem. Again, it is not clear how one can be both gloomily fatalistic about an organisation and at the same time reduce one's cognitive dissonance about dealing with it.

Second, while the direction of a causal relationship may run from esteem to trust in the case of banks and GPs, it is not clear that it does in the case of, say, central government agencies, which attract very low public esteem in general, according to other surveys, or of telephone companies, which attract quite high esteem.

Third, the story about the reduction of cognitive dissonance yielding high trust ought to work best in the context of monopoly organisations, where people have little or no choice but to use them. But the data do not bear this out, save in the case of local authorities. BT still has a near monopoly in residential wired telephony, yet the telephone companies attract rather low levels of trust. In many areas of the country, choice of supermarkets is limited to a local duopoly which has driven out alternative small local suppliers and the supermarkets attract very low trust.

Fourth, if trust were little more than a positive re-description of fatalism, then it would be very difficult to make sense of the sociodemographic profile of the high ranking trusters in supermarkets. High ranking trusters in supermarkets are generally the younger, more affluent groups in the southern half of the country who are in general more consumerist in their values, more confident in their ability to negotiate a reasonable deal for the surrender of personal information and are the least likely to be fatalistic about their relationships with large organisations.

Finally, the fact that large proportions of the sample picked reputation as an important reason for trust, even in public sector bodies which are not subject directly to market forces, as well for oligopoly

private sector organisations, suggests that fatalism about the capacity of public opinion to influence the behaviour of large organisations is not the majority view. While people may take a very realistic view of their own power as individuals to change the behaviour of large and powerful bodies, they clearly feel that the public collectively has some influence.

At best, then, these statements might explain some special cases within the group of organisations and the attitudes of some segments of the population, but cannot provide a general account of the findings. The error that underlies each of these statements, when they are made as general accounts of public attitudes, is the same as above – namely, a complacency that public attitudes are of rather low importance, that most people's regard can be bought relatively cheaply. In part this mistake flows from too much focus on the reasons for trust and too little attention to the findings on tasks or perceptions of risk.

Possible future trends in public trust

Developing scenarios about future trends in attitudes from cross-sectional data is always risky and needs to be set about with heavy qualifications. Such future scenarios are vulnerable to all kinds of social change, particularly when they concern not fundamental values that change slowly and in relatively predictable ways[28] but specific attitudes to risks associated with and reasons for faith in particular organisations.

One straightforward way to develop scenarios is to posit the operation of some well-understood mechanisms of attitudinal change. The following are the ones that are most obviously relevant:

- *Cohort replacement.* There are some attitudes that, once formed in youth, remain with individuals for most of their lives, but which differ between cohorts. Thus, as older cohorts die off and younger cohorts age, some attitudes that are typical of a wide span of the younger cohorts may become dominant across the whole society.
- *Generational change.* There are some attitudes that are typically adopted by a cohort in youth, toned down on

marriage, house purchase or securing a regular job and income or in middle age and for the most part abandoned by retirement.

- *Gradual adaptation to experience.* There are some attitudes that are gradually adapted, revised or abandoned in the light of experience, as people observe changes taking place in the economy, politics and society.
- *Sudden polarization/convergence in response to conflict and shock/settlement.* Events can shape some attitudes by exacerbating divisions between different segments of the population, or by healing such divisions.

Examination of the differences between age groups in our survey shows that those under 34 were, in general, less likely than those over 55 to pick 'don't know' and 'none' in answer to the questions on reasons and tasks. They were more likely to have confidence in commercial organisations and less likely to place high ranking trust in central government than were older people. However, these differences are not very marked and the differences for many individual reasons and tasks are not statistically significant.

Is this greater confidence likely to remain with these cohorts and become dominant, to be displaced by the normal course of life events, revised in the light of experience, or subject to polarisation or convergence?

The attitudes that remain with cohorts and become dominant by replacement tend to be those that reflect fundamental values rather than empirically revisable views on particular organisations. Therefore, a simple roll-out of the greater confidence of the young seems unlikely.

There are some life events that bring people into contact with certain organisations and require the provision of personal information. For example, the payment of taxes, acquisition of mortgages, life insurance, even personal pension plans for the better off, the encounter with the personal data handling of employers is more likely to face those over 25. In fact, the crosssectional differences between the under and over-25s are not for the most part dramatic.

Therefore, it seems most likely that views on reasons and tasks for trust will be the kind of attitudes that will be revised in the light of experience. Whether that will be gradual or sudden depends in some measure on the strategies of the organisations that collect and use personal data. However, we can say from out qualitative research that people tend to become more aware of privacy risks, but rather gradually so. Sudden changes in strategy by business and public sector bodies tend to filter down gradually to the public. For example, despite the large scale take-up of supermarket loyalty cards, we found that public understanding of the privacy issuses raised was limited and unevenly distributed.

Therefore, one plausible scenario for the future of public attitudes in this area, if business and government strategies in personal data handling remained as they are today, is that awareness of risks will gradually heighten and consumers and citizens will gradually become more demanding about the terms on which they will trade personal information.

Implications for the organisational strategies

We have argued throughout this report that there are reasons why public and private organisations should take public trust in their personal data handling seriously, and should positively seek greater public trust in this regard. Volume 1 sets out more detailed general recommendations on ways forward. However, a few specific points are appropriate here.

Organisations seeking higher public trust can take little comfort from the high proportion of our respondents stressing the law. A deeper look at the data suggests that, in fact, among the most important areas for strategists to work are:

- how the organisation is experienced in the tasks it carries out to minimise key privacy risks
- how reliable its staff are believed to be
- how it takes care of its reputation.

Public commitments such as codes of practice and specific written agreements with individual clients clearly have an important role to play in reassuring many people, but strategists need to find ways of showing people how personal data is used. In a previous publication, we argued for organisationally independent means of securing subject access,[29] which would be a start; the Future Foundation survey also found that it would be popular.

On this analysis, then, staff training in the handling of personal data to avoid those privacy risks which are of particular public concern, in the implementation of codes of practice and in the requirements of the data protection legislation, seems to emerge as a high priority.

Many organisations make more effort on security and accuracy than in the reduction of other privacy risks. Our data suggest that the public clearly welcomes these efforts. However, it would be a misreading of the data to concentrate on these alone. Other tasks that may have attracted lower proportions of the sample nonetheless reflect important latent concerns. In particular, the avoidance of unjust inferences in the use of personal data is a key risk, which may rise up the public agenda as the use of geodemographic profiling tools together with new technicques of data matching and data mining in order to make decisions on entitlement and treatment. The development of codes of practice provides an institutional reason which may not, of itself, be particularly powerful, but if the implementation of such codes can be brought to the attention of consumers and citizens, then it may feed into experience and reputation and hence into trust.

Conclusions

Privacy is an important, if partly latent, concern for the British public. It matters, it almost certainly does influence behaviour, and organisations that are complacent about it will face real costs, albeit gradually. Moreover, the public is quite discriminating in its perception of risks and the weight it places on different reasons for placing confidence in organisations, despite not being perfectly informed about the risks it faces or the organisational imperatives behind the use of personal information.

Despite the generally low esteem in which government is held, public sector bodies do not start from a particularly low base of public trust in personal data handling. Whether an organisation is in the public or private sector is not an important factor for most people in making their trust decision.

The conventional segmentation of the population into privacy pragmatists, privacy fundamentalists and the unconcerned does capture something real. However, when we look more deeply at the unconcerned (as we did in our qualitative work) and the fundamentalists (as we did in the analysis of the survey data), the conventional analysis seems less than wholly accurate. The fundamentalists, who see only risks and no reasons to trust, are very few indeed. Many of the unconcerned seem more fatalistic than positively trusting. This suggests that most of the population – a larger proportion than previous surveys have identified – are privacy pragmatists. But because such a label applies so widely, it means rather little. Certainly, it does not mean what many of the more complacent business and government strategists have taken it to mean – namely, that their concern can be bought off and their trust gained with a few simple enhancements of service.

Most people are willing to provide some kinds of personal information in return for some enhancement of service. But it does not follow that, given that improvement in service, they no longer have any concerns about how their personal information is used. Younger and more affluent groups within the population are more confident that they can make the right trade-off in such negotiations, but they are also the groups with the more institutionally based trust, which is significantly less robust.

The existence of the legal duties enshrined in data protection legislation are important to a majority of the British population and provide some reassurance. However, few people are particularly literate in the use and enforcement of the legislation and very few regard it as a sufficient protection of their legitimate interests in their personal information.

Understood carefully and sensitively, the public mood on privacy should give business and government agencies pause to reconsider

their strategies and to question the widespread complacency that privacy is no longer of any real importance. Moreover, the public mood can be used to guide the development of strategies to build public trust. Codes of practice, staff training, clear procedures for ensuring that privacy risks are minimized and greater transparency in the uses to which personal information are put are all possible and would be welcomed by a majority of the public.

Different types of organisations face different challenges, and benchmarking exercises between different industries should be designed with some care if they are to be relevant. However, there are some lessons that the organisations that face low public trust can learn from those which have secured higher public trust, about the relative importance of different reasons for trust and tasks entrusted. As their positions seem to be poles apart in this survey, perhaps supermarkets could consider whether there are lessons to be found in the best practice in the banking sector.

The British public will remain an important and an active player in the development of a culture of personal information handling. The complacent and the fatalistic who suggest otherwise are wrong.

Appendix 1
Focus group topic guide

Introduction (necessary formalities)

- Welcome
- Describe purpose of exercise. Nowadays more information about individuals ('personal information') is held on computer by professionals (doctor, dentist), government bodies (DSS, Inland Revenue, local council). Private companies (shops, supermarkets, banks). Want to explore how people feel about the pros and cons of this
- Emphasise that there are no right answers and no need to reach an agreed view – we just want to hear views
- Tell them that session will be taped, but emphasise that no views will be attributed to individuals
- Ask them not to attribute views to individuals afterwards

Opening question (break the ice – get people to say something)

- Tell us your name and any one piece of information about yourself.

Introductory questions (start people thinking about the topic)

- How many people or organisations can you think of which hold information about you?

- In general, how do you feel about people or organisations holding information about you? Does it do you any harm? Does it do you any good?

Transition questions (move towards key questions)

- Do you think the amount of information organisations hold about you has grown/is growing?
- Have you ever been surprised by how much an organisation knew about you? When and how did that happen? How did you feel about it?

Key questions

- I'd like to talk about some different types of organisations.
- Step through the following one by one. How many we get through may depend on how the groups go.
  - Banks
  - Inland Revenue
  - Supermarkets [loyalty cards]
  - Department of Social Security
  - Your telephone company
  - Your GP
  - Your electricity company
  - Police
  - Your local council

For each type of organisation:

- What sort of information do you think this sort of organisation might hold about you?
- What would you be happy for them to do with your information? What would you not be happy for them to do with your information? [Trans-border flows?]
- How confident are you that they will only use it for purposes you would approve of?

- How would you feel about [organisations of this type] sharing information about you with [organisations of same/another type]? Or other parts of the same organisation? Where are the boundaries?
- Do you have similar confidence in all [organisations of this type], or more in some than others? If more in some, which? Why?
- Generally, what is it that makes you confident/not confident about [organisations of this type]?
- Going beyond the question of personal information, how do you feel in general about [organisations of this type]?

Repeat for another type of organisation. About half an hour before end of group, move on:

- Have you ever given information to an organisation even though you weren't happy to do so? Why did you give it? Have you ever refused to give information?
- Have you ever been upset at what someone did with information about you? Can you tell us about it?
- How confident are you that data held on computers are secure?
- If you weren't happy with what people were doing with information about you, what do you think you could you do about it? What legal rights do you think people have about information held on them? Are there other rights you think they should have?

Excessive information/inferences?

Ending question

- Now we've had this discussion, have your feelings changed at all?

Wrap-up (necessary formalities)

- Thank
- Remind about confidentiality
- Answer any questions

Appendix 2
The survey questionnaire

Now some questions about privacy and personal information. By personal information, I mean information about you or other individuals.

Statements given to respondents in preface to each first question about each organisation to help them think about the questions

- Local councils hold information about individual citizens, including details about the Council Tax, education, social services and housing
- Banks hold information about individual customers, including details of income, cash withdrawals, payments, mortgages, overdrafts and loans
- Central government departments hold information about individual citizens. These departments include the Inland Revenue, the Department of Social Security, the Benefits Agency, the Contributions Agency and the Driver and Vehicle Licensing Agency.
- Supermarkets hold information about individual customers who hold cards (such as the Safeway ABC Card, Sainsbury's Reward Card or Tesco's ClubCard), including how much those customers spend, what they buy and when and where they buy things.

- Phone companies such as British Telecom, Mercury or cable companies hold information about individual customers. This information includes the customer's telephone number, the telephone numbers they make calls to and the length of the calls they make.

Questions one to five

- Here are some reasons which might give you confidence that … will handle personal information properly. Which two or three of these reasons do you find most convincing? Just read out the letters that apply.

local councils; banks; central government departments; supermarkets; telephone companies

Showcard

- Under the law, they have to handle personal information properly.
- They take care to handle personal information properly, because their reputation would be damaged if they didn't.
- They sign written agreements promising that they will dealwith personal information properly.
- They say publicly that they will deal with personal information properly.
- The people who work there can be relied on to handle personal information properly.
- As far as I know, people don't often have problems with the way they handle personal information.
- Because they're British [local], they can be relied upon to handle personal information properly.
- None of these
- Don't know.

Questions six to ten

- Here are some statements about how … handle personal information about you. Which two or three statements do you agree with most strongly. Just read out the letters that apply.

local councils; banks; central government departments; supermarkets; telephone companies

Showcard

- They don't send me mail or telephone me unnecessarily.
- They keep information about me secure.
- They don't disclose sensitive information about me without my permission.
- They use the information they hold to provide services that meet my particular needs
- They don't hold more information about me than they need to.
- They keep the information they hold about me accurate and up-to-date.
- They don't use information they hold to make judgements about me which may be right or wrong.
- They don't collect information about me from other places without telling me.
- They tell me what they use information about me for.
- They don't hold information about me for longer than they need to.

Question eleven

- Here's a list of the five types of organisations. I'd now like you to rank them from 1 (the organisation you have most confidence in) to 5 (the organisation you have least confidence in), in terms of 'they will only use information about you for the purposes they told you about when they

collected it'. Which would have you have most confidence in … [repeat for others].

Showcard

- Banks
- Central government departments (e.g. the Inland Revenue and the Department of Social Security)
- Local councils
- Telephone companies
- Supermarkets

Question twelve

- Looking at the list again, I'd now like you to rank them from 1 (the organisation you have most confidence in) to 5 (the organisation you have least confidence in), in terms of: 'they won't use the information they hold to make judgements about you which may be right or wrong'. Which would have you have most confidence in..[repeat for others].

Showcard

- Banks
- Central government departments (for example, the Inland Revenue and the Department of Social Security)
- Local councils
- Telephone companies
- Supermarkets

Appendix 3
Selected analyses of data from the survey

Section 1: Data tables for Figures in the text (14–29)

Organisation	*Mean score*
Banks	2.07
Central government	2.62
Local councils	3.01
Phone companies	3.38
Supermarkets	3.78

Ranking goodwill trust: 'they won't use the information they hold to make judgements about you which may be right or wrong' (1 high, 5 low)

Organisation	*Mean score*
Banks	2.55
Central government	2.78
Local councils	3.05
Phone companies	3.16
Supermarkets	3.37

Figure 32 Data tables for Figure 14: Ranking minimal trust: 'they will only use information about you for the purposes they told you about when they collected it' (1 high, 5 low).

Type of reason	*Local councils*	*Central government*	*Banks*	*Supermarkets*	*Phone companies*
Experience	15	10	10	15	13
Reputation	38	33	47	48	47
Characteristics	22	24	29	19	20
Institution	77	78	79	61	71

Figure 33 Data table for Figure 15: Percentage of sample selecting each type of reason for trust, by organisation.

Type of reason	*Local councils*	*Central government*	*Banks*	*Supermarkets*	*Phone companies*
Prudence/minimal	12	12	14	13	12
Contract/competence	57	60	72	42	57
Goodwill	69	60	63	64	64

Figure 34 Data table for Figure 16: Percentage of sample selecting each type of task to entrust, by organisation.

Task / *Reason*	*Prudence / minimal*	*Contract / competence*	*Goodwill*
Experience	-0.015	0.006	0.024
Reputation	0.017	0.040	**0.077
Characteristics	0.020	*0.048	0.030
Institution	**0.073	*0.057	0.031

Figure 35 Data table for Figure 17: Median correlations of each task and reason type for all organisations.

Task / *Reason*	*Prudence*	*Contract*	*Goodwill*
Experience	159	237	426
Reputation	597	1038	1298
Character	390	711	676
Institution	1702	2973	2733
N	2915	5011	5138

Figure 36 Data table for Figure 18: Numbers in the sample consistently selecting types of reason to trust, by task entrusted.

Task / Reason	Prudence	Contract	Goodwill	N
Experience	159	1071	1457	2767
Reputation	597	3941	4649	9545
Character	22	117	102	248
Institution	88	494	364	958

Figure 37 Data table for Figure 19: Numbers in the sample consistently selecting types of task to entrust, by reason to trust.

Type of task	Local councils	Central government	Banks	Supermarkets	Phone companies
3 goodwill	0.38	0.41	0.38	0.25	0.35
2 goodwill, 1 contract / competence	0.43	0.46	0.41	0.31	0.38
2 goodwill and 1 prudence	0.45	0.49	0.47	0.32	0.45
1 goodwill and 2 contract / competence	0.49	0.51	0.45	0.37	0.41
1 goodwill, 1 contract / competence, 1 prudence	0.51	0.53	0.51	0.39	0.48
3 contract / competence	0.55	0.56	0.49	0.44	0.44
2 contract / competence, 1 prudence	0.57	0.58	0.54	0.46	0.51

Figure 38 Data table for Figure 20: Fitted probabilities that the median respondent will choose at least two of the institutional reasons for trusting each organisation to handle personal information, by choice of task.

Characteristic	*Whole sample (no=2018)*	*Reason fundamentalists (weighted n=32)*	*Task fundamentalists (weighted n=54)*
Age: 15-24	16		**6
Education: GCSE / O level	23		**7
Education: other	11	**9	**13
Income: £15,500-29,999	17	**6	13
Work: student	7		0
Number of children: 2	14		**4
Number of children: 5	0		**2
Region: Wales	4	**13	

** significant at the 5 per cent level

Figure 39 Data table for Figure 22: How reason and task fundamentalists differ from the population as a whole (%).

	High ranking trusters	*Low ranking trusters*	*Difference (high ranking trust % minus low)*
Local councils	398 (20%)	400 (20%)	0%
Central government	661 (33%)	361 (18%)	15%
Banks	1075 (53%)	206 (10%)	43%
Supermarkets	277 (14%)	812 (40 %)	-26%
Phone companies	519 (26%)	661 (33 %)	-7%

Figure 40 Data table for Figures 24 and 25: Numbers of high and low ranking trusters and the gap between them.

	Local councils	Central government	Banks	Supermarkets	Phone companies
Weighting	*n=398*	*n=661*	*n=1075*	*n=277*	*n=519*
Reason					
Experience					
Don't know of problems	19[b,c,p]	10[l,s]	9[l,s,p]	22[b,c,p]	13[l,b,s]
Reputation					
Reputation	40[b,s]	39[b,s]	50[l,c,p]	53[l,c,p]	43[b,s]
Characteristics					
Reliable staff	20[b,c]	26[l,b,p]	31[l,c,s,p]	02[l,b]	18[b,c]
British / local	08[b,c,s,p]	05[l]	03[l]	04[l]	04[l]
Institution					
Legal duty	66[s,p]	72[s,p]	63[s,p]	39[l,b,c]	43[l,b,c]
Written agreement	33[b,c,s]	38[l,s,p]	40[l,s,p]	21[l,b,c]	24[l,b,c]
Public commitment	19[s]	19[p]	20[s,p]	27[l,b,p]	14[b,c,s]

[l] statistically different from the percentage for local councils
[b] statistically different from the percentage for banks
[c] statistically different from the percentage for central government
[s] statistically different from the percentage for supermarkets
[p] statistically different from the percentage for telephone companies

Figure 41 Data table for Figure 26: High ranking trusters' reasons for trust, by organisation (%).

Weighting	Local councils n=398	Central government n=661	Banks n=1075	Supermarkets n=277	Phone companies n=519
Reason					
Prudence					
Tell me what use for	11[s]	13[p]	15[p]	17[l,p]	08[b,c,s]
Contract					
Keep secure	38[b,s,p]	43[b,s,p]	50[l,c,s,p]	18[l,b,c]	24[l,b,c]
Don't disclose without my permission	29[s,p]	29[s,p]	33[s,p]	18[l,b,c]	20[l,b,c]
Keep accurate	20[b,s]	20[b,s]	31[l,c,s,p]	13[l,b,c,p]	19[b,s]
Don't hold longer than need to	07	08	06[s]	09[b,p]	05[s]
Goodwill					
Don't mail or phone unnecessarily	28[b,p]	24	21[l,s]	28[b,p]	20[l,s]
Use to provide services to my needs	28[c]	19[l,b,s,p]	28[c]	34[c,p]	25[c,s]
Don't hold more than need to	22[b,c,p]	16[l,s]	15[l,s]	24[b,c,p]	12[l,s]
Don't make judgements	15[b,p]	15[b,p]	10[l,c]	12	08[l,c]
Don't collect without telling me	14[p]	13[p]	14[p]	13[p]	08[l,b,c,s]

[l] statistically different from the percentage for local councils
[b] statistically different from the percentage for banks
[c] statistically different from the percentage for central government
[s] statistically different from the percentage for supermarkets
[p] statistically different from the percentage for telephone companies

Figure 42 Data table for Figure 27: High ranking trusters' tasks entrusted, by organisation (%).

	Local councils	Central government	Banks	Supermarkets	Phone companies
weighting	*n=398*	*n=661*	*n=1075*	*n=277*	*n=519*
Reason					
Experience					
Don't know of problems	16[c]	10[l]	12	15	12
Reputation					
Reputation	33[b,s,p]	28[b,s,p]	49[l,c]	48[l,c]	48[l,c]
Characteristics					
Reliable staff	11[b,s,p]	14[b,s]	26[l,c,s,p]	19[l,b,c]	16[l,b]
British / local	05[s]	06[s]	05	09[l,c]	04
Institution					
Legal duty	64[b,s]	63[b,s]	49[l,c,p]	42[l,c,p]	59[b,s]
Written agreement	36[s]	36[s]	36[s]	23[l,b,c,p]	33[s]
Public commitment	18[b,s]	19[b]	11[l,c,s,p]	24[l,b]	23[b]

[l] statistically different from the percentage for local councils
[b] statistically different from the percentage for banks
[c] statistically different from the percentage for central government
[s] statistically different from the percentage for supermarkets
[p] statistically different from the percentage for telephone companies

Figure 43 Data table for Figure 27: Low ranking trusters' reasons for trust, by organisation(%).

Reason	Local councils Weighting n=398	Central government n=661	Banks n=1075	Supermarkets n=277	Phone companies n=519
Prudence					
Tell me what use for	12	10[p]	13	13	15[c]
Contract					
Keep secure	25[p]	31[s]	31[s]	23[b,c,p]	32[l,s]
Don't disclose without my permission	29[c,s]	22[l,b,p]	32[c,s]	18[l,b,p]	28[c,s]
Keep accurate	14[b,p]	18[s]	21[l,s]	12[b,c,p]	19[l,s]
Don't hold longer than need to	06[p]	06	05	08	06l
Goodwill					
Don't mail or telephone unnecessarily	31[b,s,p]	28[b,p]	13[l,c,s,p]	23[l,b]	22[l,b,c,s]
Use to provide services to my needs	20[b,s,p]	19[b,s,p]	27[l,c]	27[l,c]	25[l,c]
Don't hold more than need to	18[c]	11[l,s,p]	12[s,p]	20[b,c]	20[b,c]
Don't make judgements	17[s,p]	12	11	12l	10[l]
Don't collect without telling me	12	10[b,p]	16c	14	25[c]

[l] statistically different from the percentage for local councils
[b] statistically different from the percentage for banks
[c] statistically different from the percentage for central government
[s] statistically different from the percentage for supermarkets
[p] statistically different from the percentage for telephone companies

Figure 44 Data table for Figure 29: Low ranking trusters' tasks entrusted, by organisation (%).

Section 2. Percentage tests on the key hypothesis: examples of cross–tabulations on consistent trusters for the particular organisations

Figures 18 and 36, 19 and 37 summarise the test for all organisations. In this section, we offer examples of the test by organisational type. Space does not permit the inclusion of all ten figures, but the following five have been selected as illustrative of the range of strength of the statistical bias that supports the key hypothesis using this test.

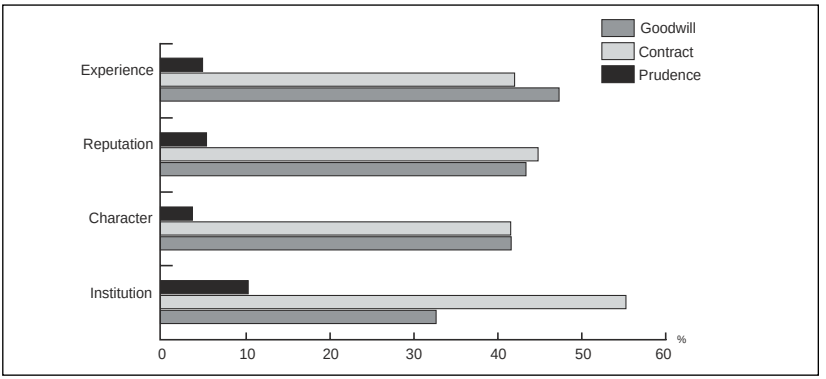

Figure 45 Tasks entrusted to central government agencies, by reason to trust.

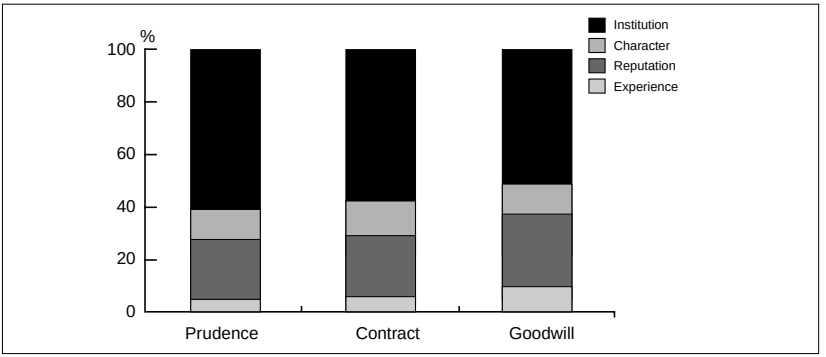

Figure 46 Reasons to trust central government agencies, by task entrusted.

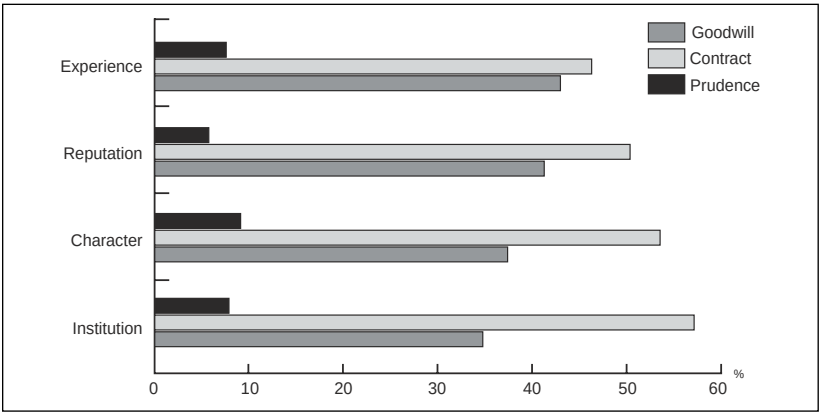

Figure 47 Tasks entrusted to banks, by reason to trust.

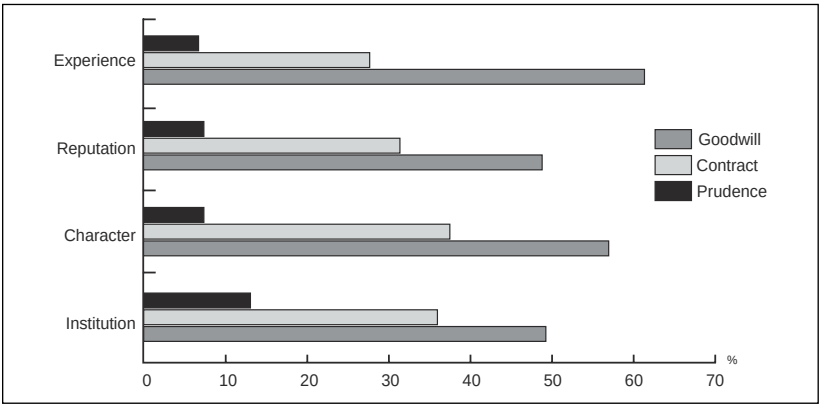

Figure 48 Tasks entrusted to supermarkets, by reason to trust.

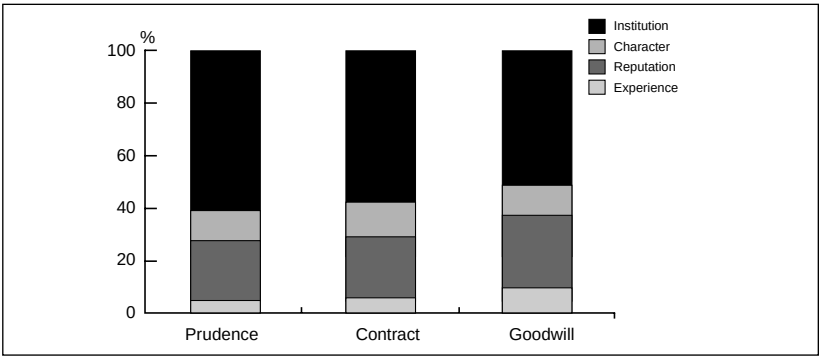

Figure 49 Reasons to trust phone companies, by tasks entrusted.

Section 3. Maximum likelihood test on the key hypothesis: methods and standard deviations

One 'prudence' task, 4 'contract/competence' tasks and 5 'goodwill' tasks were available to the respondents for selection. From these, we constructed several others which were counts of each of the types of tasks for each organisation. These new variables are: (for Banks) GOODWB, CONCOMPB, PRUDB, (for Central government) GOODWC, CONCOMPC, PRUDC, (for Local councils) GOODWL, CONCOMPL, PRUDL, (for Supermarkets) GOODWS, CONCOMPS, PRUDS, and (for Telephone companies) GOODWT, CONCOMPT, AND PRUDT.

There were 1 'experience' reason, 1 'reputation' reason, 2 'characteristic' reasons, and 3 'institutional' reasons. We constructed two sets of dependent variables used to test the two hypotheses. They are all dichotomous, binary variables and within each set there is a variable for each organisation. The first set indicates whether a respondent chose both the 'experience' and 'reputation' reasons. They are: (for Banks) EXPREPB, (for Central government) EXPREPC, (for Local councils) EXPREPL, (for Supermarkets) EXPREPS, and (for Telephone companies) EXPREPT. The second set indicates whether or not a respondent chose at least two of the 'institutional' reasons. These are: (for Banks) INSTB, (for Central government) INSTC, (for Local councils) INSTL, (for Supermarkets) INSTS, and (for Telephone companies) INSTT.

We constructed four logit models for each of the institutions. The first two used the first dependent variable described above. For example, for Banks it was the EXPREPB. One of them used only the task related variables we constructed (e.g., GOODWB, CONCOMPB, and PRUDB) Corresponding to the same institution as explanatory variables. The other used these plus some socioeconomic variables. The last two models used the other dependent variable: INSTB for Banks. The same explanatory variables were used as for the first two models. The explanatory variables were linearly combined to form the systematic component of the model and the stochastic component was the logistic. The resulting maximum likelihood estimators are presented in the Appendix. Fitted values were calculated and are preseated in Figure 20.

The socioeconomic variables used in the models are age, income, race, sex and social class. They are defined and summary statistics provided for each in the following figures.

Variable name	*Mean*	*st. dev.*	*Median*	*Minimum*	*maximum*
AGE	44.812	18.498	42	15	92

Figure 50 Summary statistics for AGE of median respondent.

Category	*Value*
1: less than £2,500	1.2%
2: £2,500-£4,499	5.4%
3: £4,500-£6,499	6.3%
4: £6,500-£7,499	3.8%
5: £7,500-£9,499	4.1%
6: £9,500-£11,499	4.8%
7: £11,500-£13,499	3.9%
8: £13,500-£15,499	4.4%
9: £15,500-£17,499	4.1%
10: £17,500-£24,999	9.7%
11: £25,000-£29,999	6.9%
12: £30,000 and up	12.5%
Mean	7.718
st. dev.	3.524
Median	8

Figure 51 Frequency count and summary statistics for INCOME of median respondent.

Mean	*st. dev.*
0.043	0.202

Note: RACE is a binary variable where '1' indicates that the respondent is not white.

Figure 52 Summary statistics for RACE of median respondent.

Mean	*st. dev.*
0.478	0.5

Figure 53 Summary statistics for SEX of median respondent.

Category	*Value*
1: A	1.4%
2: B	17.0%
3: C1	26.6%
4: C2	22.8%
5: D	17.0%
6: E	15.2%
Mean	3.825
st. dev.	1.35
Median	4

Figure 54 Frequency count and summary statistics for SOC (social class) of median respondent.

Section 4. Characteristics of experience and reputation based trusters, and institutionally based trusters: examples of regression analyses

Two sets of models were estimated with logistic regressions for the dependent variables of being a consistent experience or reputation based truster, and for being an institutionally based truster in each organisation, using

- all the attitudinal variables on tasks for the relevant organisation (but not for any other organisations and not the rankings of organisations), and
- the sociodemographic variables of age as a continuous variable and income by brackets, degree level educatior., sex and socioeconomic class.

Figure 21 in the main body of the text summarises the principal findings. In this section, we present as an example of the twenty regressions on which these results are based, just the case of banks, for which four regressions are presented for comparison, being both with and without sociodemographic variables, and for the two kinds of truster.

The factors that are significant at the 10 per cent level are asterisked and appear in italics. However, only those that are significant at the 5 per cent level are used in Figure 21 or given any weight in the interpretation offered in the main body of the text.

Variable	*Beta coefficient*	*Standard error*	*Significance*
Use only for purpose told	*0.6321*	*0.2918*	* *0.0303*
Don't collect	0.4063	0.3055	0.1836
Don't disclose	*0.8819*	*0.2404*	* *0.0002*
Secure	*0.5222*	*0.2416*	* *0.0307*
No more than need	*0.7706*	*0.2855*	* *0.0069*
No longer than need	- 0.6281	0.6511	0.3347
Don't mail / phone	0.0524	0.3126	0.8668
Accurate	*0.8599*	*0.2452*	* *0.0005*
Don't judge	0.3706	0.3641	0.3088
Personalise	0.0229	0.2797	0.9347
None	- 0.3898	1.0624	0.7136
Don't know	- 0.4832	1.0618	0.6491
Constant	*- 4.3281*	*0.3467*	* *0.0000*
N= 2018			
Goodness of fit=1963.367			

Figure 55 Institutionally based trusters in banks, model I using task variables only.

Variable	*Beta coefficient*	*Standard error*	*Significance*
Use only for purpose told	*0.6398*	*0.2933*	* *0.0292*
Don't collect	0.3984	0.3065	0.1936
Don't disclose	*0.9255*	*0.2427*	* *0.0001*
Secure	*0.5014*	*0.2421*	* *0.0384*
No more than need	*0.7798*	*0.2865*	* *0.0065*
No longer than need	- 0.6046	0.6409	0.3454
Don't mail / phone	0.0664	0.3130	0.8321
Accurate	*0.8607*	*0.2465*	* *0.0005*
Don't judge	0.4020	0.3646	0.2702
Personalise	0.0261	0.2815	0.9262
None	- 0.2458	1.0664	0.8177
Don't know	- 0.3208	1.0681	0.7639
Age	*- 0.0118*	*0.0067*	* *0.0770*
Higher education	-0.5144	0.4257	0.2269
Gross income	0.0369	0.0335	0.2712
Sex	0.0672	0.2260	0.7661
Social class	- 0.0243	0.0993	0.8068
Constant	*- 4.1122*	*0.7812*	* *0.0000*
Goodness of fit=1820.140			

Figure 56 Institutionally based trusters in banks, model 2 using task and sociodemographic variables.

Section 5. High and low ranking trusters: examples of regression analyses

Figure 31 in the main body of the text provides a summary of the factors that proved to be statistically significant in explaining high and low ranking trust in each type of organisation. In this section. We present examples of some of the regressions that support that Figure.

We conducted a series of logistic regressions in which the following list of controlling and explanatory variables of high and low ranking trust was applied:

- all the attitudinal variables on reasons and tasks for the relevant organisation (but not for any other organisations and not the rankings of organisations), and

Variable	*Beta coefficient*	*Standard error*	*Significance*
Use only for purpose told	0.4898	0.3228	0.1293
Don't collect	0.0883	0.3660	0.8093
Don't disclose	0.0388	0.2748	0.8877
Secure	0.1706	0.2593	0.5107
No more than need	0.3803	0.3196	0.2339
No longer than need	- 1.5557	1.0319	0.1317
Don't mail / phone	*0.7191*	*0.2787*	* *0.0099*
Accurate	0.1524	0.2727	0.5763
Don't judge	*0.6133*	*0.3480*	* *0.0780*
Personalise	0.4376	0.2737	0.1099
None	- 0.8940	1.0718	0.4042
Don't know	0.6543	0.5906	0.2680
Constant	*- 3.8239*	*0.3747*	* *0.0000*
Goodness of fit=2086.369			

Figure 57 Experience and reputation based trusters in banks, model 1 using task variables only.

Variable	*Beta coefficient*	*Standard error*	*Significance*
Use only for purpose told	0.4585	0.3242	0.1574
Don't collect	0.0294	0.3687	0.9365
Don't disclose	0.0662	0.2764	0.8105
Secure	0.2102	0.2627	0.4236
No more than need	0.3612	0.3225	0.2627
No longer than need	- 1.6479	1.0404	0.1132
Don't mail / phone	*0.7259*	*0.2800*	* *0.0095*
Accurate	0.1600	0.2749	0.5605
Don't judge	0.5554	0.3512	0.1138
Personalise	*0.4995*	*0.2762*	* *0.0705*
None	- 0.9260	1.0748	0.3890
Don't know	0.5434	0.6023	0.3670
Age	0.0017	0.0064	0.7900
Higher education	0.0246	0.4051	0.9516
Gross income	- 0.0404	0.0314	0.1983
Sex	0.1914	0.2340	0.4135
Social class	0.1508	0.1016	0.1377
Constant	*- 4.2403*	*0.8126*	* *0.0000*
Goodness of fit = 2111.599			

Figure 58 Experience and reputation based trusters in banks, model 2 using task and sociodemographic variables.

Variable	Beta coefficient	Standard error	Significance
R: Public commitment	- 0.0317	0.1588	0.8416
R: Written agreement	- 0.0561	0.1383	0.6851
R: Legal duty	0.1707	0.1468	0.2448
R: No problems	*0.3014*	*0.1706*	* *0.0773*
R: Reliable staff	0.0344	0.1573	0.8271
R: British / local	*0.4781*	*0.2422*	* *0.0484*
R: Reputation	0.0196	0.1354	0.8846
R: None	- 0.4426	0.3724	0.2346
R: Don't know	0.3035	0.3666	0.4077
T: Use only for purpose	- 0.2212	0.1869	0.2366
T: Don't collect	0.0064	0.1756	0.9709
T: Don't disclose	- 0.0053	0.1440	0.9706
T: Secure	*0.3359*	*0.1355*	* *0.0132*
T: No more than need	0.1908	0.1524	0.2106
T: No longer than need	- 0.2076	0.2308	0.3683
T: Don't mail / phone	- 0.2247	0.1454	0.1221
T: Accurate	0.1554	0.1577	0.3243
T: Don't judge	- 0.0400	0.1724	0.8164
T: Personalise	0.1522	0.1490	0.3071
T: None	*- 0.9082*	*0.3596*	* *0.0116*
T: Don't know	*-0.7539*	*0.3385*	* *0.0259*
Constant	*- 1.5754*	*0.2434*	* *0.0000*
Goodness of fit = 2021.335			

Figure 59 High ranking trusters in local councils: model I, using reason and task variables only.

- the sociodemographic variables of age as a continuous variable and income by brackets, degree level education, sex and socioeconomic class.

As with the regressions on experience or reputation based trust and institutionally based trust, we estimated models both with and without the sociodemographic variables. Conducting regressions using each type of model on both high and low ranking trusters for each of the organisations yields twenty regressions. There is not sufficient space here to reproduce them all. Therefore, we present only the case of local councils.

Variable	*Beta coefficient*	*Standard error*	*Significance*
R: Public commitment	0.0010	0.1601	0.9949
R: Written agreement	- 0.0076	0.1405	0.9566
R: Legal duty	0.1645	0.1493	0.2706
R: No problems	*0.2881*	*0.1721*	** 0.0941*
R: Reliable staff	0.0081	0.1586	0.9593
R: British / local	*0.4758*	*0.2453*	** 0.0525*
R: Reputation	0.0580	0.1367	0.6711
R: None	- 0.5094	0.3741	0.1733
R: Don't know	0.2719	0.3711	0.4638
T: Use only for purpose	- 0.2473	0.1888	0.1902
T: Don't collect	- 0.0144	0.1775	0.9353
T: Don't disclose	- 0.0329	0.1449	0.8205
T: Secure	*0.3344*	*0.1366*	** 0.0144*
T: No more than need	0.1641	0.1534	0.2845
T: No longer than need	- 0.2195	0.2317	0.3434
T: Don't mail / phone	- 0.2379	0.1467	0.1050
T: Accurate	0.1313	0.1600	0.4120
T: Don't judge	- 0.0229	0.1740	0.8955
T: Personalise	0.1414	0.1498	0.3451
T: None	*- 0.9928*	*0.3622*	** 0.0061*
T: Don't know	*- 0.7925*	*0.3421*	** 0.0205*
Age	0.0032	0.0032	0.3202
Higher education	*0.5843*	*0.1798*	** 0.0012*
Gross income	*- 0.0381*	*0.0159*	** 0.0164*
Sex	0.1658	0.1178	0.1593
Social class	*0.1000*	*0.0509*	** 0.0492*
Constant	*- 1.8975*	*0.4442*	** 0.0000*
Goodness of fit =2036.765			

Figure 60 High ranking trusters in local councils: model 2, using reason and task and also sociodemographic variables.

The factors that are significant at the 10 per cent level are asterisked and appear in italics. However, only those that are significant at the 5 per cent level are used in Figure 31 or given any weight in the interpretation offered in the main body of the text.

Variable	*Beta coefficient*	*Standard error*	*Significance*
R: Public commitment	0.0483	0.1600	0.7627
R: Written agreement	0.1641	0.1381	0.2347
R: Legal duty	0.1850	0.1534	0.2278
R: No problems	0.2415	0.1770	0.1724
R: Reliable staff	*- 0.5952*	*0.1870*	** 0.0015*
R: British / local	0.0211	0.2772	0.9392
R: Reputation	- 0.1322	0.1396	0.3434
R: None	*0.6526*	*0.2849*	** 0.0220*
R: Don't know	- 0.2135	0.3774	0.5717
T: Use only for purpose	- 0.0049	0.1861	0.9790
T: Don't collect	- 0.1900	0.1858	0.3066
T: Don't disclose	0.2166	0.1482	0.1439
T: Secure	- 0.1976	0.1469	0.1787
T: No more than need	0.0371	0.1609	0.8175
T: No longer than need	- 0.1737	0.2388	0.4669
T: Don't mail / phone	0.0729	0.1499	0.6267
T: Accurate	- 0.1825	0.1755	0.2983
T: Don't judge	*0.3335*	*0.1685*	** 0.0478*
T: Personalise	- 0.2435	0.1615	0.1317
T: None	0.2924	0.2671	0.2736
T: Don't know	- 0.2369	0.3049	0.4371
Constant	*- 1.5028*	*0.2499*	** 0.0000*
Goodness of fit = 2010.495			

Figure 61 Low ranking trusters in local councils: model 1, using reason and task variables only.

Variable	*Beta coefficient*	*Standard error*	*Significance*
R: Public commitment	0.0569	0.1608	0.7232
R: Written agreement	0.1294	0.1394	0.3533
R: Legal duty	0.1584	0.1554	0.3080
R: No problems	0.2375	0.1776	0.1811
R: Reliable staff	*- 0.6062*	*0.1876*	** 0.0012*
R: British / local	0.0123	0.2793	0.9649
R: Reputation	- 0.1301	0.1403	0.3541
R: None	*0.6124*	*0.2857*	** 0.0321*
R: Don't know	- 0.1964	0.3795	0.6047
T: Use only for purpose	- 0.0255	0.1871	0.8915
T: Don't collect	- 0.1992	0.1863	0.2850
T: Don't disclose	0.2200	0.1487	0.1390
T: Secure	- 0.2116	0.1475	0.1515
T: No more than need	0.0376	0.1616	0.8161
T: No longer than need	- 0.1857	0.2395	0.4380
T: Don't mail / phone	0.0641	0.1504	0.6702
T: Accurate	- 0.1796	0.1767	0.3093
T: Don't judge	*0.3081*	*0.1694*	** 0.0690*
T: Personalise	- 0.2528	0.1621	0.1189
T: None	0.2918	0.2686	0.2773
T: Don't know	- 0.1891	0.3064	0.5371
Age	*- 0.0087*	*0.0033*	** 0.0090*
Higher education	0.0615	0.1788	0.7307
Gross income	- 0.0185	0.0163	0.2561
Sex	0.1040	0.1164	0.3720
Social class	0.0183	0.0507	0.7190
Constant	*- 1.0260*	*0.4453*	** 0.0212*
Goodness of fit = 2011.882			

Figure 62 Low ranking trusters in local councils: model 2, using reason and task and also sociodemographic variables.

Notes

1. I am not sure just how conscious an echo this was of the remark by Marc Rotenberg, Director of the Electronic Privacy Information Centre in Washington DC, who said that 'privacy will be to the information economy of the next century what consumer protection and environmental concerns have been to the industrial economy of the twentieth century', in 'Behind closed doors: Big Brother is us', *New York Times,* 29 September 1996, cited in Cate FH, 1997, *Privacy in the information age*, Brookings Institution, Washington DC, 3.
2. Walzer M. 1983, *Spheres of justice: a defence of pluralism and equality,* Blackwell, Oxford; and Elster J, 1992, *Local justice: how institutions allocate scarce goods and necessary burdens,* Cambridge University Press, Cambridge.
3. Castells M. 1996, *The rise of the network society,* Blackwell, Oxford.
4. Lyon D, 1994, *The electronic eye: the rise of the surveillance society*, Polity Press, Cambridge.
5. 6 P, 1994, 'Trust, social theory and public policy', Demos and School of Social Sciences, University of Bath.
6. 6 P, Jupp B and Bentley T, 1996, *Open wide: futures for density in 2010*, Demos, London: ch. 5.
7. Data Protection Registrar, 1997, *The thirteenth annual report of the Data Protection Registrar*, The Stationery Office, London.
8. Henley Centre for Forecasting, 1995, *Dataculture: privacy, participation and the need for transparency in the information age,* Henley Centre for Forecasting, London.
9. 6 P with Briscoe I, 1996, *On the cards: privacy, identity and trust in the age of smart technologies,* Demos, London.
10. Direct Marketing Association and Informix, 1997, *The new information trade*, Direct Marketing Association and Informix.
11. See Equifax, 1990, *The Equifax report on consumers in the information age*, Equifax, Atlanta, Georgia; Equifax 1991, *Harris-Equifax consumer privacy survey 1991,* Equifax, Atlanta, Georgia;

Equifax 1992, *Harris-Equifax consumer privacy survey 1992,* Equifax Atlanta, Georgia; Equifax 1995, *Harris-Equifax mid-decade consumer privacy survey 1995,* Equifax, Atlanta, Georgia.

12. Direct Marketing Association, 1996, *The DMA census of the UK direct marketing industry 1996,* Direct Marketing Association, London.
13. Hine C, Eve J and Woolgar S, 1996, *Privacy in the electronic marketplace, Centre for Research into Innovation, Culture and Technology,* Brunel University, Uxbridge.
14. Hedges A. 1996. *Confidentiality: the public view,* Department of Social Security Research Report no 56, The Stationery Office, London.
15. Kable, 1997, *Electronic government services? If you ask me&…,* Kable for Bull Worldwide Information Services, London.
16. Patterson M, O'Malley L and Evans M, 1997, 'Database marketing: investigating privacy concerns', *Journal of marketing communications,* no 3, 151–174.
17. Henley Centre for Forecasting, 1994, *Teleculture 2000,* Henley Centre for Forecasting, London.
18. See note 9.
19. On focus group methods, see Krueger RA, 1994, *Focus groups: a practical guide for applied research,* 2nd Ed, Sage, Thousand Oaks, California.
20. Hedges, A, 1987, *Report on a qualitative study of data subjects,* Office of Data Protection Registrar, Wilmslow; Chrzanowska A, 1989, *Qualitative research on fair obtaining,* Office of Data Protection Registrar, Wilmslow.
21. See notes 5 and 6.
22. See note 6.
23. There is of course a huge literature on the meaning, scope and role of the concept of privacy, written by legal, moral and political philosophers, jurisprudents, comparative and black letter law scholars: see Volume I for a very brief review of some of the main strands. The locus classicus of conceptual and philosophical analysis remains Westin AF, 1967, *Privacy and freedom,* Athenauem, New York, but see also Schoeman FD, 1982, *Privacy and social freedom,* Cambridge University Press, Cambridge, and McWhirter DA and Bible JD, 1992, *Privacy as a constitutional right,* Quorum, New York. A recent comprehensive comparative law review is Bennett CJ, 1992 *Regulating privacy: data protection and public policy in Europe and the United States,* Cornell University Press, Ithaca, New Jersey; also dealing with the question is Cate, 1997 (see note 1).
24. See note 6.
25. For a recent discussion of the relative merits of rating and ranking questions in eliciting attitudes, see Inglehart R, 1997, *Modernisation and postmodernisation: cultural, economic and political change in 43 countries,* Princeton University Press, Princeton, New Jersey: 117–122.
26. The resulting maximum likelihood estimates are in some ways analogous to regression coefficients. However, whereas in an ordinary least squares regression, the coefficients are determined by minimizing the combined distances between the actual data and the predicted regression line,

using a linear equation, in an estimation of maximum likelihoods, any kind of equation will serve, and the test essentially finds its derivative and determines estimates that would make the equation equal to zero.

27. 6 and Briscoe, 1996 (see note 9), 58, from Data Protection Registrar, 1992, *The eighth annual report of the Data Protection Registrar,* The Stationery Office, London.
28. See Inglehart, 1997 (note 26).
29. See note 9.