We no longer control what others know about us, but we don't yet understand the consequences . . .

DEMOS

FYI

The new politics of personal information

Peter Bradwell
Niamh Gallagher

About Demos

Who we are
Demos is the think tank for everyday democracy. We believe everyone should be able to make personal choices in their daily lives that contribute to the common good. Our aim is to put this democratic idea into practice through our research and dissemination.

What we work on
We focus on six areas: public services; science and technology; cities and public space; identity; arts and culture; and global security. Many of our projects link more than one area, and we consistently seek to explore and strengthen our understanding of those connections.

Who we work with
Our partners include policy-makers, companies, public service providers and social entrepreneurs. Demos is independent of any party – we work with politicians across political divides. Our international network, spanning six continents, provides a global perspective and enables us to work across borders.

How we work
Demos knows the importance of learning from experience. We work collaboratively with communities and individuals, and we test and improve our ideas in practice by working with people who can make change happen.

How we communicate
As an independent voice, we can create debates that lead to real change. We use the media, public events, workshops and publications to communicate our ideas. All our books can be downloaded free from the Demos website.

www.demos.co.uk

First published in 2007

ISBN 978 1 84180 191 9
Copy edited by Julie Pickard, London
Typeset by utimestwo, Collingtree, Northants
Printed by IPrint, Leicester

For further information and
subscription details please contact:

Demos
Magdalen House
136 Tooley Street
London SE1 2TU

telephone: 0845 458 5949
email: hello@demos.co.uk
web: www.demos.co.uk

FYI

The new politics of personal information

Peter Bradwell
Niamh Gallagher

DEMOS

DEMOS

Contents

Acknowledgements

We are extremely grateful first of all to the Information Commissioner and his Office for his early help in the project and their consistent support and advice throughout the research. Special thanks also to our steering group members Rodney Austin, Caspar Bowden and Madeleine Colvin; their generous expertise and comments were invaluable. Thanks also to the many people we have spoken to through the course of our research, all of whom contributed generously with their time, thoughts and advice. In particular we are grateful to Sue Milnes, Neil Munroe and Andy Phippen.

Huge thanks to all our Demos colleagues for their support, ideas and enthusiasm. In particular, to Duncan O'Leary for his guidance and intellectual interventions. Similarly, thanks to Sam Jones, Simon Parker, Charlie Tims, Jack Stilgoe, Alessandra Buonfino and William Higham for their thoughts and inspiration. We are extremely grateful to the Demos interns who have supported the project so intelligently: Louise Wise, Outi Kuittenen and Miae Woo. Thanks, finally, to Vikki Leach and Roger Sharp at O2 for supporting the research.

Errors and omissions remain, predictably, our own.

Peter Bradwell
Niamh Gallagher
December 2007

Executive summary

Aims of the study

This report has three aims:

1. to connect the value people gain from an information-rich society with the challenges that arise from giving away personal information
2. to raise awareness of the consequences of the increasing reliance on personal information by institutions in the public and private sector
3. to provide a framework within which policy-makers, businesses and individuals can address these challenges in the long term.

This report is intended to push the debate on personal information beyond the legal and technical language associated with data protection and identity management. The debate must move towards something that people – through day-to-day experiences in their own lives – have a stake in. New trends of communication, customer services, personalisation, and issues of social inclusion and privacy are helping to create a new framework for the discussion of personal information.

Our argument

Personal information has become central to how we live – from

banking online and supermarket shopping, to travelling, social networking and accessing public services. The visible result of this is a trend towards personal, tailored services, and with this comes a society dominated by different forms of information gathering. This is not just something people are subjected to. They are more and more willing to give away information in exchange for the conveniences and benefits they get in return, and are often keen for the recognition and sense of self it affords.

But there is a tension here. By sharing personal information we surrender control in the longer term by leaving ourselves open to judgement by different groups in different ways. The drive to personalise or tailor services, which is shaped by those judgements, can lead to differences between what people experience and have access to. This can mean a narrowing of experience, can lead to social exclusion, and has significant implications for how we live together as a society. We argue that these problems can only be resolved by a more open understanding of and better democratic debate about the boundaries, rights and responsibilities that regulate the use of personal information. That debate should focus on developing the collective rules that determine individuals' ability to negotiate how personal information is used.

Chapter summaries

Introduction: asking for it

Problems of data protection, privacy, technology and identity are inseparable from the benefits we enjoy from the open information society we live in. There is a hazy distinction between the lifestyle and social benefits that can result from sharing our personal information, and the way information can change how organisations and institutions find out and make decisions about us. Personal information creates a *political* challenge because it is the basis on which decisions about interventions from institutions are made. This pamphlet will focus on the resulting tension, between empowerment *through* information and control *by* information, that sits at the heart of the move towards a personalised, tailored services agenda.

Chapter 1: Being watched, and needing to be seen

Being watched through the exchange of personal information in our everyday lives has become ever more central to our identities, to our experiences of services, and to how we relate to other people. But the Big Brother metaphor cannot fully explain the significance of how personal information is used. This chapter shows why there has been an increased prominence of what we will call 'interpersonal surveillance': people watching people. We argue that this opens the potential for more people to be involved in what surveillance is for: judging, sorting and responding to the people and ideas around them.

Chapter 2: The convenience of being known: what organisations and institutions do

Information has become the tool that enables product and service specialisation based on individual wants, needs and aspirations. This chapter explores the assumptions behind the personal 'offer' by looking at the practical reality of individually tailored services – first through the private sector, and then through government. It maps the realities of information use, what the consequences are, and outlines people's ability to influence the decisions made about them.

Chapter 3: We care, but we're not sure why: attitudes to personal information

The rate of technological change and professional practice can move faster than the public's awareness. Though people are beginning to understand how their information is used and what the implications are, that understanding is marked by ambiguity. That makes it even more difficult for people to make sense of the benefits and dangers of giving away information. In this chapter we will explain why this is, focusing on people's attitudes and understanding.

Chapter 4: Protecting and promoting: data protection and digital identity management

This chapter looks at the means through which people can try to manage and control what happens to their personal information.

Empowering people through their personal information has to be just as much about negotiating and managing the way other people 'see' a person – through their personal information – as it does about securing it. The chapter highlights the tension between individuals' decisions about rights over personal information, and institutional or organisational rights to use and make decisions on the basis of it. There is a consequent tension between 'top-down' solutions to the management of personal information and 'bottom-up' approaches.

Chapter 5: The new politics of personal information

Rational distinctions between types of people based on their personal information can lead to differences between what those individuals experience and have access to. This can result in a narrowing of experience, can exacerbate social exclusion, and can have significant consequences for how we live together as a society. This is the political battleground of personal information. This chapter explains why the 'rules of engagement' in personal information need to be more open and democratic, and how to make that happen through policies and approaches from government, organisations and individuals.

Recommendations

People themselves must be put at the centre of information flows. Our findings suggested a number of measures that government, the private sector and individuals could follow to improve the relationship between people, personal information and the institutions that use that information.

For individuals, we recommend:

- The first step is for individuals to take measures to protect their personal information – for example, by securing wireless networks. Second, they must recognise the connections between the benefits of sharing information, and the often less tangible costs and dangers that can result. A better understanding of this relationship is the necessary step towards bottom-up policy driven by

collectively negotiated norms and rules, rather than policy driven by the narrower needs and interests of government or business. However, this does need considerable support from government and the private sector to start the process.

For government, we recommend:

- The government should develop a more coherent strategy around personal information use. This strategy should clarify the links between how government will use personal information, in specific contexts, and what the potential benefits or costs might be for individuals. Each government department using personal information must say how they are accessing personal information, for what purpose, and how it affects people. They should also employ 'cash-handling' disciplines for dealing with people's personal information.
- The government should begin long-term research and thinking into increasing levels of information about individuals, coupled with personalising services and experiences. Segmentation and increasing knowledge of individuals will create markets that exclude in ways that current uses of information do not. That will have a significant impact on what is meant by equality. For example, will a new frontier of the welfare state be providing life insurance for certain types of people who are deemed bad investments by private insurance providers?
- The Information Commissioner's Office (ICO) needs greater capacity to cope with the range of demands of an information society, which continue to extend away from just security of data towards data use and the nature of information sharing. For example, that could include the ability for the ICO to audit organisations' use of personal information without needing their consent.

- 'Privacy impact assessments' should be used for major projects across public and private sectors to assess the use of personal information early in development, led by the ICO.
- There needs to be a serious, renewed debate about the identity card scheme, with the kind of engagement that should have happened at the start of the process. Otherwise, the scheme should be dropped. There needs to be more open consideration of what kind of information the cards would hold, why, and in what circumstances they will be used. Meaningful engagement with the public about how the technology should work must be foremost in shaping what the cards do, if they are to go ahead.

For business and the private sector, we recommend:

- The rights of access individuals have to information held about them in the private sector should be extended, including the right to know what groups people have been 'segmented' into, and allow greater ability for individuals to challenge and change existing information about themselves that they believe to be invalid, incorrect or unfair.
- Information holders should engage in an open debate about where responsibility for personal information lies, with a view to clarifying the rights and responsibilities of businesses and individuals.
- There should be a common sense test for privacy statements and personal information policy. The private sector must provide simple, accessible explanations of why personal information is gathered. It is too easy currently to adapt and rely on established legalistic policies. A move away from jargon is needed. This means, for example, requiring businesses to follow the legal concept of the 'reasonable person' when drawing up policy statements on personal information.

- Banks should consider a 'no claims bonus' for customers who successfully protect their personal information.
- Technical distinctions used by business – between authenticators and identifiers, for example – should be binned. As for government, private sector involvement in digital identity should be grounded in the ways that people use and value their digital identities. That should imply a move away from using information people are likely to divulge – such as family maiden names, dates of birth – as 'authenticators' instead.
- As a bridge between people, policy-makers and technologists, a body such as the ICO should be given the remit and resources to lead open discussions and debate to help build more secure, effective and appropriate technology for personal information.

The research

This report is the result of nine months of Demos research, focused on understanding the value of personal information to government, the private sector and individuals. The process involved interviews with over 30 experts – from fields of technology, business, government, security, academia and media – all associated with the use, protection or promotion of personal information use; a half-day workshop with information and privacy specialists; a wide-ranging literature review; eight focus groups; and six in-depth case studies of information use in the public and private sectors, and by individuals.

In May and June 2007, we ran eight focus group meetings exploring attitudes to personal information. The groups comprised a random sample split by age: 17–25, 25–35, 35–45 and 45+. In addition to a range of focused questions, participants designed personal information 'maps' – demonstrating what information was most personal to them, who they would share it with and in what context. Following the group meetings, participants were asked to fill in 'information diaries' for a month, detailing when and where they encountered transactions involving personal information.

Introduction

Asking for it

Millions of travellers in London use their Oyster card to board the tube or bus to get to work, commute home, or simply get around. With a swipe of plastic they share private information – the times, frequency and destination of their journeys, how much they pay and how – in a public setting. The card uses 'radiofrequency identification' (RFID) technology, meaning it transmits data about the commuter's credit, and the ticket barriers receive it.

The card generates and relies on commuters' information. It records people's movements. That might happen in public, but the *logging* of when and where a card was used generates information many would consider private. The information is held by the operators of the scheme Transport for London (TfL), with access for other government agencies through data legislation. That information is connected, in the case of registered cards, to further information – names, addresses, birthdays and bank details. Services like the Barclaycard OnePulse,[1] for example, offer a combined credit, Oyster and 'cashless' card meaning that, as well as travel information, those cards can generate purchasing and bank details.

The Oyster card is a convenience, potentially cutting down the number of ticket purchases, making them cheaper and, in using plastic rather than flimsy card, making the ticket more difficult to break. It allows for a better understanding by TfL of journeys through the Underground system, as they can more easily monitor which

stations are used most at what times, and on which days. These are all connected to the information commuters give away in using Oyster. But at the same time, beyond a ticket it is hard to know what deal people are getting – exactly what information is held where, by whom, and under what circumstances. And it is difficult to decide not to give that information away – the Oyster card has been promoted through price discrimination, with significant disparities between Oyster and paper ticket prices; it is costly to opt out.

In 2004, the Information Commissioner Richard Thomas warned that we are 'sleepwalking into a surveillance society'.[2] A report for his Office two years later announced that 'it is pointless to talk about the surveillance society in the future tense'.[3] Surveillance of some form has become a prevalent if not dominant means to manage, regulate and organise the modern world. 'Personal information' is a central part of how that surveillance works, and what it means.

Despite rich coverage from experts, academics and commentators there is a mixed attitude to what this era of surveillance means. Concerns on a general level about privacy have not disappeared. But people's attitudes to surveillance are perhaps better summed up by community requests for *more* closed circuit television (CCTV)[4] rather than collective outrage at constant unwelcome intrusion. There is a disconnect between people's standard concerns about privacy and Big Brother on the one hand and, on the other, their willingness to be part of a world to which surveillance of some form is fundamental.

As a result, few people connect those concerns to their everyday experiences. This is not surprising, given that personal information is often gathered as part of transactions, interactions or situations we enjoy or find beneficial. That hazy distinction – between the lifestyle benefits that can result from sharing our personal information, and the way information can change how organisations and institutions find out about us – is the basis of this pamphlet. Current debates miss how problems of data protection, privacy, technology and identity are inseparable from the benefits we enjoy from the open information society we live in.

This is because it is impossible to untangle the positives of an

information-rich world – convenience, choice and collaboration – from a set of potential dangers and challenges.

There are two trends that make this problem more fraught:

1 There has been a drive in recent years towards 'personalising' public services. As a public services policy review from March 2007 urged, public service reform looks to offer 'a Britain where . . . services are geared ever more to the personal needs of those who use them'.[5] This reflects existing approaches in the private sector that seek to build relationships with customers through tailoring services to their needs. Both are driven by people's desire for more bespoke, responsive services.
2 There are many new ways people communicate, share experiences and associate with each other, and the way we come to understand ourselves, and others come to find out about us, has changed as a result. People now have greater ability and desire to find out about and judge each other in their everyday lives, making surveillance not just something done to us, but something we potentially take a greater part in together.

Personal information is inextricably linked to both of these. Services and products are becoming tailored around the 'footprints' people leave, a footprint that increasingly takes the form of personal information. The information generated by the two trends mentioned above means that other people and institutions are more able to make decisions about us. Personal information creates a *political* challenge because it is the basis on which decisions about interventions from institutions are made. This pamphlet will focus on the resulting tension between empowerment *through* information and control *by* information that sits at the heart of the move towards a personalising, tailored services agenda. The pamphlet argues that personal information use needs to be far more democratic, open and transparent (see box 1).

Box 1. Three approaches to personal information

- *Paternalistic:* Collective rules and decision-making about personal information use that provide security, for example, legislation granting security services access to communications data, or decisions about using information about children's diet to intervene in family life.
- *Deregulatory:* Lack of collective rules on use, allowing the market and individuals to decide the rules of how personal information is used, for example, the Conservative Party's Redwood policy review suggestion that the Data Protection Act should be repealed as a piece of expensive bureaucracy. Using this model, good practice and consumer interests would be served by market forces.
- *Democratic:* Collective rules that create the possibility of individual negotiation. When institutions, public or private, make decisions based on personal information there is an assumption about what sort of people can make decisions about particular types of behaviour, and what the consequences of those judgements should be. That ranges from whether a security service can access someone's phone records, towards allowing the music industry to use information from internet service providers about what their customers do online to prevent file-sharing.[6]

  People's attitudes to where this is appropriate vary. A more democratic use of personal information means giving people the opportunity to negotiate how others use their personal information in the various and many contexts in which this happens. We need collective rules that establish people's rights to do this, and increase their ability to make informed choices. Deregulated and more paternalistic approaches may be appropriate in different contexts. However, a democratic approach entails a more open negotiation of when and where those approaches are taken.

The problems arising from the use of personal information stem from some basic questions about how a society decides what kind of behaviour and relationships to encourage, support, regulate or intervene in. Decisions, increasingly based on personal information, are significant in determining outcomes for people – whether it is when applying for benefits, trying to get a mortgage for a new house, or deciding which photos to put up on a social networking site. In the case of government, there are very good reasons why at times these decisions are against the wishes of the individual concerned. However, because of the impact these decisions have on people, it is important that they have a chance to negotiate openly the terms of engagement, and what sorts of decisions this applies to.

Currently people do not have enough opportunity to do that. The relationship tips in favour of the data holder, who often has the means of coercion to exploit our desire for convenience and the benefits sharing data afford. But the tools that people use to learn about each other, communicate and share knowledge *can* be tools to tip that balance back towards the public – making 'surveillance' through information, and decision-making, something more people are part of. Not doing so means, as this pamphlet will argue, the potential for more 'pigeonholing', a narrowing of experience and a fragmented public realm.

We argue that policy on personal information needs to be based on collective rules and regulations that give people the ability to be more involved in how personal information is used. Instead of simply questioning data security, or wondering how to regulate flows of international information, we need to hold a debate about the basis on which information exchanges happen, the rationale for the profiling that takes place, and the means for accountability and redress. The question is not whether we are in a society dominated by surveillance, but whether that means more or less control, in this particular sense, for individuals over their lives, and over decisions and policy of collective interest.

1. Being watched, and needing to be seen

There's a lot of watching going on.
Roger Clarke, 'Have we learnt to love Big Brother?'[7]

As part of his 2006 Turner Prize display, artist Phil Collins set up a working office under the name 'shady lane productions' in Tate Britain's exhibition space. He and his staff worked nine 'til five researching 'the influence that the camera exerts on the behaviour it seeks to record'.[8] Their work drew on the experiences of people who have suffered from the compelling draw but often unseemly aftermath of involvement in reality television.

The focus of the exhibit was the power of others' eyes, and the ways that our behaviour changes before them. But the office itself stood within a high-profile, popular art competition. The lives of those within it became the subject of visitors' inquisition – visitors who were asked simultaneously to interpret the meaning and value of the piece itself while comprehending the significance of the job, behaviour and reactions of 'shady lane' staff. People stared and peered in, looking for answers from the office workers. Gallery attendants and closed-circuit television oversaw the public's reactions. Seeing all were the judges of the competition, charged with ascribing the institutional value of the exhibits, the public's views left on walls of postcards accumulated at the end of the show. There was no escape

from the watching, only inferences about the power that different people hold while it is happening.

Watching each other, watching us, watching them

Surveillance is usually talked of as a tool for 'Big Brother', an idea at whose heart lies a disconnect between individuals and the systems or institutions through which their lives are lived. From the authoritarianism of Orwell's nightmare, to the underground DNA vaults of the *X-Files*' evasive shadow government, the common story of surveillance is of a power with a malevolent or intangible intent.

Being watched through the exchange of personal information in our everyday lives has become ever more central to our identities, to our experiences of services, and to how we relate to other people. But the story of Big Brother cannot fully explain the significance of how personal information is used. A dependency on information-based 'surveillance' is in part a function of how we all now communicate, live and work together. Even though identity and social status have always been about how people are seen, personal information use is part of a change in *how* people are seen, and how they see each other – a change in how we should think of the word surveillance.

This chapter shows why there has been an increased prominence of what we will call 'interpersonal surveillance', and what it means for how we understand the potential power and control that surveillance through personal information brings. We argue that this opens the potential for more people to be involved in what surveillance is for: judging, sorting and responding to the people and ideas around them.

Being watched . . .

Instead of surveillance being something done *to* us, the sort that happens everyday is now almost as much about how we watch each other. Figure 1 sketches some examples of how this everyday surveillance looks. It is divided into four, with two key distinctions made. The first, between private and public, is based on distinctions drawn from our focus groups in which we asked participants to map

Figure 1. Everyday surveillance

	Public	Private
'Them' – institutional	● CCTV ● Congestion charging ● Traffic cameras/smart transport systems ● Health records ● Benefits and welfare records ● Tax and income details	● Loyalty cards ● Internet service providers ● Search engines ● Credit information (bank loans) ● Customer loyalty cards ● Oyster cards ● Children's database ● National DNA database ● Border control and passenger data
'Us' – interpersonal	● Reality television ● Fashion ● Facebook and MySpace (open privacy settings) ● News and current affairs commentary ● Citizen journalism ● Webcams ● Blogs ● Flickr sites	● Facebook and MySpace (closed privacy settings) ● Gossip ● Private detectives (honeytraps)

the information and activities they considered private and public. The second distinction is between 'us' (which we call interpersonal) and 'them' (which we call institutional), characterised by whether the watching in question is being done 'bottom-up', by people, or 'top-down', by organisations, institutions or businesses.

The grid maps the connections between activities like blogging and

photo sharing, the use of loyalty cards in supermarkets, to traffic cameras and CCTV cameras. They are all points at which our behaviour is seen and interpreted; they are the means for institutions, businesses and individuals to find out about and judge each other. The boundaries are fluid, and contestable – where each transaction sits lies a judgement about who decides what behaviour is appropriate in particular contexts. The way that information is recorded and used switches the emphasis of a transaction or of someone's behaviour from public to private surveillance, and between interpersonal or institutional surveillance. Encounters listed in one quadrant can overlap into other spheres. For example, the information on our loyalty card, produced through public behaviour, creates information many see as 'private'.

The top half of figure 1 details the more traditionally understood 'institutional' surveillance – where a business or government monitors individuals or groups and takes decisions based on that monitoring, or where the private sector tracks consumer habits and tastes. In the UK, strong tendencies towards government surveillance are clearly visible. Governments still look for better ways to regulate behaviour according to the values or principles they embody. It has been estimated that the UK has 4.2 million CCTV cameras;[9] and the largest DNA database of any country, with 5.2 per cent of the population registered on it.[10] Recent legislation gives a range of government departments access to communications data from phone records in the UK.[11]

Both government and private sector surveillance can happen when we are conscious of it – people often know CCTV cameras are silently absorbing the street scenes or bank foyers they are in, for example. And, as we shall discuss in the following chapter, people seem to happily give away details of their shopping habits for the benefits of a loyalty card. Often, however, we are unaware that active surveillance is happening. Sometimes, people are simply not aware that their behaviour is leaving a 'trail' – on the internet, for example. But, as people do not know or understand who has access to information, surveillance can be going on surreptitiously.

. . . Needing to be seen

> *Politicians often wallow in the act of baring their souls. We in turn expect them to demonstrate ever more of their private lives in order to convince us . . . that they live lives like our own . . . Celebrities live by a kind of striptease of their own privacy.*
>
> Perri 6[12]

The tools of surveillance mean businesses and government come to recognise, profile or differentiate the public. They also help people come to a sense of who they are.

The bottom half of figure 1 details what we call here 'interpersonal watching'. This type of 'surveillance' has come to play a bigger role in the story of contemporary surveillance. Institutional surveillance is about the authority that decides on a reading of a person's or group's behaviour. Interpersonal watching means people more collaboratively seeing, interpreting and judging. It is a process in which it is much easier for 'the many' to take part. MySpace, for example, gives people and groups the ability to build communities of interest around associations of bands and types of music. Citizen journalists, such as those involved in experiments like NewAssignment.net,[13] have the tools to report and comment on news. Bloggers comment and write, but also link and associate, meaning that they are building a sense of where they stand in relation to the ideas and people around them. Interpersonal surveillance is about people watching each other, and coming to a decision about people, the choices they make, and how they are valued.

But why has this interpersonal surveillance become such a feature of everyday life? Not only do we live through being watched, but equally through a *need* to be seen. The fascination with celebrity and the now fading love affair with reality television suggest a culture enamoured of display. Social networking sites like MySpace and Facebook work through a kind of fervent associative clamour, giving people the means to differentiate their 'profile' through the people, music, photos and opinions they connect with. Programmes like *Wife*

Swap purport to reflect different models of family life, and are predicated on people judging the merits and circumstances of the people taking part. All involve the surrendering of information in return for judgements, affirmation and recognition. We like to watch, and we like to be watched; the compulsion to perform our identities is a marker of how keen we are for the recognition it affords.

An important part of this story is the proliferation of access to the means of communication. For example, 61 per cent of households in Great Britain had internet access in 2007.[14] At the end of 2006 there were more active mobile phone subscriptions in the UK than people, up 4.2 million from 2005 to 69.1 million.[15] The mobile phone quickly moved from simply connecting voices to being a device that stores photos, audio and video from people's everyday experiences. Much of the internet now operates along the principles of 'Web 2.0', which places the emphasis on the content, links and associations created by the users rather than the creators of websites.

Now, people have greater potential to relay their experiences of everyday life back to each other, and these new ways to communicate serve a broader need. Greater insecurity in the sense of attachment and identity places more importance on the points at which people come to understand themselves, and their position in relation to other people. On the one hand, in a world marked by transnational flows of people and multiple identities, traditional monolithic identities such as class, race, nationality and political allegiance often overlap or become more complex. The 2007 report *Blair's Britain: The social and cultural legacy*, for example, found only one in ten British people mentioned nationality as most important in describing who they were.[16]

Yet on the other hand, the pull and significance of class or race have not necessarily diminished; difference and inequality have certainly not disappeared. A poll for the *Guardian* in October 2007 found 89 per cent of respondents felt they were judged by class, with 55 per cent saying that class, rather than ability, affects the way they are seen.[17] The final report from the Commission for Racial Equality argues that such inequalities have, in fact, become more pronounced:

> *Britain . . . is still a place of inequality, exclusion and isolation. Segregation – residentially, socially and in the workplace – is growing. Extremism, both political and religious, is on the rise as people become disillusioned and disconnected from each other. Issues of identity have a new prominence in our social landscape . . .*[18]

The meaning of those differences is partly about how things or people relate to each other. For example, a person's sense of religion may be informed by dogma and tradition. But it takes on meaning through experiences of other people and situations, suffusing the 'reference points' of everyday life with significance. Those reference points have changed dramatically, making our sense of who we are more fraught and sensitive, and placing more emphasis on the moments at which we work out who we are in relation to other people. The burden of identification has been pushed towards the individual, and the tools we use to stake out our social status are predicated on our being seen. Personal information is increasingly the raw material through which this happens.

Personal information and control

If surveillance is about the power to watch and interpret, but also to judge and regulate on the basis of that 'watching', then what does the new mix of institutional and interpersonal surveillance mean for how this works?

In each sphere of life, from Facebook to the workplace, there are norms of behaviour and rules of success or failure. 'Surveillance', whether by an authority such as the government, a business or employer, or our peers, is the key means through which our success or failure in these spheres is judged. This is important, first, because the judgements made structure organisations' responses to the needs, tendencies and interests of those profiled; and, second, they contribute to defining the relationships between people, and between people and ideas. Both of these result in differences of access, aspiration and outcome. As David Lyon writes:

> *[S]urveillance sorts people into categories, assigning worth or risk in ways that have real effects on their life-chances. Deep discrimination occurs, thus making surveillance not merely a matter of personal privacy but of social justice.*[19]

It is in the distinctions between 'them' and 'us' that power works, in bestowing authority on institutions or people to make decisions about others. The shift towards offering the means of communication, and surveillance, to the many rather than the few informs the rhetoric of new media, the internet and technology, suggesting that those decisions become more open.

However, decisions about how accessible information is, to whom, are often not decisions taken by the individual concerned, but by others. Staff at Oxford University have used the personal information on social networking sites to regulate and punish their students, checking the photos on their profiles to monitor behaviour.[20] Wearing slogan T-shirts not only differentiates a person visually (or superficially) but, if paid for by card, the point of purchase yields information about when, how and where it was bought. Government can request access to a range of personal information justified with reference to public goods like security and law enforcement, through to economic interests and people's wellbeing.

Our question, then, is: *has* the process of surveillance, sorting and judging become something more accessible to an increasing number of people? To answer that, the understanding of surveillance needs to be augmented with a description of the way we watch each other, in the countless spheres in which we are seen, sorted and assessed in everyday life. The discriminatory sorting that follows personal information use is not done by a single body, but as a response across myriad spheres to the desire and need to manage, relate with, regulate and sell to a population with complex and fluid identities. In addition to guarding against the mistakes and wrongdoings of large information holders – which remains an important task encompassing governments, international organisations and businesses alike – we need also to focus on the many different arenas in which we are

sorted and distinguished from each other. And with that, our understanding of control changes too. Control is less about being told what to do and when, and more about the shaping of norms of behaviour and the rules for success, the rationale behind the many spheres in which we are judged – by others or ourselves.

This is the broad sense of the term 'surveillance' used in this pamphlet. The condition of being watched has changed what surveillance and control mean, and it changes how we should approach the use of personal information. A reliance on databases, personal profiles and segmentation increasingly structures our everyday lives. Understanding the relationships between the watched and the watcher, relationships often marked by significant differences in power, is still the key challenge.

Personal information and the way it is used matters politically, and democratically, because it is intimately connected with how we are seen, represented and treated by the people, organisations and institutions that hold influence and power over us. It influences the 'space' that we have to decide and negotiate who we are and how we feel. It grows in significance, but becomes more difficult to control, in an era in which people readily take advantage of consumer convenience; where we flock to the engaging tools of social networking; where identities form along unpredictable lines, with unpredictable consequences; and where the state apparently has less of a claim to influence, determine or manage them.

2. The convenience of being known

What organisations and institutions do

The past years have seen a drive towards a 'personalisation' of services in the public sector, supported by a government emphasis on efficiency and an increase in the availability of and access to new technologies. There is a longer-standing private sector approach to categorising customers according to tastes, behaviours and past choices, and shaping what they offer based on what individual customers want, need or aspire to. Putting the individual at the centre of a service is considered to be empowering; yet surveillance is seen as negative, and disempowering. But the relationship between convenience and surveillance is close. To offer the personalised services we have become accustomed to organisations and governments have come to rely on millions of tiny parts of our identities, held together by increasingly sophisticated technology.

Information has become the tool that enables product and service specialisation based on individual wants, needs and aspirations. Instead of being about the disconnect between individuals and institutions, much of today's surveillance takes on the label of empowerment for the individual, by connecting them with institutions, and providing them with services or products they desire. It implies a relationship of mutuality and shared aims. This chapter explores the assumptions behind the personal 'offer' by looking at the practical reality of individually tailored services – first through the private sector, and then government. It maps the realities

of information use, what the consequences are, and outlines people's ability to influence the decisions made about them.

Private sector

It is the compelling pull of convenience – better service and product discounts for example – that fuels the growth of a plethora of banks of personal information in the private sector. These data banks collate preferences, tastes and behaviours, making it difficult to avoid leaving a trail of information in our wake – details of the average economically active adult in the developed world are located in around 700 major databases, for example.[21] Like a farmer's wife having to cross a muddy field with an identifiably soled shoe every time she sneaks to her farmhand lover's cottage, almost all of the points of interaction with the private sector yield a recordable 'footprint' – when we use loyalty cards that log purchasing habits, the gathering of statistics about consumer behaviour online, and tracking response rates and reactions to marketing emails (see box 2).

Box 2. Loyalty cards

Our mission is to earn and grow the lifetime loyalty of our customers.

Sir Terry Leahy, chief executive officer (Tesco), quoted in Tesco's 1998 annual report[22]

Tesco is one of the world's leading international retailers boasting an annual turnover of £43.1 billion and record profits of £2.28 billion in 2006, employing 450,000 staff worldwide, and currently operating 1988 stores in the UK – with plans to develop 142 more in 2007/08.[23] It is the market leader in its field.

Credited with placing the individual at the centre of its business model, the Tesco Clubcard programme – which includes ten million active households, captures 85 per cent of weekly sales, and sends four million unique quarterly mailings[24] – is driven by the

desire to provide tailored services to each individual shopper. Jim Barnes, executive vice president of Bristol Group, a Canada-based marketing communications and information firm, and a customer relationship management expert, said:

> *They (Tesco) know more than any firm I have ever dealt with how their customers actually think, what will impress and upset them, and how they feel about grocery shopping.*[25]

Through monitoring customer behaviour via its Clubcard, Tesco uses complicated customer segmentation methods to classify customers as cost-conscious, mid-market or up-market. From there it breaks them into categories like healthy, gourmet, convenient and family living. These sub-segments are then segmented into even smaller groups and communications are tailored to each, creating a unique picture of every Clubcard user based on their retail habits.

In the five-year period following the implementation of the Clubcard programme, Tesco sales increased by 52 per cent and continue to grow at a rate higher than the industry average.[26] Store openings and expansions have increased Tesco's floor space by 150 per cent, and the company has managed to reduce promotional costs, improve focus on their 'best' customers, and build relationships with other organisations.[27]

'Shared insight' means that Tesco's major partners – consumer packaged good suppliers, media companies, researchers, space planners and more – have access to the customer information that is gained from the Clubcard programme. This 'cooperation' is not unusual, the website of the Nectar card, of which Sainsbury's is a part, reveals over 90 participating companies, all of whom can access and use associated data.[28]

Using these databases, there has been a move towards marketing mass-produced goods at carefully understood segments of the

consumer population or, in some cases, towards offering more tailored services. This shift is seen as empowering; by enabling people to define themselves through products that reflect or project certain values and aspirations – for example, using a RED credit card allows someone to be seen as committed to fighting HIV aids.

The private sector targets in this way by doing three main things with the information it gathers:

1. *Segmenting customers*: Grouping customers – according to past behaviour – helps businesses understand who their customers are. Categories like 'economiser', 'self-confident' and 'home-oriented', or the more detailed 'soccer moms', 'office romancers' and 'extreme commuters'[29] create a picture for businesses of who they are working with, and how to shape their offer.
2. *Marketing*: Working with detailed pictures of customer categories businesses can then market products to particular groups, in particular places, at particular times, saving time and money on promotion, while still reaching a target audience.
3. *Developing brands*: Finally, businesses want to understand the aspirations of their customers, in order to develop a 'relationship'[30] with them. Understanding who likes them and who doesn't, what works and what fails, can help organisations tailor their brand to keep existing customers and attract new ones.

The private sector gives customers a sense of what the information is for, and offers rewards in exchange for personal data. It builds trust and business by emphasising choice and consent, while simultaneously categorising its customers – sifting through large databases using complex mathematical formulas to discover patterns and predict future behaviour. So the convenience associated with private sector transactions is predicated on the close information-gathering relationship between consumer and business. Information is

produced not only through consumption of products, but also through the way we behave and associate. For example, the internet is rich with tools for collaboration that thrive off connections between people based on shared facts about them. But Tim O'Reilly spots the coincidence of business and convenience motives:

> *[There is] a major theme of web 2.0 that people haven't yet tweaked to. It's really about data and who owns and controls, or gives the best access to, a class of data.*[31]

Whoever gathers a specific set of data related to a kind of activity – career information or travel habits for example – owns a powerful tool to help businesses 'understand' and react to the public. Personal information becomes, then, an increasingly valuable asset in itself. It helps develop ideas about when and where to sell things to people.

Despite awareness that the gathering of information creates service benefits for customers, little is known of the precise connection between the two. This is partly because of a lack of awareness about exactly what is done with or to personal information, and what the consequences are. Part of the secrecy surrounding this is driven by concern in the sector about people's reactions to the level of information gathering that happens.

But the demand for an end to that secrecy is hardly deafening. Despite growing awareness of how much information the private sector handles – perhaps driven by the press, as the *Independent* headline 'Google is watching you' suggests[32] – it can be difficult to express why this matters. The ability of the private sector to control or coerce its customers can seem low – it does not openly tell people what to do. Usually, concerns about the personal information given away are hard to articulate; discussing what information loyalty cards hold often ends with retorts such as: So what? We get cheaper beans. But the reality is more complex – there are problems associated with the justifications for private sector use of information: people's choice and consent.

First, the ability to opt out of information gathering is inhibited by

a sort of coercion; our ability to access services or products often depends on agreeing to privacy policies or data sharing notices. These are presented, often, as benefits of participation – cheaper fares, better designed websites – but they demonstrate how price and rights to access can serve as tools to distort the justification of consent on which the private sector finds much of its legitimacy. Second, it can be difficult to negotiate the 'terms of engagement' – if we want to use a service or product, however important, then the choice is usually between accepting the privacy policy offered or leaving. Third, one of the central goals of marketing is not only to understand choices, aspirations and needs, but to mould and influence them.

So there are problems with the story of convenience. First, there is a potential 'narrowing' of customer experiences as a result of more targeted, customer-centred service. Certain products strengthen existing habits, and limit opportunities to move from one type of behaviour to another. Newspapers, like supermarket products, are often targeted at particular groups, creating the potential for people to construct a personal cultural diet. Families receive vouchers and brochures for certain kinds of holidays, or different kinds of financial services. These micro-level examples have disproportionate implications for how we live together and our feelings of mutual belonging and responsibility.

Second, the private sector does not have to address the value of people's decisions, or the social context that shapes them. That means, potentially, an impressively segmented public but one that has little regard for the impact of these categories in a social context. These are decisions, as we shall explore further later on in the pamphlet, that could deepen inequalities of access, aspiration and outcomes – involving, for example, increasingly targeted financial products – insurance or lending options – for those on a lower income, or limited employment options for those with a history of poor health.

It is more difficult for the public sector to claim neutrality of judgement. There is an assumption that businesses will not tell you if your basket of shopping is healthy or unethical. The state has more of

an inclination, or incentive, to do just that. The question of power and control becomes more obvious, then, in the case of the public sector.

Personal public services

> *Our great ambition now: a National Health Service that is also a personal health service.*
>
> Gordon Brown, Labour Party conference speech, 2007[33]

In terms of service delivery, government aims to gather and use information for two main reasons: better and more efficient personal public services, and increased safety and security. The latter involves the processing and authenticating of passport applications and national security surveillance, for example. The former is part of a three-fold effort evident since 1997: increased emphasis on technology as a tool for government; a private-sector-style efficiency drive in service design and delivery; and a focus on personalised, citizen-centric services. Initiatives like e-government[34] and trans-formational government[35] further emphasise increased, and more efficient, information use as a priority. That involves checking benefit claims for fraud, changing how government websites work, and using and storing medical records in new ways.

Our focus in this section will be the move towards personal public services; and how personal information is central to its success. The three examples below – Connecting for Health,[36] ContactPoint[37] and the identity card scheme[38] – help to illustrate the government's aspirations and attitudes, draw out what government policy looks like, and show whether, combined, they offer a means to achieve the aim of empowering people through personal information.

Personal information and wellbeing

Connecting for Health is the name given to the nine major projects and £6.2 billion investment into modernising healthcare in the UK, including plans to improve how medical information is stored and shared. The project aims to replace the disjointed IT systems pre-

viously used by doctors and the health service by connecting around 5000 different computer systems with a nationwide infrastructure – one that supports a better interface between patient and service, facilitates better communication between health professionals, and makes storing and retrieving medical information simpler.

The ContactPoint database is considered a key part of the Every Child Matters agenda by government. It forms part of the drive for more 'joined-up' services, claiming to help identify children at risk, and provide better services to children and their families. The database – which will cost £224 million to build, and another £41 million per year to run[39] – will contain the name, address and gender of all 11 million children in the country, as well as contact details for their GPs, schools, parents and other carers. Access to the database will be available to an estimated 330,000 vetted users – including teachers, doctors and social work staff.[40]

There are real benefits to both of these. Letting doctors share records more easily brings some bureaucratic benefits such as easier to locate records that are accessible to the patient, which can translate into tangible benefits in terms of people's experience, quality of care and, ultimately, health. Similarly, the children's database potentially helps highlight 'at risk' young people, and connects the professionals who have the ability to intervene.

But, there are coincident questions of data security, contracts and third-party access to personal information given to the state, all of which need serious examination. These were singled out by Gordon Brown in his speech on liberty in October 2007:

> *A great prize of the information age is that by sharing information across the public sector . . . we can now deliver personalised services for millions of people . . . But if governments do not insist on accountability where people's data is concerned – and are not held independently to account – then we risk losing people's trust, which is fundamental to all these issues and more.*[41]

The common thread connecting both of these examples is that they

concern the decisions government makes about two sensitive areas of public policy: health and child wellbeing. The personalisation approach looks to improve services for people by becoming closer to what they need. And that rides on the collection of personal information, which in turn changes the kind of decisions and interventions government can take.

So, the power government holds to act in the common interest contributes to a suspicion as to how that power will be used. Trust in government to take those decisions is therefore vital. Many people would prefer to be in control of their own choices and outcomes, as recent examples from health and social care demonstrate.[42] That means government's job is not just that of creating the infrastructure in which more decisions are taken on the basis of personal information use. It also has to encourage a shift in the public's attitudes towards, understanding of, and democratic consent around its role, and be transparent and consistent about its aims and remit.

Bottom-up or top-down?

That transparency is currently absent, and decisions about how information should be used are, often, top-down. The drive for ID cards and NHS IT reform emanated from the centre, provoking media controversy and garnering little support on the ground.[43] Even though there are some real benefits to government using more information in better ways, the lack of clarity in the connection between the purpose and role of government, and personal information gathering, means that 'function creep' and risk management overrides debate about what the role and purpose of personal information use should be. This contributes to a situation in which people do not feel they have choice or control in the public sector – that they are subjected to surveillance in the name of the public good, rather than actively helping to shape it. The 'deal' people get from giving away personal information to government can seem like a surrendering of power, rather than an engagement with a service.

The British Social Attitudes Survey found that in 2005 just over 53

per cent of respondents thought that every adult should have to carry an identity card.[44] Yet the Public Accounts Committee, in a report on the workings of the Identity and Passport Service, insisted that:

> *the Home Office needs to explain the underlying rationale as to why citizens need an identity card as well an ePassport.*[45]

One of the key problems is that arguments for the cards have tended to be put forward on the basis of their institutional benefits – reduced fraud and security, for example – rather than on the benefits to individuals.[46] That is a problem because government has failed to connect those common or institutional goods with people's individual experiences. The connections between, on the one hand, why people will have to carry cards, where and how they will need to use them, and how the technology and management will work; and, on the other, the reduced security threat or better fraud prevention, are not clear enough. That has fuelled suspicion that the project is driven by technological possibilities and bureaucratic convenience rather than democratically debated social utility.

The approach to identity cards is indicative of two main problems in how government approaches personal information. First, government is often not good enough at connecting the top-line, institutional justifications mentioned above with benefits and costs to individuals. Second, it suggests opportunistic assumptions about the rights of government to access and hold personal information.

This opportunism is a key point. It is difficult to separate information gathering and use that happens in the name of security or risk reduction, and for the purposes of personalising services. Arguments about risk reduction mean security services have more access to a broad range of information, which often leads to more extensive *gathering* of data. That ultimately offers a wealth of information for the broader aims of personalising of services. This relationship helps to explain the appearance of 'function creep', and the sense that the 'deal' in any exchange or surrendering of information is unclear.

For example, the recent focus on enabling and justifying government use and access to data through changes to the Regulation of Investigatory Powers Act[47] in October 2007 coincides with an updated data retention policy that clarifies how long certain communications companies should retain data.[48] The changes were passed largely on the basis of security in the wake of apparent attempted bombings in London in 2007. But it extends the range of officials able to check certain kinds of communications data well beyond the needs of national security.

Who's in charge? The merging of private and public

The use of personal information in both private and public institutions holds particular challenges for each. But perhaps the most important factor in the development of personal information use is the merging of public and private sector roles. This developed through the contracting out of public service delivery to the private sector in the 1980s, and has progressively blurred the distinction between the two as their functions intertwine. This has served to exacerbate the questions of power, responsibility and coercion in both.

This merging coincides with an increase in demand for good quality, comprehensive data, and competition among data suppliers, making connectable information about every aspect of an individual's life easier to come by than ever before. Personal information has become, as a result, less easy to segment in terms of what is relevant for public or private sector purposes. One of the clearest examples of this trend playing out is through credit agencies, which provide the information that forms the basis of risk judgements by others – such as banks and loan companies. Having traditionally been tasked with checking customer credit ratings for banks, mortgage providers and estate agents, they are now under pressure, from government and business clients, to increase the *types* of data they hold – going beyond credit towards lifestyle choices and behaviour – in order to give a more complete picture of the risk, or level of 'trustworthiness', associated with an individual. As one credit agency representative told us:

> *There are already people thinking about where to put an expanded range of information, and how to treat it – because there are pressures to include information beyond traditional definitions of credit checking. We're moving from describing ourselves as a credit agency to being a business that deals in risk management.*[49]

The result is that credit agencies become involved in decisions that are not about credit. The availability of this kind of information risks decisions being made about people on unfair grounds – in the future, armed with comprehensive data about clients, firms may be able to choose customers rather than the other way around. The life insurance market, for example, which traditionally pooled the risk of high- and low-risk clients, might choose to exclude people with poor access to health care or particular lifestyles, based on the level of risk they pose.[50] This implies a change in the role of the state, and new kinds of responsibility on the private sector and individuals. In these circumstances, does government act as guarantor, for example?

The lack of consistency and coherence in government strategy and policy around information sharing makes these challenges difficult to address. The increased prominence of interpersonal surveillance and the reliance on personal information mean the individual decisions people make about giving away personal information are ever more important. There is a risk that in the longer term, as private and public roles and responsibilities merge and blur, information from our everyday lives – the 'footprint' of our choices and behaviour – will be used to make important decisions we would not have anticipated. Without clarity over purpose, it becomes impossible to understand, and even harder to challenge, the rationale for the judgements being made. The failure to debate changing rules of access to additional information by government and its partners contributes to lack of awareness, and thus informed action, by citizens.

3. We care, but we're not sure why

Attitudes to personal information

Days in the life

John wakes up to the sound of his mobile phone. He checks it for messages and heads for a shower. Afterwards, he switches on his computer and, over breakfast, reads the news online a little too leisurely. He dashes out, forgetting his Oyster card is low, and runs for the tube. His automatic top-up, direct from his bank account to his Oyster card, means he gets to work on time. He swipes into his office, climbs the stairs, and logs onto his computer. John had forgotten to pay his council tax in advance, so his first job is to get online and pay through the council website, before calling his gas company to pay off an outstanding charge. He works until lunchtime, taking some calls on his mobile, and checking his Facebook page at (too) frequent intervals. For lunch he has a sandwich and a smoothie from the local supermarket – boosting his loyalty card points – and he pays on his debit card . . .

Molly gets up late. Her taxi arrives to take her shopping after calling her to let her know it's on its way. She gets into town and visits the shops – butcher, baker and grocer. She pays in cash, which she takes out of her local post office account. In the post office she pays her phone bill and her TV licence. She watches flickering, grainy CCTV images on a screen as she waits in the queue. She calls another taxi using her mobile phone, and goes home via the GP surgery – she needs her leg checked. She is preoccupied by the GP typing at the

computer as she speaks – he barely looks at her. She wonders why he needs so many details. On the way home Molly picks up her prescription and buys a magazine – she likes the competitions. She gets home, unpacks her shopping, before booking flights to the United States – a family holiday tradition – over the phone. For the evening she settles in front of the TV with a magazine and catalogue and nods off . . .

John and Molly's days are based on personal 'information diaries' we collected as part of our research. Their stories are indicative of the central role personal information plays in our lives. But the rate of technological change and everyday professional practice can move faster than the public's awareness. As the previous chapter showed, the way that institutions gather and use information can be opaque, and difficult to grasp. Though people are beginning to understand how their information, with or without their knowledge, is used and what the implications are, that understanding is marked by ambiguity. In this chapter we will explain why this is, focusing on people's attitudes and understanding. We will be drawing on our focus groups, and on a range of attitudinal work that has been carried out in the last few years into privacy and the technologies of information.[51]

Do we care?

Often the concern expressed at a general level about the rights of others to monitor and gather information about us is not matched by the things people do to protect their personal information. Our newspapers almost weekly cry 'Big Brother', normally criticising government surveillance, but in the more recent past 'exposing' the databases that lie in the hands of the private sector – from supermarkets tracking consumer behaviour to search engines gathering intimate details of our lifestyles, interests and concerns. Seventy per cent of those surveyed for the Oxford Internet Survey said going online puts a person's privacy at risk.[52] But still we have taken to the smooth convenience of online shops – pushing the value of 'e-retail' sales to £4 billion in July 2007, up from £1.8 billion the

previous year.[53] Despite rigorous border control measures – fingerprinting, passenger information demands[54] – demand for travel to the US continues to grow.[55]

Decisions about when and where to share information tend to look like small, personal risk assessments. Context and choice have become crucial in shaping attitudes to the use of personal information, and in determining our behaviour. Our ideas about when, where and how information is being used is the first step to making a judgement about how appropriate it is, and what can be done about it. The problem is that those ideas are formed through a haze of difficult to comprehend relationships. Marked by ambiguity, those personal cost–benefit analyses tend to be dominated by the benefits – convenience – rather than the often intangible costs – cultural narrowing and social exclusion.

The primary cause of this ambiguity is confusion about distinctions between what is public and private. As well as the merging of the roles of the public and private sector discussed above, there is more discrete merging of our public and private spheres. In our focus groups the things that people considered private could be broadly split into two types. One was deeply personal: our relationships, our homes, our bodies and our possessions; the other seemingly less personal: the services we use and how we use them – bank details, shopping habits, the internet.

These distinctions hold the key to understanding attitudes to personal information. Some of the confusion mentioned above can be put down to complicated language, and a lack of transparency in how information is used, who has access to it, and why they want it. But, importantly, the effect of this lack of transparency is compounded by changes in the distinctions between what is personal, private and public. That complicates the lines we draw between the most intimate elements of our private realm, and the more extraneous pieces of information – such as our shopping habits, where we like to spend time, and what we read and watch.

It can, as a result, be difficult to work out when and where we are being watched. There are new spaces in which our behaviour and

information can be seen and, therefore, judged. Being 'in private' while we are being watched – through the logging of our behaviour online by internet service providers or search engines, monitoring by CCTV cameras as we travel across cities, and 'listening' by invisible ears while we chat on our mobile phones – creates new situations and contexts in which people can find out about us, and take decisions about who we are.

But does it matter?

There are four main problems arising from this: the consequences of personal information use; responsibilities associated with those consequences; levels of accountability for when things go wrong; and the amount of power others hold over our decisions and behaviour.

Consequences

The paths our information follows are often opaque, and the precise role of the information holders can be difficult to grasp. So the consequences of giving away or losing control of personal information can be hard to understand. For example, how do our current shopping habits influence our future choices? Who gets to see information about my behaviour on a website – what I buy, or how long I spend reading what, for example – and what do they do with it? And how can we be sure about where our passenger information goes when we enter the US? How do we know if we have been selected as suspects on a terrorist monitoring list – based on a complicated risk assessment procedure – and what power do we have to alter incorrect decisions?

Responsibility

Even if we are sure of the consequences, why does it matter? What can happen to me? Responsibility in the realm of personal information is a murky area. Banks and retail outlets have thus far taken full responsibility for any misuse of customer information, reimbursing customers for stolen cards and online fraud. The recent TK Maxx

story, where hundreds of customers had their bank details stolen, severely damaged the company's reputation, but affected customers were fully compensated.[56] Banks are constantly developing new tools to secure online transactions, yet when things do go wrong they take full responsibility, not the customer. But how long can this continue? 'The banks can't keep coughing up forever', according to one focus group participant, while another claimed not to worry about protecting his personal financial information because 'the bank will sort it out'.

As people become more aware of how to manage personal information, and are equipped with the necessary tools, will the burden of responsibility shift away from organisations and towards individuals? What are the obligations of banks or the government, or individuals themselves, to raise the levels of awareness of the smart uses of personal information? In a world where information is the single most valuable commodity in the criminal world,[57] clarity around roles and responsibilities of both service provider and consumer becomes critical.

Accountability

People's decisions about whether to make purchases online are increasingly based on past experience, and the strength of an organisation's reputation and brand. Relationship building and trust between individuals and organisations has become important – we might shop online at Amazon.com because of positive stories and previous experience, but may choose to be wary of the NHS based on technological incompetence in the past. This shift in what matters to consumers is driving a new responsibility among companies and service providers to prove their ability to handle information securely – NatWest now sends a handheld PIN device to customers' homes to allow them more secure access to online banking, and eBay – an online community 'built on trust' – prides itself on providing extensive 'tools and education to help users stay safe while transacting online'.[58] It is usually easy to spot declarations about the value of people's privacy in organisations' mission statements, even if it is

more difficult to ascertain how that declaration is followed up in practice.

Those in our focus groups perceived the private sector to be more accountable than public sector organisations in matters of information security. That sometimes involved claiming that the impact of bad practice on the private sector is more damaging – businesses risk rapid demise, as consumers refuse to accept bad practice and vote with their feet. AOL, the internet service provider, suffered serious damage to its reputation, and lost three staff members, including its head of technology, when it released details of 23 million searches carried out by 650,000 customers in August last year. Having felt safe in the way they were open only with selective information, they had nonetheless failed to anticipate the ease with which users were identifiable through what they did release. The reaction was sharp. But it was still marked by a sense of confusion about consequences or forms of redress, as well as simple accountability.

Perceptions of government's track record on IT failure – the quiet axing of the Department for Work and Pensions' Benefits Processing Repayment Programme,[59] HM Revenue and Customs' almost annual IT difficulties with tax returns,[60] and the revealing of junior doctors' personal information online[61] – fuel people's concern.

The power and role of regulators, auditors, select committees and ombudsmen to severely punish government or businesses for bad or negligent practice regarding information use was seen as slight by our focus group participants, or was not understood. This is in part down to the opaque process of legislation and policy decisions in this area, making it difficult for people to understand what the government is doing and why.

Control

These ambiguities exacerbate the difficulty of knowing what the consequences of the 'convenient' lifestyle offered by the private sector might be. We know that the private sector can influence decisions, shape choices and improve individuals' service experience; but, as we

have noted, it does not *claim* to make value judgements about people. The public sector meanwhile is perceived to make judgements and take actions that can change lives. However, as we discussed in the previous chapter, these fine distinctions between the responsibilities falling on the public and private sector are not easy to make.

Underneath the surface of our acquiescence to consumer convenience and choice are serious issues of power and control. In the individual risk assessments people take, convenience is often more heavily weighted than the vague notion of control. Clarifying the confusions outlined in this chapter is important, because it allows us to navigate the information society as informed individuals, rather than passive, trusting consumers. When that understanding takes shape, there are a number of methods and tools people can use to help them manage information accordingly. These methods and tools are the focus of the next chapter.

4. Protecting and promoting

Data protection and digital identity management

Search engines are about making information more accessible. Google's mission statement, for example, is 'to organize the world's information and make it universally accessible and useful'.[62] Their algorithms do much of the hard work – scouring, sorting and prioritising. This shifts the barriers to discovering information, something the internet more generally has become famed for. For example, it is now much easier to find out about what is said in parliamentary debates.[63] Access becomes less about who you are, and more about where you are – whether you have access to the internet.

But access is also, still, inescapably about money. The debate about 'network neutrality' serves as a good example of how the 'flat' design of the internet and open information tools might be changing. The debate concerns the concentration of access and traffic in a small number of telecommunications companies. It focuses on the implications of distinguishing between internet users based on their ability to pay, systematically prioritising, for example, the traffic of a City finance firm over a grandma from East Ham. The long-term consequences of this damage the principle of the 'flatness' of access, which is borne of the blindness of intent the internet architecture was built around. Instead, it builds in decisions about what kinds of activity and people the technology should serve and promote.

This is indicative of the internet's direction of travel in terms of content, too – away from a series of connected documents, towards bits of data connected through the meaning people give to them. Tools like search engines are seen as empowering – giving people access to new sources of information. But just as in the debate around net neutrality, technology is starting to embody a particular kind of limit to access by shaping what is on offer around decisions about who you are. Google, for example, is working to 'personalise' its service, potentially giving more 'relevant' searches by moulding search results around users' history and apparent preferences. For example, it already responds to health searches based on 'expertised' categories from trusted medical sources, and has plans to use individual medical records to further 'personalise' its response in the future. This is about inserting *context* and meaning back into words and associations of words, with the inevitable consequence that they become more relevant or appropriate for some people than others.

This chapter looks at the means through which people can try to manage and control what happens to their personal information. The examples above demonstrate how inseparable the two main tools for regulating the use of personal information – data protection and digital identity management – are. Empowering people through their personal information has to be just as much about negotiating and managing the way other people 'see' a person – through their personal information – as it does securing it. The examples highlight the tension between individuals' decisions about rights over personal information, and institutional or organisational rights to use and make decisions on the basis of it. There is a consequent tension between 'top-down' solutions to the management of personal information and 'bottom-up' approaches.

Data protection and the privacy paradigm

Data protection (DP) is an area of law that seeks to maintain an individual's limited right to privacy by regulating the collection, use and dissemination of personal information regarding the individual.[64] It is about making sure that the whereabouts and

security of, and access to, information is managed or regulated. Its recent history in the UK can be traced back to 1984. The act passed in that year, and its subsequent revisions, place important rights in the hands of individuals – or 'data subjects' – whose information is held by others. But it also gives license to organisations – data 'holders' – to use information in particular ways. DP legislation looks to manage both a person's right to control what others do with information about them, and the financial, bureaucratic, social or organisational benefits others might derive from using it. In Europe, DP legislation acknowledges the value of personal information; regulation has moved from having an emphasis on individual privacy towards recognising the interests of those that benefit from information use – organisations and governments.

Data protection is rooted in what Colin J Bennett and Charles Raab call the 'privacy paradigm'. They argue that modern DP regimes are predicated on a particular assumption about the distinctions between individuals, other people, and 'society' – and between public and private.[65] But there are a number challenges to how data protection works within this paradigm.

The international context

Personal information does not respect the boundaries of nation and region through which the regimes to manage it operate. That is partly because the technology, to some extent, is equally disrespectful of borders, partly because people connect socially and for business purposes across and between those boundaries, and partly because organisations, and organisational needs, stretch across the world.

Peter Fleischer, Google's global privacy counsel, argues in the Demos collection *UK Confidential* that global privacy standards are needed to provide a framework that matches the unbounded nature of information.[66] The nature and severity of those standards then becomes an important question, along with the accountability and legitimacy of the standards themselves, and the regulatory body designed to oversee them.

Public/private relationships

The merging of the roles performed by the public and private sector affects how personal information is used and gathered for a range of important services. For example, Census 2011 will outsource some data collection and handling – including information about 'sensitive' topics like income, race and ethnicity – to private sector contractors. This raises questions about the clarity, accountability and security of information gathered within the remit and with the authority of the public sector, but undertaken by private businesses. Problems around clarity of purpose are compounded when the job of maintaining a service is passed on to a business with different channels of accountability. Systems and auditing might be clear and secure, but the integrity of the information is entrusted to a set of people, with differing motivations and incentives.

Linking and forgetting information

Storage costs of information reduce over time, meaning questions of how long information should be kept, and when and where it should be connected to other sources of data, become more prevalent and fraught.

Individual or group rights

One of the mistakes made in thinking about privacy and the use of personal information is focusing too heavily on information that is personally identifiable – or traceable to an individual. Just as important are the groups or broader profiles into which people are put; in short, what kind of privacy or information rights groups hold.[67]

Identity management

There are further challenges for how personal information is managed. The most recent revision of data protection legislation was in 1998. Then, online social networking was barely heard of. MySpace – a popular site to associate with friends and display profiles – did not

launch until 2003, with Facebook following a year later. Such a simple change in how we interact and share information with one other, and with organisations, is indicative of the disconnect between legislation and our day-to-day realities.

This can have serious consequences. In October 2007 the All Party Parliamentary Group on Identity Fraud warned of the dangers of people's fervent desire to use social networking sites. Our loose lips in the informal connected realm see us freely displaying our phone numbers, addresses and birthdays. The group recommends that government play a role in deepening people's understanding of the dangers of carelessness in what we show to whom, and in explaining just how useful and valuable personal details online can be to fraudsters.[68]

But crucially, the connections between the more organic understanding of identity and the institutional sense are missing in the parallel debates about the social values of technology and bureaucratic identity.

Importantly, with the increasing interdependence between on- and offline worlds many people's 'digital' and 'real' identities are barely separable. But it is difficult to make the connection between a general willingness to use technology to build incredibly personal profiles and reflections online, and the more technical understanding of what our 'identity' is. Connecting our social identity with 'identity' in a more technical sense – the details businesses and institutions see and interpret – is difficult. How we use technology is important in this process – rather than digital identities being separate from our 'real' self, for many of us they are more and more important to how we build a sense of who we are.

Identity is not static, but fluid and changeable, shifting in different contexts: at work, with friends and at home. To respect the many different ways people project themselves in different spheres, the ability to disconnect these different contexts is important. The problems of not being able to draw these lines are three-fold. It increases the likelihood that people can commit 'identity fraud' by using readily available personal information to lie about who they are

to obtain credit, goods or services. It makes it more likely that people will be, seriously or otherwise, 'misunderstood' as personal information about them is read out of context. And, it makes it more difficult to be sure about who will be able to see what personal information and why.

For example, organisations often ask us to 'authenticate' our identities using information like our date of birth, or mother's maiden name, but for any committed impersonator these details are easy to find out, and for most of us they are not private. Bill Thompson addressed the problems associated with traditional authenticators on his blog earlier this year:

> *[Personal] information should apparently be carefully protected because criminals can use it to fill in applications for credit cards or loans, stealing our identities and causing all sorts of problems. This seems to be entirely the wrong way around.*
>
> *I have never kept my birthday secret from my friends, partly because I like to get cards and presents, and I do not see why I should have to keep it secret from my online friends. If that means that other people can find out about it then the systems that assume my date of birth is somehow 'secret' need to adapt, not me.*[69]

The role of data protection needs to be seen in this broader context of how institutions and others find out about people, and how they change their 'offer' as a result. In that context, there is an emerging and developing role for tools of identity management.

Digital identity management (DIM) is about how we relate to other people, to systems or to institutions via the personal information held about us. It extends to the ability to manage our own data and how it flows, allowing individuals some control over what and how people find out about them. DIM focuses on where the individual sits in transactions of which they are a part. The relationships that DIM applies to differ from 'real world' or offline relationships in two key respects: first, how they demonstrate that the

person somebody is interacting with online is really that person, and, second, the context and credentials needed to complete a transaction.

DIM allows us to develop different ways to identify ourselves that are not linked to our personality or family, but are purely transactional in nature – a number or identity code for example. Technologies that might be grouped into the field of identity management include tools to help individuals or businesses 'protect' how their personal information is used – programmes that anonymise internet browsing,[70] browser settings that prevent or manage the use of 'cookies',[71] and document encryption tools. But DIM is more than these. It is about an infrastructure that helps individuals know about, and decide, where information about them is kept. It also helps to set rules about who can find out what about an individual, and how much information they can ask for in a given context. It opens up negotiation about the kind of 'proof' needed to complete a transaction – how to prove who I am – and how connectable pieces of information are, both to other bits of information and to the person they are 'about'.

But the way that government has responded to challenges of personal information use reveals a potential tension. Legislation can counteract individuals' attempts to protect information – the focus on enabling and justifying government use and access to data through changes to the Regulation of Investigatory Powers Act[72] in October 2007 coincides with an updated data retention policy that clarifies how long certain communications companies should retain data,[73] and potentially extends the range of officials able to check certain kinds of communications data. This extends to the debate over top-down initiatives of DIM, and bottom-up initiatives that stem from business or individual needs.[74]

The value and meaning of personal information

One of the legally established principles of data protection is that personal information gathering should be done on the basis of informed consent. But given the problems highlighted above, there is a sense of information asymmetry – much greater knowledge on one

side of the interaction than the other. People are often unaware of, and not invited to engage in, the context in which decisions about information use are made. So far, data protection law has not in itself provided adequate means for democratic engagement with these principles beyond the redress offered through norms regulated by the Information Commissioner's Office.

Data protection and identity management are essential in helping to place people at the centre of an information society, and to offer democratic engagement. Yet the complexity of language and technical details associated with both can be off-putting. Data protection is governed by a combination of difficult to understand legal arrangements and legislation, and often opaque presentation in the everyday – usually in the form of badly written, jargonistic privacy policies. DIM is often seen through the lens of technical possibility, meaning that discussions of people's practical and everyday aspirations – how they want to use technology – become secondary, overshadowed by technological boasts about decentralised or centralised networks or splendidly complex cryptography.

It is a failure if identity management or data protection are too complex for non-technologists or mathematicians to understand, because this process is fundamental to the way that institutions, businesses and other people find out about who we are and decide how to react to us. This is especially true now, as technology becomes ever more central in mediating 'relationships'. For example, the privacy policies on a social network can determine the level of ownership over the content the user puts online. And further, the design of identity management 'systems' like the national identity card scheme determine where personal information is held, for how long and who can access it.

We do not expect to exert full control over what is said, known or thought about us. Bits of information are needed about us by others, usually governed by principles or rules about when and where it is appropriate for people to have access to that information. So, for example, if we want to buy a house, then the bank lending us the money to do so might run a credit check – the information fed to

them is the basis on which they can make a judgement about the kind of people we are. Less instrumentally, people need to share and learn about others; to share thoughts and feelings to build a sense of understanding over the world around us. Usually, there are means of redress if a person believes another's opinion is incorrect or damaging in some way. 'Digital identities' – either the ones we actively help produce or the identities held in electronic form by institutions – are increasingly as intimately a part of these processes as people's offline selves. Personal information is the raw material for this, and DIM offers a simple question: how do we think we should prioritise claims over how personal information is managed?

But, in this respect, how heavy do we want the rights of individuals and institutions to be? Giving too much power to the 'owner' of the personal information would be too constrictive, just as giving too much to the data holder – the e-retailer, the marketing firm, the government – removes the element of negotiation. As with other 'tradable' intangibles like music, personal information has both a value and a meaning. The value may be easier to barricade and form rights around, but the meaning of personal information is something that requires much more open and fluid negotiation. Arguing for this open attitude in the realm of personal information and identity – where the ability to challenge, debate and construct new meaning around our relationship to other people is fundamental to a functioning democracy – should be easy.

But at the moment it is not. Too often, despite the rhetoric of convenience, the institutional or organisational benefits outweigh the claims of individuals. There are some serious benefits to allowing others to use and share personal information, from better health care, safer places, cheaper clothes and more efficient public services to the connections we can make socially or culturally. But at present people are too far removed to wield any serious influence over where and how limits and regulation work.

Different technological 'architectures' allow information to flow in different ways. In the way technology is designed, there is an opportunity to embed the level of control an individual has over their

personal information. In the choice between the top-down and bottom-up models lie these questions of control, autonomy and power. So the way that both DP and DIM develop requires some political choices, which will inform the mix of decentralised, bottom-up technology and practice. The choices are bound up in broad political challenges associated with information, openness and the role of government. They directly affect whether people are empowered or controlled by information. And they are also, crucially, bound up in how responsibility is balanced between individuals, institutions, organisations and the state. It is to these challenges we turn in the next chapter.

5. The new politics of personal information

Rational distinctions between types of people based on their personal information can lead to differences between what those individuals experience and have access to. This can result in a narrowing of experience, can exacerbate social exclusion, and can have significant consequences for how we live together as a society. This is the political battleground of personal information.

But these links between increasing use of information, in new contexts, and how we live together are not commonly made. Instead, a distorted sense of convenience drives the exchange of information, and justifications like national security tend to excuse the access and use of the information that results. 'Function creep' can be too tempting for those with potential access to broader sets of data.

Further, lack of clarity and openness in personal information policy mean people are unsure when and where they are 'being watched'. That leads to confusion over the connections between our use of technology, the information generated as a result, and where it will be used. The knowledge of whether someone is being watched, and by whom, helps to determine how they behave. So, clarity over the areas in which people are to be seen and by whom, or the justifications for why we cannot find this out, is important.

From our level of access to the internet to whether we are judged a success at work – segmentation happens according to a particular rationale for assigning difference. The capacity for interpersonal

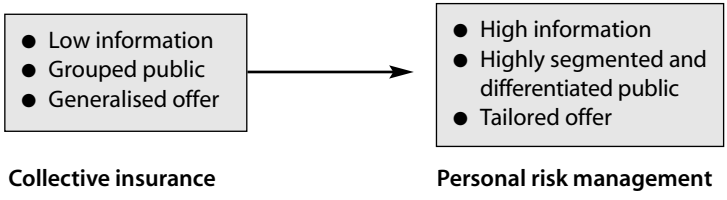
surveillance – a kind of collective watching – creates the opportunity for democratic negotiation of the boundaries and segmentations that ascribe worth and value to people. This chapter explains how to capitalise on this; on why the 'rules of engagement' in personal information need to be more open and democratic, and how to make that happen through policies and approaches from government, organisations and individuals.

Personal offers and the risk management of everyone

The development of information as a tool in the public and private sectors has created a model where the value, worth and meaning of a person can be judged more easily through the information that is held about them. The implications of this in practice are perhaps most evident in what happens to insurance – as more comprehensive information becomes available about a person's likely worth, lifestyle and future outcomes, the obvious temptation is to use that information to make better decisions about whether a person is worth the 'risk'. This can be characterised as a move from collective insurance towards individual risk management, visualised in figure 2.

The diagram demonstrates how exclusion *by* information functions[75] – by defining the value of individuals or groups through comprehensive sets of data, and structuring services and opportunities around decisions about their worth. The consequence of this is that institutions are able to see people with much greater definition, and can differentiate offers, prices and benefits as a result. In the case of insurance once again, it makes little sense to insure a blind man to drive. But it also makes little sense to offer the same life insurance to a woman with a known heart condition who eats only junk food and is married to a recently paroled murderer as to a vegan fitness fanatic who lives in a pacifist commune of renowned doctors. As having access to this level of detail becomes normal, and the means for prediction become more refined, decisions about the risk people pose or their value, such as those taken in insurance, become more discriminatory across individuals.

Figure 2. The risk management of everyone



As the example of credit agencies suggested earlier, this is a model of increasing relevance across sectors – government using more and different types of information, for example, to make 'better' decisions about where it allocates resources, and businesses offering the most attractive offers to their 'best' customers.

The consequences of refining services lie in a potential reinforcing of distinctions between people and a narrowing of experience. This trend makes it more likely that our cultural 'diet' will be more acutely defined, and reduce exposure to other ideas, people or sources of information. On the one hand this is a good thing – it means people can potentially stitch together their own cultural experiences. Through the things they eat, see, read, consume and share people have the tools to negotiate a sense of self. But on the other hand, as Sam Jones discussed in *Talk Us Into It*, it poses a problem for a political system that is predicated on a healthy *public* realm, in which ideas and opinions are exchanged and debated.[76]

Information held about us can influence our experiences, contribute to social exclusion and, through a dearth of debate, damage the public realm, but that is not all. There is a danger that we forget the distinction between the *process* and *content* of categorising. Though the process is automated, the categories into which people are sorted are devised by other people, and reflect the social distinctions of our society. Once ingrained, perceptions of difference

are difficult to shift. That includes both how institutions and businesses see people, and how people see themselves.

The danger is that the fragmenting of experience that results from exclusion by information can be reinforced by the technology and architecture built around divisions and rights of access. Bennett and Raab argue that such segmentations 'lay down the tramlines for the way organisations understand things, and for the way in which people understand themselves and their relations with institutions'.[77] As we saw with net neutrality, technology can reinforce these existing divisions. Parallels exist between this process and what is happening to public space; for example Stephen Graham and Simon Marvin argued in *Splintering Urbanism* that the physical and information architecture of the urban environment is being moulded to reflect social inequalities.[78] The Demos pamphlet *Seen and Heard*, for example, found that the economic rationale that plays a central role in how many places are organised has contributed to the exclusion of young people from public space.[79] It is often economics that determines and justifies how many different spheres of life are sorted and judged, which impacts on the kind of behaviour and activity that is encouraged or punished. Information surveillance is often deployed as the means to enact that 'control' in regulating the rules and success and norms of behaviour.[80]

These trends mean that it is more likely that people can get 'stuck' in categories they do not choose, do not agree with and which have significant consequences for their opportunities and aspirations. The likelihood of particular people being treated differently, and using prior information and profiles to make decisions about people, is of course not new. The disproportionate number of black males on the national DNA database is one example of the consequences of this;[81] another is the tendency to stop and search people from certain minority ethnic groups more than others – a disparity that is widening.[82]

However, the reliance on personal information means there are new ways that discrimination and segmentation can happen. The level of data that organisations and institutions have access to is new

and continually growing, and how they will use the data is both unknown and, at the moment, insufficiently debated. Further, with reduced storage costs and easily connected information, questions of data retention – when to delete and 'forget' data and personal information and for what reasons – become more pronounced. That is especially so in the context of emerging research into the capabilities of data 'mining', the aim of which is to draw conclusions from increasingly large amounts of information – inferring, for example, authorship of documents or relationships between seemingly unconnected people.[83]

This often goes unnoticed by those helping to create these divisions through the gathering and use of data. If differences between people are simply read from existing social inequalities, we risk accepting and 'rationalising' rather than questioning and challenging them. That makes the circularity of causes and consequences of inequality more fraught.

There is, as we saw in the case of credit agencies, increased pressure on the scope of data held in a connectable way, and on the rights of access to it. So a complex relationship between the roles of private and public sector mean that the *responsibility* to understand and, further, to make judgements about people's behaviour becomes ever more difficult. These challenges entwine personal information gathering, use and sharing to the role of the state in intervening in inequality, supporting opportunity and promoting safety. This process of segmentation is not market failure, but extreme market *success*, prompting a set of challenges. In the longer term, how will increasing knowledge of the value, tendencies and relationships of a person affect their chances and aspirations? How will this affect their relationship with other people in the society in which they live? What is the role of government in intervening in the market successes that tend to exacerbate those profiles? Further, what is the responsibility of the private sector in the behaviour and decisions they encourage or reward?

But currently government does not connect consistently enough its use of personal information in a bureaucratic or strategic sense with

its stated willingness to engage people through new communication, collaboration and information tools.[84] The private sector is not open enough in what information it gathers and uses, and the responsibilities this may bring. That means it is difficult for individuals to judge the negative implications of the very clear benefits they get from embracing openness. In these tensions between empowerment *through* information and control *by* information, then, sits the problem of how the costs and benefits of increased use of information by individuals, organisations and institutions are negotiated. The direction of travel leaves us with three options:

1. *Reverse the trend*. Try to work towards stopping the movement along the continuum sketched in figure 2. That would mean a pause in the trend towards personalising services in both the public and the private sectors.
2. *Impose clearer limits and rules*. Establish limits on who can access what, and when – through openly debated and strict access laws, backed up by clear routes of accountability.
3. *Identify a clearer role for the state*. Establish what the role of government is in intervening in 'differences' to mitigate for inequality. Openly debate when, where and how it is legitimate to act, and how it plans to do so.

This report shows why having more information available to more people – quicker, easier to access and on demand – means that *personal* information has become a more important commodity than ever before. For this reason an open debate about information policy and practice, that engages the public, industry and representatives across government, cannot just happen on data protection and identity fraud grounds. A democratic approach to personal information means finding clear limits and rules on information use. That needs to be based on a sharper understanding of the role of the state, connected to an openness about the sorts of information it will need to perform it. That, in turn, rests on a longer-term debate about

the sort of support and interventions people want and hope for in future, personalised services.

We casually leave trails of information behind ourselves. But data and facts retain a significance well beyond the convenient transactions they may have been generated by. Here, the personal becomes political. Democratic policy on personal information, then, means maintaining the spirit of collaborative openness that information technologies promise. To achieve that, we need collective rules about when and where individuals have the right to control, or influence, the use of the information that increasingly determines their worth.

Recommendations

This pamphlet is based around a tension at the heart of the offer of more personal services. Far from being necessarily something to guard against, however, there are examples of approaches to personal services and personal information that successfully negotiate the concerns we raise in this pamphlet. For example, the finest examples of personalising public service reform take a *participative* approach, placing more direct control over resources and responses to need in the hands of the user, rather than providers.[85] Research into identity management systems and personalised technologies has yielded a plethora of options for providing secure services that maintain an emphasis on user control and the potential for individual negotiation.[86] There are identity card systems that maintain a separation of different kinds of information, meaning a range of information is not held by a single body or in such a connectable form. That makes decisions about when and where connections are made between records of personal information, by whom, and what kind of information is relevant, in what context, more negotiable.[87]

It will be increasingly important to make such approaches the norm. People must be placed at the centre of information flows. Our findings suggested a number of measures that individuals, government and the private sector could follow to improve the relationship between people, personal information and the institutions that use that information.

For individuals, we recommend:

- The first step is for individuals to take measures to protect their personal information – for example, by securing wireless networks. Second, they must recognise the connections between the benefits of sharing information, and the often less tangible costs and dangers that can result. A better understanding of this relationship is the necessary step towards bottom-up policy driven by collectively negotiated norms and rules, rather than policy driven by the narrower needs and interests of government or business. However, this does need considerable support from government and the private sector to start the process.

For government, we recommend:

- The government should develop a more coherent strategy around personal information use. This strategy should clarify the links between how government will use personal information, in specific contexts, and what the potential benefits or costs might be for individuals. Each government department using personal information must say how they are accessing personal information, for what purpose, and how it affects people. They should also employ 'cash-handling' disciplines for dealing with people's personal information.
- The government should begin long-term research and thinking into increasing levels of information about individuals, coupled with personalising services and experiences. Segmentation and increasing knowledge of individuals will create markets that exclude in ways that current uses of information do not. That will have a significant impact on what is meant by equality. For example, will a new frontier of the welfare state be providing life insurance for certain types of people who

are deemed bad investments by private insurance providers?

- The Information Commissioner's Office (ICO) needs greater capacity to cope with the range of demands of an information society, which continue to extend away from just security of data towards data use and the nature of information sharing. For example, that could include the ability for the ICO to audit organisations' use of personal information without needing their consent.
- 'Privacy impact assessments' should be used for major projects across public and private sectors to assess the use of personal information early in development, led by the ICO.
- There needs to be a serious, renewed debate about the identity card scheme, with the kind of engagement that should have happened at the start of the process. Otherwise, the scheme should be dropped. There needs to be more open consideration of what kind of information the cards would hold, why, and in what circumstances they will be used. Meaningful engagement with the public about how the technology should work must be foremost in shaping what the cards do, if they are to go ahead.

For business and the private sector, we recommend:

- The rights of access individuals have to information held about them in the private sector should be extended, including the right to know what groups people have been 'segmented' into, and allow greater ability for individuals to challenge and change existing information about themselves that they believe to be invalid, incorrect or unfair.
- Information holders should engage in an open debate about where responsibility for personal information lies, with a view to clarifying the rights and responsibilities of businesses and individuals.

- There should be a common sense test for privacy statements and personal information policy. The private sector must provide simple, accessible explanations of why personal information is gathered. It is too easy currently to adapt and rely on established legalistic policies. A move away from jargon is needed. This means, for example, requiring businesses to follow the legal concept of the 'reasonable person' when drawing up policy statements on personal information.
- Banks should consider a 'no claims bonus' for customers who successfully protect their personal information.
- Technical distinctions used by business – between authenticators and identifiers, for example – should be binned. As for government, private sector involvement in digital identity should be grounded in the ways that people use and value their digital identities. That should imply a move away from using information people are likely to divulge – such as family maiden names, dates of birth – as 'authenticators' instead.
- As a bridge between people, policy-makers and technologists, a body such as the ICO should be given the remit and resources to lead open discussions and debate to help build more secure, effective and appropriate technology for personal information.

Notes

1 See www.barclaycard.co.uk/products/apply/barclaycardonepulse.html (accessed 16 Oct 2007).
2 R Ford, 'Beware rise of Big Brother state, warns data watchdog', *Times Online*, 16 Aug 2004, see www.timesonline.co.uk/tol/news/uk/article470264.ece (accessed 13 Nov 2007).
3 K Ball et al, 'A report on the surveillance society', for the Information Commissioner by the Surveillance Studies Network, Sep 2006, see www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf (accessed 13 Nov 2007).
4 'Community asks for more CCTV cameras', *BBC News Online*, 28 Mar 2007, http://news.bbc.co.uk/2/hi/uk_news/england/manchester/6503333.stm (accessed 13 Oct 2007).
5 Cabinet Office, *Building on Progress: Public services* (London: Prime Minister's Strategy Unit, Mar 2007), available at http://archive.cabinetoffice.gov.uk/policy_review/documents/building_on_progress.pdf (accessed 25 Oct 2007).
6 'Anti file-sharing laws considered', *BBC News Online*, 24 Oct 2007, see http://news.bbc.co.uk/1/hi/technology/7059881.stm (accessed 13 Nov 2007).
7 R Clarke, 'Have we learnt to love Big Brother?', *Issues* 72 (Jun 2005), see www.anu.edu.au/people/Roger.Clarke/DV/DV2005.html (accessed 26 Oct 2007).
8 See www.tate.org.uk/britain/turnerprize/2006/philcollins.htm (accessed 13 Oct 2007).
9 M McCahill and C Norris, 'CCTV in London', working paper no 6, *Urban Eye* (Jun 2002), see www.urbaneye.net/results/ue_wp6.pdf (accessed 26 Oct 2007).
10 Home Office, 'The national DNA database', see www.homeoffice.gov.uk/science-research/using-science/dna-database/ (accessed 25 Oct 2007).
11 The Regulation of Investigatory Powers (Acquisition and Disclosure of Communications Data: Code of Practice), Statutory Instrument 2007 no 2197

(Norwich: TSO, 2007), available at www.opsi.gov.uk/si/si2007/ 20072197.htm (accessed 25 Oct 2007).
12 Perri 6, *The Future of Privacy*, vol 1 (London: Demos, 1998).
13 See http://newassignment.net/ (accessed 13 Nov 2007).
14 Internet Access, National Statistics, Aug 2007, www.statistics.gov.uk/cci/nugget.asp?id=8 (accessed 26 Oct 2007).
15 Ofcom, 'The communications market 2007', Ofcom, 2007, available at http://ofcom.org.uk/research/cm/cmr07/cm07_print/ (accessed 2 Oct 2007).
16 B Marshall et al, *Blair's Britain: The social and cultural legacy* (London: Ipsos MORI, Aug 2007), see www.ipsos-mori.com/publications/srireports/bb-social-cultural.shtml (accessed 24 Oct 2007).
17 J Glover, 'Riven by class and no social mobility – Britain in 2007', *Guardian*, 20 Oct 2007, see http://society.guardian.co.uk/socialexclusion/story/0,,2195632,00.html (accessed 23 Oct 2007).
18 Commission for Racial Equality, *A Lot Done, A Lot to Do: Our vision for an integrated Britain* (London: Commission for Racial Equality, Sep 2007), available at www.equalityhumanrights.com/Documents/Race/General%20advice%20and%20information/a_lot_done_a_lot_to_do.pdf (accessed 29 Oct 2007).
19 D Lyon (ed), *Surveillance as Social Sorting: Privacy, risk and digital discrimination* (London: Routledge, 2003).
20 P Foster, 'Caught on camera – and found on Facebook', *Times Online*, 17 Jul 2007, http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article2087306.ece (accessed 26 Oct 2007).
21 S Lace (ed), *The Glass Consumer: Life in a surveillance society* (Bristol: The Policy Press, 2005).
22 ICMR, *Tesco: The customer relationship management champion* (Punjagutta, Hyderabad: Centre for Management Research, 2003), available at http://icmr.icfai.org/casestudies/catalogue/Marketing/MKTG070.htm (accessed 26 Oct 2007).
23 See www.tescocorporate.com/page.aspx?pointerid=6A0619602CD0417A8562FED9AB7B76B5 (accessed 15 Nov 2007).
24 See www.loyalty.vg/pages/CRM/case_study_14_Tesco.htm (accessed 5 Oct 2007).
25 ICMR, *Tesco*.
26 See www.loyalty.vg/pages/CRM/case_study_14_Tesco.htm (accessed 5 Oct 2007).
27 Ibid.
28 See www.nectar.com/help/privacyPolicy.nectar (accessed 6 Oct 2007).
29 See, for example, J Borger, 'Clinton's strategist advises Brown to delay election', *Guardian Unlimited*, 6 Oct 2007, see www.guardian.co.uk/guardianpolitics/story/0,,2184922,00.html (accessed 13 Nov 2007).
30 See the large body of literature on customer relationship management.
31 T O'Reilly, 'Web 2.0 is really about controlling data', *Wired Magazine*, 13 Apr

2007, see www.wired.com/techbiz/people/news/2007/04/timoreilly_0413 (accessed 1 Oct 2007).

32 R Verkaik, 'Google is watching you: "Big Brother" row over plans for personal database', *Independent*, 24 May 2007, see http://news.independent.co.uk/sci_tech/article2578479.ece (accessed 11 Oct 2007).

33 G Brown, speech to Labour Party conference, 24 Sep 2007, see http://politics.guardian.co.uk/labour2007/story/0,,2176282,00.html (accessed 25 Oct 2007).

34 See http://archive.cabinetoffice.gov.uk/e-government/ (accessed 26 Oct 2007).

35 See www.cio.gov.uk/transformational_government/strategy/ (accessed 26 Oct 2007).

36 See www.connectingforhealth.nhs.uk/ (accessed 26 Oct 2007).

37 See www.everychildmatters.gov.uk/deliveringservices/contactpoint/ (accessed 26 Oct 2007).

38 See www.identitycards.gov.uk/index.asp (accessed 26 Oct 2007).

39 F Elliott, 'Safety fears over new register of all children', *Times Online*, 27 Aug 2007, see www.timesonline.co.uk/tol/news/politics/article2332307.ece (accessed 26 Oct 2007).

40 Ibid.

41 G Brown, speech on liberty, University of Westminster, London, 25 Oct 2007, see www.number10.gov.uk/output/Page13630.asp (accessed 29 Oct 2007).

42 For in Control, see www.in-control.org.uk/ (accessed 13 Nov 2007); and for NHS Choices, see www.nhs.uk/Pages/homepage.aspx (accessed 13 Nov 2007).

43 A Travis, 'Labour steps back in push for ID cards', *Guardian Unlimited*, 4 Aug 2005, see http://politics.guardian.co.uk/homeaffairs/story/0,11026,1542191,00.html (accessed 13 Nov 2007); 'Major NHS upgrade hit by delay', *BBC News Online*, 16 June 2006, see http://news.bbc.co.uk/1/hi/health/5086060.stm (accessed 13 Nov 2007).

44 British Social Attitudes Survey, www.britsocat.com/BodySecure.aspx?control=BritsocatMarginals&var=IDCARDS&SurveyID=228 (accessed 18 Oct 2007; registration required).

45 Identity and Passport Service: Introduction of e-Passports, House of Commons Committee of Public Accounts, Jul 2007, see www.publications.parliament.uk/pa/cm200607/cmselect/cmpubacc/362/362.pdf (accessed 18 Oct 2007).

46 See, for example, G Brown, 'Securing our future', speech to the Royal United Services Institute, London, 13 Feb 2006, see http://politics.guardian.co.uk/terrorism/story/0,,1708739,00.html (accessed 1 Nov 2007).

47 Regulation on Investigatory Powers Act 2000, see www.opsi.gov.uk/acts/acts2000/20000023.htm (accessed 13 Nov 2007).

48 See Data Retention (EC Directive) Regulations 2007, available at www.opsi.gov.uk/si/si2007/20072199.htm (accessed 13 Nov 2007); and 'Acquisition and disclosure of communications data revised draft code of

practice', available at http://security.homeoffice.gov.uk/ripa/publication-search/ripa-cop/acquisition-disclosure-cop.pdf (accessed 8 Oct 2007).

49 Interview for project, research participant.

50 See, for example, MA Rothstein (ed), *Genetics and Life Insurance: Medical underwriting and social policy* (Cambridge, MA: MIT Press, 2004).

51 See, for example, H Lacohée, S Crane and A Phippen, *Trustguide: Final report*, rev Nov 2006, see www.trustguide.org.uk/Trustguide%20-%20Final%20Report.pdf (accessed 26 Oct 2007).

52 WH Dutton and EJ Helsper, *The Internet in Britain: 2007*, Oxford Internet Survey 2007 (Oxford: Oxford Internet Institute, 2007), available at www.oii.ox.ac.uk/research/oxis/OxIS2007_Report.pdf (accessed 13 Nov 2007).

53 'e-Retail hits 80% hypergrowth – £4bn web sales in July', *IMRG*, Aug 2007, see www.imrg.org/ItemDetail.aspx?clg=InfoItems&cid=pr&pid=pr_Index_press_release_200807&language=en-GB (accessed 26 Oct 2007).

54 Council of the European Union, 'Processing and transfer of passenger name record data by air carriers to the United States Department of Homeland Security – "PNR"', Jun 2007, see www.epic.org/privacy/pdf/pnr-agmt-2007.pdf (accessed 29 Oct 2007).

55 See, for example, IATA, 'Passenger and freight forecast 2007 to 2011', IATA economic briefing, Oct 2007, available at www.iata.org/NR/rdonlyres/E0EEDB73-EA00-494E-9408-2B83AFF33A7D/0/traffic_forecast_2007_2011.pdf (accessed 29 Oct 2007).

56 'Millions are caught in great credit card heist, *The Times*, 30 Mar 2007, see http://business.timesonline.co.uk/tol/business/money/consumer_affairs/article1588849.ece (accessed 20 Nov 2007).

57 See www.getsafeonline.org/nqcontent.cfm?a_name=sponsors_1&#foundingsponsor_1076 (accessed 9 Oct 2007).

58 See www.getsafeonline.org/nqcontent.cfm?a_name=sponsors_1&#foundingsponsor_1076 (accessed 9 Oct 2007).

59 '£141 benefits computer shelved', *BBC News Online*, 5 Sep 2006, see http://news.bbc.co.uk/1/hi/uk_politics/5315280.stm (accessed 9 Oct 2007).

60 T Collins, 'Revenue red-faced as IT system wrongly fines 10,000 companies', *ComputerWeekly.com*, 17 Jan 2006, see www.computerweekly.com/Articles/2006/01/17/213687/revenue-red-faced-as-it-system-wrongly-fines-10000.htm (accessed 13 Nov 2007); and M Cross, 'Online tax gets positive return', *Guardian*, 9 Feb 2006, see http://politics.guardian.co.uk/egovernment/story/0,,1705194,00.html (accessed 9 Oct 2007).

61 L Glendinning, 'Junior doctors' personal details made public in website blunder', *Guardian*, 26 Apr 2007, see www.guardian.co.uk/technology/2007/apr/26/news.health (accessed 9 Oct 2007).

62 See www.google.com/corporate/ (accessed 13 Oct 2007).

63 See, for example, www.publications.parliament.uk/pa/pahansard.htm (accessed 13 Nov 2007).

64 V Lehdonvirta, 'European Union data protection directive: adequacy of data

protection in Singapore', *Singapore Journal of Legal Studies* 2 (2004).

65 CJ Bennett and CD Raab, *The Governance of Privacy: Policy instruments in a global perspective* (Cambridge, MA: MIT Press, 2006).

66 P Fleischer, 'Global privacy standards' in *UK Confidential: The social value of privacy* (London: Demos, forthcoming in 2008).

67 See, for example, L Bygrave, *Data Protection Law: Approaching its rationale, its logic, its limits* (The Hague: Kluwer Law International, 2002).

68 The All Party Parliamentary Group on Identity Fraud, 'All Party Parliamentary Group Report into Identity Fraud', Oct 2007, www.fhcreative.co.uk/idfraud/downloads/APPG_Identity_Fraud_Report.pdf (accessed 27 Oct 2007).

69 See www.thebillblog.com/billblog/ (accessed 15 Nov 2007).

70 See, for example, Tor, www.torproject.org/ (accessed 26 Oct 2007).

71 Small files that sit on a user's computer to relay certain bits of information about internet preferences and history.

72 Regulation on Investigatory Powers Act 2000.

73 'Acquisition and disclosure of communications data revised draft code of practice'.

74 This is often referred to as enterprise-centric vs user-centric technology. See, for example, D Kearns, 'What is "user-centric" identity?', *Network World*, Oct 2006, www.networkworld.com/newsletters/dir/2006/0710id1.html (accessed 26 Oct 2007).

75 See, for example, Perri 6 with B Jupp, *Divided by Information* (London: Demos, 2001); and Lyon (ed), *Surveillance as Social Sorting*.

76 S Jones, *Talk Us Into It* (London: Demos, 2006).

77 Bennett and Raab, *Governance of Privacy*.

78 S Graham and S Marvin, *Splintering Urbanism: Networked infrastructure, technological mobilities and the urban condition* (London: Routledge, 2001).

79 J Beunderman, C Hannon and P Bradwell, *Seen and Heard: Reclaiming the public realm with children and young people* (London: Demos, 2007).

80 For example, see research by Dr Kirstie Ball on workplace surveillance: KS Ball, 'The labours of surveillance', *Surveillance and Society* 1, no 2 (2003).

81 K Jarret, 'DNA breakthrough', National Black Police Association, 16 Oct 2006, www.nbpa.co.uk/index.php?option=com_content&task=view&id=40&Itemid=58 (accessed 29 Oct 2007).

82 See, for example, Metropolitan Police Authority, 'Report of the MPA scrutiny on MPS stop and search practice', 2004, www.mpa.gov.uk/downloads/issues/stop-search/stop-search-report-2004.pdf (accessed 29 Oct 2007).

83 See, for example, the Homeland Security Centre for Dynamic Data Analysis (DyDAn) at http://dydan.rutgers.edu/about.html (accessed 29 Oct 2007).

84 For an example of that willingness see the report by E Mayo and T Steinberg, 'The power of information', Jun 2007, www.cabinetoffice.gov.uk/upload/assets/www.cabinetoffice.gov.uk/strategy/power_information.pdf (accessed 26 Oct 2007).

85 See, for example, N Gallagher, 'Participative public services', *eGov Monitor*, 22 Oct 2007, www.egovmonitor.com/node/15293 (accessed 30 Oct 2007).
86 A Kobsa and L Craner (eds), 'Proceedings of the UM05 workshop on privacy-enhanced personalization', Jul 2005, www.isr.uci.edu/pep05/papers/w9-proceedings.pdf (accessed 29 Oct 2007).
87 See, for example, OpenID, at http://openid.net/ (accessed 20 Oct 2007); J Rosen, 'Identity crisis: how to have a national ID card that doesn't threaten civil liberties', *Wired*, Jan 2004, www.wired.com/wired/archive/12.01/start.html (accessed 29 Oct 2007).

DEMOS – Licence to Publish

THE WORK (AS DEFINED BELOW) IS PROVIDED UNDER THE TERMS OF THIS LICENCE ("LICENCE"). THE WORK IS PROTECTED BY COPYRIGHT AND/OR OTHER APPLICABLE LAW. ANY USE OF THE WORK OTHER THAN AS AUTHORIZED UNDER THIS LICENCE IS PROHIBITED. BY EXERCISING ANY RIGHTS TO THE WORK PROVIDED HERE, YOU ACCEPT AND AGREE TO BE BOUND BY THE TERMS OF THIS LICENCE. DEMOS GRANTS YOU THE RIGHTS CONTAINED HERE IN CONSIDERATION OF YOUR ACCEPTANCE OF SUCH TERMS AND CONDITIONS.

1. **Definitions**
   - **a** **"Collective Work"** means a work, such as a periodical issue, anthology or encyclopedia, in which the Work in its entirety in unmodified form, along with a number of other contributions, constituting separate and independent works in themselves, are assembled into a collective whole. A work that constitutes a Collective Work will not be considered a Derivative Work (as defined below) for the purposes of this Licence.
   - **b** **"Derivative Work"** means a work based upon the Work or upon the Work and other pre-existing works, such as a musical arrangement, dramatization, fictionalization, motion picture version, sound recording, art reproduction, abridgment, condensation, or any other form in which the Work may be recast, transformed, or adapted, except that a work that constitutes a Collective Work or a translation from English into another language will not be considered a Derivative Work for the purpose of this Licence.
   - **c** **"Licensor"** means the individual or entity that offers the Work under the terms of this Licence.
   - **d** **"Original Author"** means the individual or entity who created the Work.
   - **e** **"Work"** means the copyrightable work of authorship offered under the terms of this Licence.
   - **f** **"You"** means an individual or entity exercising rights under this Licence who has not previously violated the terms of this Licence with respect to the Work, or who has received express permission from DEMOS to exercise rights under this Licence despite a previous violation.
2. **Fair Use Rights.** Nothing in this licence is intended to reduce, limit, or restrict any rights arising from fair use, first sale or other limitations on the exclusive rights of the copyright owner under copyright law or other applicable laws.
3. **Licence Grant.** Subject to the terms and conditions of this Licence, Licensor hereby grants You a worldwide, royalty-free, non-exclusive, perpetual (for the duration of the applicable copyright) licence to exercise the rights in the Work as stated below:
   - **a** to reproduce the Work, to incorporate the Work into one or more Collective Works, and to reproduce the Work as incorporated in the Collective Works;
   - **b** to distribute copies or phonorecords of, display publicly, perform publicly, and perform publicly by means of a digital audio transmission the Work including as incorporated in Collective Works;

   The above rights may be exercised in all media and formats whether now known or hereafter devised. The above rights include the right to make such modifications as are technically necessary to exercise the rights in other media and formats. All rights not expressly granted by Licensor are hereby reserved.
4. **Restrictions.** The licence granted in Section 3 above is expressly made subject to and limited by the following restrictions:
   - **a** You may distribute, publicly display, publicly perform, or publicly digitally perform the Work only under the terms of this Licence, and You must include a copy of, or the Uniform Resource Identifier for, this Licence with every copy or phonorecord of the Work You distribute, publicly display, publicly perform, or publicly digitally perform. You may not offer or impose any terms on the Work that alter or restrict the terms of this Licence or the recipients' exercise of the rights granted hereunder. You may not sublicence the Work. You must keep intact all notices that refer to this Licence and to the disclaimer of warranties. You may not distribute, publicly display, publicly perform, or publicly digitally perform the Work with any technological measures that control access or use of the Work in a manner inconsistent with the terms of this Licence Agreement. The above applies to the Work as incorporated in a Collective Work, but this does not require the Collective Work apart from the Work itself to be made subject to the terms of this Licence. If You create a Collective Work, upon notice from any Licencor You must, to the extent practicable, remove from the Collective Work any reference to such Licensor or the Original Author, as requested.
   - **b** You may not exercise any of the rights granted to You in Section 3 above in any manner that is primarily intended for or directed toward commercial advantage or private monetary

compensation. The exchange of the Work for other copyrighted works by means of digital file-sharing or otherwise shall not be considered to be intended for or directed toward commercial advantage or private monetary compensation, provided there is no payment of any monetary compensation in connection with the exchange of copyrighted works.

c If you distribute, publicly display, publicly perform, or publicly digitally perform the Work or any Collective Works, You must keep intact all copyright notices for the Work and give the Original Author credit reasonable to the medium or means You are utilizing by conveying the name (or pseudonym if applicable) of the Original Author if supplied; the title of the Work if supplied. Such credit may be implemented in any reasonable manner; provided, however, that in the case of a Collective Work, at a minimum such credit will appear where any other comparable authorship credit appears and in a manner at least as prominent as such other comparable authorship credit.

5. Representations, Warranties and Disclaimer

a By offering the Work for public release under this Licence, Licensor represents and warrants that, to the best of Licensor's knowledge after reasonable inquiry:

i Licensor has secured all rights in the Work necessary to grant the licence rights hereunder and to permit the lawful exercise of the rights granted hereunder without You having any obligation to pay any royalties, compulsory licence fees, residuals or any other payments;

ii The Work does not infringe the copyright, trademark, publicity rights, common law rights or any other right of any third party or constitute defamation, invasion of privacy or other tortious injury to any third party.

b EXCEPT AS EXPRESSLY STATED IN THIS LICENCE OR OTHERWISE AGREED IN WRITING OR REQUIRED BY APPLICABLE LAW, THE WORK IS LICENCED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES REGARDING THE CONTENTS OR ACCURACY OF THE WORK.

6. Limitation on Liability. EXCEPT TO THE EXTENT REQUIRED BY APPLICABLE LAW, AND EXCEPT FOR DAMAGES ARISING FROM LIABILITY TO A THIRD PARTY RESULTING FROM BREACH OF THE WARRANTIES IN SECTION 5, IN NO EVENT WILL LICENSOR BE LIABLE TO YOU ON ANY LEGAL THEORY FOR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES ARISING OUT OF THIS LICENCE OR THE USE OF THE WORK, EVEN IF LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. Termination

a This Licence and the rights granted hereunder will terminate automatically upon any breach by You of the terms of this Licence. Individuals or entities who have received Collective Works from You under this Licence, however, will not have their licences terminated provided such individuals or entities remain in full compliance with those licences. Sections 1, 2, 5, 6, 7, and 8 will survive any termination of this Licence.

b Subject to the above terms and conditions, the licence granted here is perpetual (for the duration of the applicable copyright in the Work). Notwithstanding the above, Licensor reserves the right to release the Work under different licence terms or to stop distributing the Work at any time; provided, however that any such election will not serve to withdraw this Licence (or any other licence that has been, or is required to be, granted under the terms of this Licence), and this Licence will continue in full force and effect unless terminated as stated above.

8. Miscellaneous

a Each time You distribute or publicly digitally perform the Work or a Collective Work, DEMOS offers to the recipient a licence to the Work on the same terms and conditions as the licence granted to You under this Licence.

b If any provision of this Licence is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Licence, and without further action by the parties to this agreement, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

c No term or provision of this Licence shall be deemed waived and no breach consented to unless such waiver or consent shall be in writing and signed by the party to be charged with such waiver or consent.

d This Licence constitutes the entire agreement between the parties with respect to the Work licensed here. There are no understandings, agreements or representations with respect to the Work not specified here. Licensor shall not be bound by any additional provisions that may appear in any communication from You. This Licence may not be modified without the mutual written agreement of DEMOS and You.