private lives
a people's inquiry into personal information

Peter Bradwell

DEMOS

Demos is an independent think-tank focused on power and politics. We develop and spread ideas to give people more power over their own lives. Our vision is of a democracy of powerful citizens, with an equal stake in society.

Demos has several core research programmes in 2010: Capabilities, Citizenship, Security, Economic Life, Progressive Austerity and Extremism. We also have two political research programmes: the Progressive Conservatism Project and Open Left, investigating the future of the centre-Right and centre-Left.

In all our work we bring together people from a wide range of backgrounds to develop ideas that will shape debate in the UK and beyond, and engage a broad and diverse audience worldwide.

Find out more about our work at www.demos.co.uk.

First published in 2010

Magdalen House, 136 Tooley Street,
London, SE1 2TU, UK

ISBN 978 1 906693 36 7
Series design by modernactivity
Typeset by Chat Noir Design, Charente
Printed by Lecturis, Eindhoven

Set in Gotham Rounded
and Baskerville 10
Cover paper: Arctic Volume
Text paper: Munken Premium White

private lives

Peter Bradwell

DEMOS

Contents

Acknowledgements

This research behind this report has relied on a number of people's generosity. First and foremost, many thanks to the 40 members of our people's inquiry. For their wisdom and generosity, we owe a similar debt of gratitude to the experts who gave up their time to help inform the inquiry, braving cold evenings in London and colder mornings in Bradford: Liam Curren, Dan Cooper, Sue Cullen, Martin Hoskins, Natalie Hunt, Alma Whitten, Anna Fielder, Stephen Whitehead, Marlene Winfield, Michael Keegan, Dr Mohammad Al-Ubaydli, Lizzie Coles-Kemp and Stephen McCartney.

The development of the people's inquiry and the analysis of the results benefited hugely from the input of our steering group. Many thanks to Professor Charles Raab, Alma Whitten, Marlene Winfield, Anna Fielder, Nick Stringer, Natalie Hunt and Paula Bruening for their insight and intelligence throughout the project. We are also grateful for the ideas and thoughts of the participants in our three expert roundtables, who are listed in appendix C. Thanks also to Edgar Whitley for his comments on the research.

The design of our deliberative methodology was informed enormously by Tom Flynn from the University of York, who offered patient and important insights to improve the design of the inquiry.

At Demos, enormous thanks are owed for the support and skill of my co-facilitators Dan Leighton and Max Wind-Cowie, who thought nothing of the unsociable working hours and travel that running the inquiry involved. A big thank you to Ollie Haydon-Mulligan who brought insightful enthusiasm to the analysis of the inquiry transcripts and who played a vital role in the writing of section 2.

Thanks to Julia Margo for her comments on the report and to Jamie Bartlett for his support and help with the methodology. We also built on the foundations of past Demos work, in particular Perri 6's rigorous analyses of privacy and Jack Stilgoe's work on public engagement in science. Thanks to Becky Gray for her contribution to the research in its early stages. And a sincere thank you to Peter Harrington, Beatrice Karol Burks and Claire Coulier for their patience and skill in guiding the

pamphlet through production to its launch and for their help in communicating the ideas.

And finally, the project would not have been possible with the very generous support of the Information Commissioner's Office and Consumer Focus. In particular we are extremely grateful to Stephen McCartney at the Information Commissioner's Office and Linda Weatherhead at Consumer Focus. Both offered invaluable support in helping to get the project going and brought ideas and enthusiasm throughout.

All errors and omissions are our own.

Peter Bradwell
Demos
March 2010

Foreword: Consumer Focus

One reason that Consumer Focus were keen to be involved in this deliberative research was that there have been many surveys indicating that people care about privacy and personal information – but people's use of technology without much concern for their own privacy gives a different picture.

Playing fast and loose with our privacy has been seen as a trade-off for technological development. It was important to us to find out what lay beneath the surface and what people really thought about the safety of their personal data. The picture that has emerged is far more complex than it initially seemed.

There is real value to the organisations that utilise our personal information, from public interest benefits like, for example, medical research and where to build new schools and hospitals, to the 'black gold' of the online marketers who sell our information, to the hackers and fraudsters who can use it for illegal gain. There seems among the people's inquiry participants to be an underlying faith in the public sector – despite recent high profile data breaches – but a wary scepticism for the private sector in its use and storage of information.

Gaining trust and providing transparency is a big challenge for governments transitioning to cloud computing and the privatisation of information and technology. While billions of pounds are spent on research and development in technology to influence our purchasing decisions, it seems that little is being spent on the privacy protection, transparency, control and regulation needed for consumers to confidently engage with and make use of new technology. Footballers may be able to take out expensive injunctions to prevent revelations of their peccadilloes – but what about you and me, what tools and protections do we have?

Consumers want to be asked about things, not just have things done to them. They want to consent and control, but

being a consumer should not be a full-time job and so they expect protection as well. A need to foster trust underlies the dialogue. A lack of consumer confidence damages markets and restricts uptake of new technologies.

It is time to step back and look for a transparent agreement with the consumers of services – and to focus on what the public wants and needs, not on what industry or Government wants to deliver.

Linda Weatherhead, Principal Policy Advocate
Consumer Focus

Foreword: Information Commissioner's Office

Information rights matter. But how do we ensure that these rights actually count in the information age?

The online world is expanding fast. New technologies and services are transforming the way we do business. The increasing take-up not just of email and e-commerce but also of social networking and other second-generation services reflects our growing dependence on the internet as a means of conducting our lives. Marketers target their messages and the advertising keeps many online services free. At the same time, public sector agencies in the UK are making greater use of our personal information for service provision, security and crime prevention. Hundreds of thousands of items of personal data are collected, shared and used every minute by both public and private sector organisations.

Do I need to worry whether these uses are benign? How do I find out if someone is using my information who shouldn't be? Have I given consent for the use of my personal information? And even if I want to have a choice about every possible use of my information, do I have the time to keep up with all of the requests for my consent?

It is in this environment that the issue of the control and consent that individuals exercise over their own personal information is most keenly debated. Most of us have clicked to say we have read the terms and conditions when we haven't, but we still expect to be able to put things right easily when our information is misused. So where should the line be drawn between the role of regulation and the need for each of us to be vigilant on our own account?

If we are to maintain a data privacy regime that both protects and enables we need to understand how people relate to the online world. That is why my office decided to sponsor this project, in conjunction with Consumer Focus.

What emerges from the study is a fascinating picture of a public who certainly care about information rights, but who are by no means hysterical about perceived threats to liberty or privacy. There's no panic about Big Brother but trust in the public sector's data handling is fragile and there are concerns about some commercial practices.

The study points the way for the ICO to meet its commitment to respond to the real concerns of real people. Consumers want to be in effective control of their personal information and privacy. And there is support for tougher penalties for misuse of information by rogue individuals within organisations.

I hope that this report can contribute to the debate about the use of personal information, and about where the balance of rights and responsibilities should be struck, so that consumers can enjoy the benefits the online world offers, without surrendering control of their personal information or exposing it to unnecessary risk.

Christopher Graham, Information Commissioner

Public voices in the privacy debate

Lettin' the cat out of the bag is a whole lot easier than putting it back in
Will Rogers

This pamphlet is about what the public thinks about how personal information is used. It sets out the opinions and ideas expressed by 40 people following a month-long, deliberative 'people's inquiry'. Over 13 hours they were informed by a series of expert presentations, and then given the time and space to reflect, debate and decide what they thought about the use of communications data, targeted advertising and the use of medical information.

They heard from expert representatives from the NHS, search engines, mobile phone companies, from lawyers and from consumer advocates. The aim was to facilitate an informed discussion with participants considering a range of opinions on the risks, benefits, opportunities and challenges of the phenomenal explosion in the means to gather and use personal information. Across our three topics inquiry members were asked to consider the legitimacy of personal information use; the extent to which they can control it; and which 'calls to action' they demanded regulators, government and businesses listen to.

The people's inquiry indicated that people are not running scared of the database society, but at the same time they care deeply about its governance. They recognise that there are legitimate ways to gather and use information. But over the course of the inquiry they came to require more convincing that the aspirations driving the use of personal information were realistic, or that information would only be used to pursue the intended purposes.

Our participants offer a clear call for more meaningful ways to give their consent and for far stronger regulation to hold

data handlers to their word. For example, they want those who mishandle data to be named and shamed, they would like to see regulators develop a kite-marking scheme to help improve awareness of good practice and they want consumers harmed by the misuse or illicit sale of information to be compensated. The findings serve as an insight into the informed attitudes of people who are affected by information use. But equally, they serve as a demonstration of one mechanism for ensuring that the development of personal information use is legitimate and democratic.

Who let the cat out?

In November 2007, the National Audit Office asked Her Majesty's Revenue and Customs to send them a set of personal information relating to the processing of Child Benefits. They fulfilled their task by putting two compact discs in the post. Two unfortunate facts led to this rather mundane episode becoming a national scandal. The discs contained the personal information of 25 million people. And they never arrived at the National Audit Office. There were gasps in Parliament when the Chancellor, Alistair Darling, informed the House of Commons:

The missing information contains details of all child benefit recipients: records for 25 million individuals and 7.25 million families. Those records include the recipient and their children's names, addresses and dates of birth, child benefit numbers, national insurance numbers and, where relevant, bank or building society account details. I regard this as an extremely serious failure by HMRC in its responsibilities to the public.[1]

There have been a number of collective gasps since that statement as more stories of data losses have emerged. The Information Commissioners' Office announced in January 2010 that over 800 data breaches had been reported to them in two years.[2] Organisations from the public and private sectors alike have found themselves in the spotlight for losing information or having it stolen from them.

But data losses are only part of the story. Alongside fears about data insecurity there have been concerns more widely about the 'surveillance society' – a world in which everything we do is recorded, watched and judged. The House of Lords Constitution Committee report, *Surveillance: Citizens and the State*, argued that the recording of information was 'pervasive, routine, and almost taken for granted.'[3]

It is not surprising that polling data suggests concerns about data use are rising. The Information Commissioner's Office found in its Annual Track 2008 that 68 per cent of people now believe they have lost control over the way their personal details are collected and processed – rising from 53 per cent since 2004.[4] A YouGov poll reported in the Sunday Times in January 2009 found that 71 per cent of those asked were worried about private information falling into the wrong hands on the Internet.[5] An ICM poll, conducted for the Information Commissioner's Office in 2008, suggested 53 per cent of us are not confident that government, councils and banks will protect personal information, 77 per cent worry more about the safety of their personal details than they used to and 72 per cent feel powerless to protect such data. [6]

Our lives now have an information echo that resonates from the cameras that capture our movements through the streets, from the websites we visit that track our online behaviour, from our interactions with public services and from the information we volunteer on social networks. This is a world we are helping to create. In the same year that HMRC put those discs in the post, the rise in the number of visitors to Facebook in Europe was 303 per cent.[7] We are petrified of insecurity when information is others' to hold, but promiscuous with data when it is ours to give. Data is everywhere. Organisations keep losing it. There are some very public fears about how much information others hold about us. And yet we keep giving it away.

Our information echo tells others something about who we are, and in doing so informs decisions that can affect our financial well-being, our friendships and our relationship with government services. Personal information is proliferating, largely because technology has created many new ways for it be

given away or collected. It is useful, because it tells those who hold it something about the person to whom it relates. It is vulnerable, because it is easy to transfer to others deliberately, by mistake or against the holders' wishes. And it is fallible, because it is imperfect, incomplete and open to interpretation. It is not knowledge; it is an echo.

The technological possibilities that elicit this echo might be new, but the social, political and commercial aspirations of which they are in the service are not. Charles Raab and Colin Bennet argue in their book, *The Governance of Privacy*, that in this context, personal information use 'is about social relations and their management'.[8] The limits to the gathering and processing of personal information will help to determine the rights of government to enforce laws and manage people's behaviour. They may affect the public services that people are entitled to. They will determine our 'openness' to other people and the extent to which we are able to self-define and manipulate our identities. They will help shape people's financial well-being and the rights of businesses to gather data about people in order to create potentially more influential marketing.

If privacy is about these boundaries that govern when others can 'see' us, it is clear that technology has allowed them to be more easily crossed than ever. In this world so rich in the personal information that allows this to happen, privacy law expert Daniel Solove has argued that 'privacy is a concept in disarray.'[9] It is simply not clear how the social relations that information use affects are changing in practice.

The people's inquiry and the democratic database society

As technology develops and the will to manage, control and exploit is matched by the means to do so, there will be a constant struggle between the power of individuals and that of corporations, governments and others in civil society. We all have database fates: our life courses will be shaped by what our information echo says about us.

The database society in which these fates will play out is not inherently good or bad. The best we can hope for is that it is as democratic as any of the institutions, markets, or regulatory and legal mechanisms that exert power over our lives. As the laws and codes that govern information use emerge there is a need to ensure that we embed within them principles of democracy and freedom from the offline world. This requires public deliberation beyond the ballot box – opportunities for people to gather information about the issues affecting them and to reach considered positions.

Democratising personal information means not only giving people a voice in the debate, but also finding better ways of listening to what they say. In performing this role, this people's inquiry looked to participants' attitudes to these boundaries and to the way such rules are made and enforced. They recognised that there are occasions when there is a public interest in the state's uses of information. Likewise, they saw the benefits of its use in commercial contexts. But in their eyes, the legitimacy of personal information use was being undermined. They wanted the chance to make informed decisions that made a difference to how their information was used and the opportunity to hold organisations to their word. Inquiry members demanded transparency, security and the means for informed and meaningful choice. They felt that these standards were not being met.

The inquiry participants establish a set of challenges that data handlers must meet in order to live up to the principles of fair and legitimate data use. The inquiry demonstrates a way to engage in conversations that bring personal information decision-making closer to the people it affects.

1 Why a People's Inquiry into Personal Information?

Privacy is essentially the creature of conflicts of power.
Perri 6, *The Future of Privacy*[10]

The ability to gather and use information about people – to understand more about them – has increased exponentially over the past decades. Personal information has become central to the business models of the digital age; to the management of government and of state institutions; and to people's everyday lives and relationships. Despite the complexity of the technology driving this, some simple questions about power lie at the heart of personal information use.

Often there are situations in which we have a direct choice about whether to share information. Our use of Twitter, Facebook and other social networks sees us give away information about our thoughts and movements, our location, our employment history, our tastes in music, our shopping history and our political orientations. Academics such as danah boyd and Daniel Solove have written of the potential for social networks to help people manipulate their identities. But they also articulate fears about new vulnerabilities to our reputations, to bullying and the longer-term legacy of our past behaviour.[11] The capacity this gives us to project ourselves publicly is matched by the ability of others to spread information that helps to define who we are.

This information can also affect decisions we had not initially envisaged, for example, where employers monitor social networks. And as Tom Ilube of digital identity firm Garlik has argued, this new public life creates insecurities that can be easily exploited by criminals.[12] Related to this are problems of identity and authenticity, of recognising when someone is or is not who they say they are.[13] Through their decisions about the use of their

personal information, people are faced not only with maintaining social and professional networks but also with managing the risks of potential identity fraud, financial harm and reputational damage.

There are many cases in which we do not have direct control over our personal information. Governments can base their policies on ever more detailed understanding of their citizens. Many public bodies have access to personal data held by others, such as information about our time online. And governments are evolving agreements about the sharing of personal data concerning passengers travelling between countries and continents. In a commercial context, if a company gathers information about customers they can tailor products to make it more likely that customers will buy from them. They can offer free or cheaper content in exchange for advertising 'suited' to users. If you are an insurance company, through user data you can understand the level of risk associated with your potential customers with far greater definition.

Often it will either not be possible to express direct control over one's information, or one will not have sufficient control over the subsequent processing of data. But who takes the decisions about when the use of personal information in the public interest is legitimate? And how is it possible to develop the collective rules that determine individuals' ability to negotiate how personal information is used?[14] What regulatory regime would lead to a reasonable level of confidence that information is safe, and that the misuse of it will not lead to consequences that undermine the initial benefits?

The way personal information is used has ramifications for the power people have over their lives. We seem to have more control over how we are seen and understood. But at the same time, other people and organisations have more opportunity to make decisions, without our involvement, about who we are. That is a challenge in a world of individually tailored services, when the kind of services, products and interactions we encounter are dependent on such judgements. Can targeted advertising make it more likely that people get a bad deal, or might be manipulated by 'smarter' marketing? How does the

extensive gathering of personal information change how much say the government has over the management of our behaviour? Will that have adverse affects on certain groups who appear more likely to require special treatment? Are people more vulnerable when they are so exposed and does that necessitate new safeguards?

Surveillance scholar David Lyon has argued that 'those who have the capacity to influence how people are classified and categorised tend to be in positions of greater power than those who do not'.[15] This is true to the extent that the rules and laws that govern the use of personal information can deny people the chance to influence them. The rules on information use can change the powers that the state, businesses and other people have over us. The personal information echo has the potential to 'speak for us' in these contexts. What it says matters.

Why ask people about personal information?

There are three areas in which it is important to apply an understanding of people's attitudes to personal information: where people's own decision making influences how personal information is used; where people's own ability to allow information to be used is outweighed by wider interests; and where there is a regulatory and legislative regime designed to ensure information is used appropriately. In the decision making related to all three there is a clear role for taking into account public attitudes and bringing about public involvement.

First, people can expect to have some direct say when personal information is used. People take many decisions every day that involve giving away information and engage in many transactions that involve the processing of information. It is important to understand whether the decisions people are making are informed and whether they give people the amount of control they expect. The choices they make may not be well informed. There may be fears about future changes in policy or how trustworthy the data handlers are. There may be penalties associated with not giving consent, for example through price discrimination. How can people shoulder the responsibility for

managing their information decisions? What environment would ensure that people are able to make knowledgeable and meaningful decisions?

In other circumstances, individual control may be neither possible nor realistic. As mentioned above, there are now many more ways for institutions to gather information about the people they serve or provide care for. With new ways to gather information come new ways for those authorities to express their authority and power. There are inevitably questions concerning political values that are reflected in debates about civil liberties, human rights and the role of the state. Campaign groups such as Liberty argue that mass surveillance is threatening rights to privacy – Liberty's director, Shami Chakrabarti, has argued that 'law abiding people have sustained too many blanket attacks on their privacy and they've had enough'.[16] Similarly, journalists such as Henry Porter have consistently connected the uses of personal information with a broader narrative about erosions of liberty and the risks of an unthinking adoption of technologies of surveillance deployed in the public interest.[17] These have helped to feed a media narrative about the disempowering effects of personal information use, and of a state whose reach in the digital age stretches beyond reasonable boundaries.

These are legitimate debates to be had about the role of the state and the consequences of personal information use on that role. But in the debates about the collective effects of the use of personal information, there is room for examining alternative forms of democratic representation. It is important to understand more about how, in practice, the use of personal information is understood by the people it affects, and in turn to give people a greater say in what is acceptable and legitimate. If privacy is about 'social relations and their management', then it is essential to understand how these are being affected in the real world.

Politicians and campaign groups do not have a monopoly on knowledge of social attitudes. Technologists cannot second-guess the answers to ethical questions raised by their innovation. No one can claim a monopoly on the values that are reflected in the application of science, especially where innovation makes

new business models, new forms of authority or new ways of relating to each other possible. The role of public attitudes and engagement work here is to understand whether people feel that organisations are in practice reaching beyond the acceptable boundaries of their authority.

Why a people's inquiry?

A deliberative process such as the people's inquiry does not yield results that are 'representative' of public opinion in the same way that a large poll might. In gathering 40 people together, the aim cannot be to get a single picture of what people think. But statistically representative polling is not the only way to listen to the voice of the public. Deliberative methodologies provide results that are intended not to compete with polling but to complement it.

The benefit of a people's inquiry is that people are not, by the end, like everybody else; they are more informed than they were at the start of the process, since they have been exposed to the opinions and ideas of their fellow participants and of the contributing experts. The people's inquiry is designed to create the space for an informed discussion and to provide an opportunity for participants to make more decisions about the topics being covered. In these methodologies these biases are considered to be of value rather than to limit the validity of the research.

Deliberative methodologies have become popular in the world of public engagement in science and technology.[18] They create an opportunity to involve people more directly in decision making about complicated issues. There are a number of aspirations behind their use. As Jack Stilgoe argued in the Demos report, *Nanodialogues*, this form of public engagement can help mitigate public concerns and confer added legitimacy to decision making. But just as important is the idea that by linking together members of the public with experts and decision makers, deliberation 'might help us to shape innovation trajectories, strengthen the public value of technologies and open up new spaces for political leadership.'[19]

A people's inquiry helps to develop extended conversations between the public and experts about 'science, values and what we expect and want from technology-based innovation'.[20] It can help to bridge the gaps between people and the ethical and political questions raised by scientific and technological innovation. So, this is not just a story about managing problems – this people's inquiry is also about enabling the participants to recognise the conditions under which we can take advantage of the benefits of personal information use.

Reflecting this, this pamphlet not only reports on people's attitudes, but also looks at the decisions our participants made about what action is necessary to ensure the appropriate use of personal information. It does not claim to be the voice of the 'people', but only of those participants who took part in the inquiry itself.

We have tried to maintain a clear separation between Demos's analysis and the voices of the inquiry participants. The findings have to be contextualised as the opinions of 40 members of the public within the profile ranges we set.[21] On this basis, we have been led by the transcripts and we allow the voices of the participants to speak through the pamphlet. Chapters 2 to 5 set out the shape of discussion over the course of the inquiry on our three chosen topics – the use of communications data, targeted advertising and medical information – and on the participants' overall attitudes to control and legitimacy. Chapter 6 on calls to action examines the decision making that participants undertook in the final week. On the basis of these findings, we make certain claims about their implications in the final chapter, generalising from the participants' findings to suggestions for how to act on the demands of the inquiry participants.

Why now?

This is a critical moment in personal information policy making. Personal information is everywhere. There is little we do every day that does not create some trail of data. And as our information echoes grow louder and clearer, so do their possible uses.

That has led to a number of cases where the rights to share, gather or use information are under scrutiny, and where organisations' new power through information is being deployed. In the US in February 2010, for example, the parents of a high school student took federal court action against a school, accusing the school administration of activating students' laptop webcams without their knowledge in order to monitor their behaviour.[22] Google announced in January 2010 that it would review its business operations in China following cyber-attacks, the discovery of which produced, according to the company, 'evidence to suggest that a primary goal of the attackers was accessing the Gmail accounts of Chinese human rights activists'.[23] And following a dispute with a neighbour, a man in the UK was wrongly accused of being a paedophile on Facebook, leading to recriminations from those who wrongly believed the accusation and forcing him to leave his job.[24]

New technologies such as unmanned drone CCTV cameras and body scanners at airports are deployed in the interests of security and law enforcement. And there are ever more ingenious ways to analyse data, for example Experian's Mosiac, which uses 'over 400 data variables … updated annually, [to] paint a rich picture of UK consumers in terms of demographics, socio-economics, lifestyles, culture and behaviour'.[25]

In response, the infrastructure of the database society is passing through a transformative stage. A number of laws and regulatory decisions are being passed that will govern how the questions of individual control and its limits play out in practice. Nowhere is this clearer than in the three policy areas we chose for the inquiry: the use of communications data, targeted advertising and medical information. The topics were chosen because they are live topics that have clear consequences for people's lives. At the same time, all three have ongoing policy debates associated with them that are helping to define individuals', institutions' and organisations' rights and responsibilities on the use of personal information. These three topics set the context for our people's inquiry.

Communications data

The facts of our online behaviour are recordable in minute detail. Some of this information is gathered and stored by the organisations that provide people with mobile phone subscriptions or Internet connections: 'communications service providers' (CSPs). In the past decade, the UK government has passed legislation in cooperation with CSPs that determine how long communications data is held for and when it is legitimate for it to be accessed. The legislations' definition of communications data is the 'who, what, when and where' of communication, not the content of communications (what was said or written). The two most relevant laws are the Data Retention (EC Directive) Regulations 2009[26] and the Regulation of Investigatory Powers Act 2000 (RIPA).[27] CSPs must retain certain kinds of information usually for 12 months, and a number of public bodies are able to request it from them. The laws set out what justification is required to access this information and what oversight exists on its use.

This framework of legislation is under review. In April 2009, the Home Office launched a consultation, *Protecting the Public in a Changing Communications Environment,* looking at changes to the way that communications data is gathered and stored.[28] In the Foreword to the report, then Home Secretary Jacqui Smith said that the aim was to find the 'right balance between maximising public protection and minimising intrusion into individuals' private lives.'[29] The paper argued that advances in technology had led to a need to update powers of access for law and security. Proposals included requiring Communication Service Providers to collect data from third parties.

There was also a consultation in 2009 on the legislation governing access to communications data, the Regulation of Investigatory Powers Act (RIPA).[30] The act has been heavily criticised for being unnecessarily intrusive and for giving too many public bodies access to the data, with the justification for access too widely defined; for example, Liberal Democrat Shadow Home Secretary Chris Huhne said that 'without reform, RIPA will continue to be a snoopers' charter'.[31] A number of responses to the consultation document proposing changes to RIPA were concerned about the scope of access and highlighted

concerns that clearer definitions were needed about the 'necessity' and 'proportionality' of access rights under the act.[32]

But the Interception of Communications Commissioner, who is charged with the task of overseeing the use of the act and ensuring that any access to traffic data fits within legislative boundaries, suggested in his 2008 review that there was no evidence 'to indicate communications data is being used to investigate offences of a trivial nature … On the contrary it is evident that good use is being made of communications data to investigate the types of offences which cause harm to the public'.[33]

At the same time, there have been moves in the UK towards using similar kinds of information to enforce a wider range of laws. For example, the Digital Economy Bill sets out measures that would involve using information about online behaviour as evidence of copyright violation. Detractors have suggested that the bill is not clear enough about the process through which the relevant information would be stored and disclosed.[34] And in an international context, countries like China engage in widespread filtering and censorship of citizens' Internet use.[35]

What laws warrant the use of personal information use? What boundaries should there be around the kind of information generated and stored about what we do online and what it can tell others?

Targeted advertising

There are other ways to use the information gathered from our time online in commercial contexts. One example of this is marketing that tailors what is presented to users based on some understanding of them. That might be as simple as advertising that reflects what is on the page users are currently looking at, or it might extend to using 'cookies' to build a more detailed picture of past behaviour and preferences and then adapting content based on the knowledge thus obtained.

Phorm, a provider of one particular type of tailored online advertising, attained an unfortunate level of infamy in 2008 and 2009. The company attracted significant criticism from privacy

and digital rights campaigners largely for failing to get the consent of customers in trials of the technology[36] – despite having had their technology reviewed by privacy experts and claiming themselves that their technology 'can never identify individuals, never stores any personally identifiable information and keeps no record of where they have been. It anonymously understands what a user likes in order to match it to the right content or advertising'.[37] This led to the UK being subject to an infringement proceeding from the EU in April 2009, concerning the implementation of directives designed to ensure that communications are 'intercepted' only with consent.[38] The EU moved to the 'second phase' of the infringement proceeding later in 2009, maintaining that 'the UK is failing to comply with EU rules protecting the confidentiality of electronic communications like email or surfing the internet'.[39]

Many services such as Google rely on advertising revenue. And advertisers are looking to targeted advertising of some form to improve the returns on advertising spending. In the first half of 2009, Internet advertising expenditure grew 4.6 per cent, to £1.75 billion, overtaking TV for the first time. The Internet Advertising Bureau found that one of the drivers of this growth was 'insight tools which mean more advertisers flock to the medium to take advantage of its targeting, accountability and measurability.'[40]

In response, there have been tentative steps towards intervention from regulators. In October 2009, the Office of Fair Trading announced it was launching a scoping project designed to look at the impact of targeted advertising.[41] And in the US, the Federal Trade Commission issued 'Rules of the Road' designed to protect 'business and consumers – and help maintain the credibility of the Internet as an advertising medium.'[42] The same year the Internet Advertising Bureau published its self-regulatory 'Good Practice Principles' for online behavioural advertising, with a number of leading advertisers signed up.[43] The Information Commissioner's Office began developing its 'code of practice' for online information in early 2010.

The concerns about targeted advertising relate in the main

to the extent to which consumers are aware of the information they are giving away and of the way that the information is used, and the extent to which they are able to control when they give it away and manage the effects of its transfer.

Medical information

In 2002, the government launched the National Programme for Information Technology (NPfIT). Central to the programme is the development in the NHS of the Care Records Service and a national Summary Care Record (SCR), containing basic information which 'will be available to people providing you with care anywhere in England.'[44] The role of the SCR is to enable the communication of essential patient information across various parts of the NHS, such as A&E where access to a patients' full medical record is currently unavailable. The Care Records Service covers the transfer of paper medical records to electronic records systems.

The result is a series of possible benefits including greater efficiencies, speed of access and patient control. Electronic records are designed to improve access to medical records among professionals, to be a tool to help people manage their own care more effectively and to encourage a better relationship between professional and patient. However, there are a series of challenges too. By digitising records, the information in them is made more available to more people, creating new vulnerabilities. The extent to which this is the case depends on the success of the processes controlling access.

Further, medical information could be used to inform the perceptions of people's well-being and health-related decisions. This opens the possibility of using such information to try to encourage healthier lifestyles. This is especially so in an environment of 'Nudge' politics in which the role of state interventions into health behaviours is highly contested.[45] The raw material for judgements about behaviour and lifestyles, and what services are offered in what ways as a result, is available as never before. As medical records are used more widely in digital

environments, that means we might put at risk the very principles on which records sharing is based: autonomy and empowerment over health and well-being.

Lastly, with a greater amount of easily accessible information, there are opportunities for medical research to gain access to more of the raw material of research. With the ease of sharing comes the risk that sensitive information about medical histories will be used in ways that some find objectionable.

The debate around electronic medical records has centred on the means of storing medical records, its security, and people's ability to consent to its various uses, whether it be the sharing of records among health professionals, for medical research, or its access by those outside of NHS and the public sector. Will the design of systems create more points of vulnerability for medical records? Who should legitimately be allowed access, and what control will people have over those decisions? Can people opt out of uses they do not agree with?

The questions for the inquiry

This policy context set up some clear questions for the inquiry to explore. As traffic online increases, generating far greater quantities of data about people's online behaviour, what sort of law enforcement surveillance is acceptable?[46] Further, for what broader purposes is it legitimate to access this kind of data? In making decisions as consumers, how well informed are people about the kind of advertising and marketing presented to them? Do people feel this is tipping the balance of power away from the consumer?

Overall, do we need greater checks and balances against the power that accrues to those who handle information? Do people feel that legislation and current practice provides them with enough control over what their information echo says – and over how it affects their lives?

The findings from the people's inquiry

Written with Ollie Haydon-Mulligan

In November 2009, Demos gathered 40 members of the public to embark upon a month-long investigation into the use of personal information. Twenty people met in the Demos offices in London on Wednesday evenings, and 20 in the basement function room of a Best Western hotel in Bradford on Saturday mornings. Both groups met four times, once a week for 3½ hours each time, covering three discrete policy areas as well as the broader issues of consent and regulation. By the end of the month they had heard from a series of experts, completed 13 hours of deliberation and settled on 42 'calls to action' that highlighted responsibilities for government, regulators and businesses.[47]

The people's inquiry discussions were framed by the questions of legitimacy and control. That led to a focus in the first week on what personal information is, who uses it and people's capacity to consent to its use. To introduce these issues in London, in the first week of the inquiry we invited Liam Curren, a researcher on the EnCoRe project,[48] and Dan Cooper, partner at law firm Covington & Burling LLP. In Bradford, we welcomed Sue Cullen from Information Law experts Amberhawk. These themes of control and legitimacy ran through the inquiry and informed the approach to the discussions of our three topics.

This section outlines the results of the people's inquiry by reporting on the key themes that emerged from the discussions of each of the topics. We explain the shape of the discussion and reflect the inquiry members' voices as clearly as possible. Following these three chapters, we set out what participants told us about the broader issues of control and legitimacy. We also report on how attitudes changed over the course of the inquiry. This includes results from the survey of participants that we ran at the start and at the end of the inquiry, asking people about

their awareness of personal information issues and the trust they place in organisations that handle information. This fifth chapter details how participants came to identify informed choices and stronger regulation as the key components of legitimate information use.

The section closes with our inquiry members' 'calls to action' – the recommendations they felt would help address the challenges they had identified. In response to the concerns echoed across the findings, these calls to action were aimed at creating better conditions for individual decisions; making the choices people make to give information away and consent to its use more meaningful; and holding organisations to their word through better regulation.

2 The use of communications data

In its second week, the people's inquiry focused on the issue of online information. This covered the use of communications data as well as targeted advertising. This chapter sets out participants' attitudes to the way communications data is used and how access to it is regulated. Inquiry members considered the public interest arguments behind the legislation granting access to communications data, the degree to which they consider these arguments legitimate and whether the public interest should outweigh individuals' ability to consent to its use. At the same time, they discussed the kind of laws that communications data should legitimately be used to enforce.

To help introduce this topic, we invited Martin Hoskins, Head of Data Protection at T-Mobile, to talk about the retention of communications data by providers, and Natalie Hunt, of law firm Hunton & Williams, to provide an overview of the law that governs the release of communications data. In Bradford, we again hosted Martin Hoskins, who covered both the gathering of data by communications providers and the legislation surrounding access to it, with a handout from Natalie Hunt available to participants summarising the points from her talk in London. In the second half of week two, the inquiry turned to the issue of targeted advertising, covered in the following chapter.

What participants said

Male: I'm actually much more concerned about my wife and kids seeing a dubious search history on my computer than I am about any government seeing the search history.

Session 2, London

Our participants were comfortable with aspirations to use communications data for law enforcement and security and they evidenced high levels of trust in the institutions charged with doing so. These sentiments extended to the use of communications data by local authorities and the list of public bodies cited in RIPA. There was no sense that legislation had gone 'too far', and there was no overall fear of the 'snooper state' when talking of RIPA. In Bradford, for example, one participant confessed that 'I've got no problem with the local authority being able to check up on me to make sure that I'm not cheating benefits.'[49]

The groups felt that RIPA allows information to be used for useful and legitimate purposes: saving money for the taxpayer and, above all, fighting crime, from benefit fraud to the more serious offences that are of concern to the police and law enforcement. RIPA was seen as serving the public interest, and some participants justified the uses RIPA permits even where individuals object:

That's why we've got it for everybody haven't they? It's not individuals. Imagine if we all said 'Oh, I don't want them to be able to access it.' It's out of our hands isn't it? … whether you like it or not, it's not a personal choice.[50]

As the following quote from the London group exemplifies, the public interest in organisations having access was crucial:

There's bound to be an element of misuse … but the object and the purpose and the benefits that are derived from it, by and large, probably outweigh the disadvantages.[51]

For some there was even a concern that it could be *too* hard to get access for those that need it, especially for the purposes of law and security. In London, for example, one participant argued that 'there [are] definitely too many hoops … to get the information they need to protect us.'[52]

But is it that clear-cut?

However, the participants' faith in government and law enforcement was not unconditional. Members recognised that this was a delicate balance, that there should not be a situation 'where they can just phone up a bank and get information.'[53] There were concerns about cases where the official justification is sound but is undermined by insecurity, along with other times when the justification for the use of communications data is questionable.

For example, participants had fears that an overzealous pursuit of law enforcement might lead to misplaced suspicion. Further, there were concerns that the idea of using personal information for the public good, and specifically for law enforcement, would be applied too loosely, to laws that were not considered serious enough to warrant that form of enforcement. The principle of enforcing the law through the use of communications data was not considered to be absolute.

Insecurity and human error

There were also fears about insecurity due to human fallibility, whether this be through mistakes or corruption. As one participant in Bradford suggested, 'there's always human error … There's always going to be someone who's going to be manipulative and they might use it for the wrong reasons.'[54] There was seen to be a security risk relating to so large a volume of information being available: 'you don't know whether they're selling it to all the authorities that are named on the list. It's whether an outside businessman comes who has got a bit of money and he wants to buy information. Will they sell it or not?' And there were some concerns that the Interception of Communications Commissioner does not have the resources to properly regulate RIPA. These all tended to undermine the belief that the information will be used only in the intended ways, that the powers will not be abused and that data will be kept secure.

Unease at how much information is available

Reflecting this concern about who has access to the data itself was a degree of unease with regard to the amount of information available now and what might be available in the future. Some participants expressed unease at the thought simply of strangers accessing personal information and at the prospect of more detailed tracking than RIPA allows (even if it is for law-enforcement purposes):

The thing is though, I don't mind you … knowing who I am … I don't want you to know who I am, where I am, what I do … how much I earn, what I do in my spare time, what movies I like watching, what music I like listening to. What I do on a Saturday, what I do on a Friday morning … I don't know you. And that's my problem.[55]

This was manifested, for example, in a belief that diligence in enforcing the law might lead to innocent people having to justify themselves and accept an unwarranted level of suspicion. The hassle and irritation caused by such suspicion was typified by an experience one participant had in their bank:

There was a bank clerk asking me [about why I was paying in cash]. And I know she's only [doing her job], but she [said] 'well why haven't you just done it direct from your account?' But I was paying with last week's money in cash to pay towards my credit card … you know, sometimes you get asked too many questions and you just get a bit fed up with it.[56]

This exemplified a concern that the use of communications data might lead to miscarriages of justice, by creating misplaced suspicion and causing suffering to law-abiding citizens.

In a similar line of thinking, participants rejected the idea of having online 'content that you're looking at' monitored, and 'the emails you've sent': 'well that's private isn't it,' explained one participant. 'To me it just seems wrong,' admitted another.

Function creep

While participants were fairly comfortable with pubic interest arguments as they currently stand, there was a concern about the

justifications for access creeping beyond reasonable boundaries. For example, participants worried that definitions may be too broad – that, in effect, organisations 'can ask for anything' – and participants worried about how these definitions and their scope are decided upon. These questions were seen as candidates for a more open debate, as demonstrated by the feeling of the following participant from Bradford: 'the spectrum of what's important and what's not – in itself, it would have to be a debate … It's not something that can be determined necessarily by the local authority.'[57]

There were also concerns about future changes in policy that might stretch the powers to use data in ways that undermine the public interest argument. Being clear about the justification for access was therefore held to be important:

It's not the fact that people have access to it. It's the justification for [it]…. I'd hate to think that someone at the local council had wanted to know who I'd been calling.[58]

The crime matters

One aim of the discussion of communications data was to understand the limits of when this kind of information should be used. Did participants feel that it was legitimate to use communications data to enforce laws less directly connected with law enforcement or the work of public bodies? Part of week two was spent discussing the possibility of using communications data as evidence of copyright violation.

Participants felt that there are areas where the fact of illegality may not justify the use of personal information for enforcement. Law enforcement was important, but in some cases the law might be wrong, and the crime might not warrant the particular method of investigation. There was a concern that prosecution through access to data might happen for 'minor misdemeanours … not worth prosecuting…'[59] And there was concern that 'it has to be proportionate. The enforcement of the law has to be proportionate to that crime.' As one participant summed up when discussing illegal downloading, 'it should

be quite literally, the most prolific use … They should be prosecuted'.[60]

It was considered less important to enforce laws that served private interests rather than the public interest. There was therefore a dilemma in reconciling the motive for enforcement and the illegality of the act, summed up in Bradford:

Female: The authorities are doing it [for] crime. The only reason they do it [for copyright] is profit.
Male: Yes, but it is crime.

Participants acknowledged that, in the context of copyright infringement, the activity is wrong, and a sense that this legitimised trying to catch the person doing it: 'if it's something wrong it's something wrong isn't it? They spend loads of money on CDs or music and then you just grab it for nothing. It doesn't really make sense.'[61] However, at the same time, they felt that there should be no easy access to the information for those whose motive is commercial; even if copyright law should be enforced, the copyright holders themselves should have limited access to information about offenders.

Participants' concern was often about who would have access to the information itself. When talking about copyright holders' rights, one participant summed this up neatly: 'They shouldn't get the information [about] who is doing it. What they're doing. But there should be a way to prosecute people who do it. But … to get my name, my address, my details to say that I've done it? It should be secured.' Similarly, another envisaged that a better system would be 'if it was just a report of the offence without the information being passed to them.'[62]

People recognised the need to use communications data to enforce laws, in the interests of security, or by other public bodies carrying out their duties. The public interest in the law and security context was seen as strong partly because the use of the data seemed proportionate to the power participants would expect such authorities to exercise, and because the laws that can be enforced through RIPA were not, in the opinion of our study members, trivial. However, the belief that the current use of

communications data was appropriate was tempered by concerns about the extent to which present aspirations regarding future restrictions on use were realistic, with questions about the scope of access, possible mistakes and human error, and the insecurities and vulnerabilities of the data itself.

Key findings

- *Faith in the aspirations to use communications data for law enforcement and security was high, as was confidence in the uses specified under RIPA.*
- *Participants displayed high levels of trust in the relevant institutions and in the motivations of people working within them.*
- *Concerns existed with regard to cases where the justification for the use of communications data is questionable (for example, in enforcing what participants saw as less important laws, or where innocent people could be placed under unnecessary suspicion).*
- *Participants worried about cases where the official justification is sound but is undermined by insecurity (for example, through human error or corruption).*

3 Targeted advertising

In the second half of week two, we examined the use of 'targeted advertising' and the various techniques for using personal data to understand something about customers in order to change the offer available to them. The aim was to outline some of the different ways to target content, to explore the benefits and risks and to discuss the trade-offs between them. This involved examining the possible effects of targeted advertising and the extent to which users have the ability to express their consent to its use.

To help the inquiry members in the second half of week two, we turned to Alma Whitten from Google, who set out the way that various forms of targeting work. We also wanted to set out some of the concerns that consumer advocates have, and for this we turned to Anna Fielder, a consumer rights specialist.

What participants said

'Male: I think it's useful, but then if it's not there, it's not a big deal either.'

Session 2, London

Overall, targeted advertising was not seen as a serious problem. Inquiry members' attitudes were typified perhaps by the claim from a participant in London in week two that, as far as he was concerned, 'it's just something that's almost irrelevant. It's all surface noise that you don't pay any attention to.'[63] Some went further, and in Bradford one participant said: 'there's no harm at all'[64]. The key to this impression was that in most of the forms described to them, targeted advertising was something that they, as savvy consumers, were able to manage. And

moreover, they recognised some of the benefits and trade-offs associated with targeted advertising: free or cheaper content, useful recommendations and better deals.

But at the same time, it is not the case that inquiry members did not identify problems with the use of targeted advertising. These related mainly to people's awareness of exactly what was happening, the extent to which they had any meaningful capacity to control when they give away information and their concerns about those less able to manage this new environment of choice and targeting. Even though it was considered to be something that on the whole they could deal with, participants recognised that different people would make different decisions about the trade-offs between the risks and benefits. The ability to control targeting was seen as essential, and participants expressed a desire for greater awareness of and transparency in the process. The concern about 'third parties' hung over the session as it did with all others, with a feeling that beyond every transaction there are a number of deals, mistakes or hacks that lead to information being 'passed around the houses'.

The perceived benefits

The inquiry members could see the benefits of targeting. For example, it was often considered appealing either because it led to you being presented with more relevant content or because it would help you to discover better offers. Participants also appreciated the added speed and convenience that gathering information about customers might bring.

Some participants acknowledged that there are business models that rely on successful advertising and targeted marketing. For example, during a discussion in session four in London about whether to give people more direct financial rewards in exchange for companies using their information, one participant noted that the company in question 'will turn round and say … our prices are accommodating that. Because we know that we can sell your information … we can bring our prices down by 15 per cent. You're being remunerated.'[65]

What is really new?

When talking about the purpose of targeted advertising, rather than the means of doing it, a recurring question was whether it was a new concept. Many compared it to getting to know the owner of a local shop, who may subsequently offer you good deals, get to know what you buy and predict other items you might like. Similarly, when discussing price discrimination, there was some feeling that it happens already and that in the context of insurance in particular, it was actually the right of a business to know something about their customers. The three aspects of targeting that were picked out as new were the speed at which it happens, the amount of information it is possible to gather and use and the number of people to whom it is available.

When targeting is a problem

Targeting was considered a problem when it led to the appearance of inappropriate or useless material, to increased vulnerability for less savvy consumers and where the targeting changes the balance of power in the deal between consumer and businesses. The most consistent feeling was that people had no real or meaningful capacity to make informed choices and to fully consent to the use of information. Awareness of how information is used and what the effects are was seen as being very low. And participants felt that their decisions had little effect on the behaviour of organisations that held their data. That meant that they were concerned about having no control over vulnerabilities, mistakes or deals that happen after the transaction in which they are involved.

Awareness

Female: *Sometimes I quite like targeted advertising, because if it's something that's really caught my eye, great, it saves me having to search for it.*
Male: *But it depends what they do with [the information] though.*
Female: *This is it, I'd rather know, it's being bought, where it's going and then what they're doing with it.*
Session 4, Bradford

Participants may have been aware of the issue of advertising online generally, but they were concerned that they had little awareness of how targeting works in practice. Awareness varied across the different types of targeted advertising, with more having heard of 'cookies' and of the management of browsing information in that context. On the other hand, there was very low awareness of more sophisticated forms of targeted advertising. There was a strong reaction against what participants perceived 'Deep Packet Inspection' (DPI) to be: the 'reading' of content as it passed from websites to their computers, with advertisers tailoring adverts to that content. The former was seen as more manageable because the 'cookies' are stored on people's computers and therefore lay within people's power to control. But with more sophisticated forms of targeting, participants were more wary – and they were particularly uncomfortable with DPI, over which people felt they had no control, as the process seemed to take place beyond the limits of their direct power.

Further, while inquiry members felt they could make a choice about a single transaction through giving consent, their concerns often extended to what happens afterwards – the hidden exchanges, possibly unlawful deals and third party agreements obscured by a lack of transparency and consent forms that were, in their eyes, meaningless. One example discussed was an online retailer's terms of reference. The unspecific reference to 'third parties' unsettled participants and helped feed concerns that after the transaction there would be a number of uses of their information over which they could have no control.

The problem of targeting not being good enough

Some participants worried that the targeting would not be smart enough to ensure that material was always appropriate for the user, potentially leading to embarrassment and the appearance of inappropriate material. A number of participants used the example of adverts for engagement rings:

Female: Say you were living with someone and they'd been, spent the last few months looking for engagement rings and you went on the computer and suddenly you were bombarded with engagement ring adverts, as an example – there might be things that you don't want other people using your computer to necessarily know about.[66]

This was felt to be a practical problem of more than one person using the same computer or account; that 'it may not even be about you because it says if you've got your wife, yourself, your kids on the computer, it's storing a lot of information'.[67] This was seen as a serious problem where participants envisaged more adult content based on parents' profiles being inadvertently shown to children.

When targeting is 'deal changing'

The inquiry members were clear about their relationship with the private sector. As we explain further in the chapter on control and legitimacy, the 'wary scepticism' that defines this relationship requires a feeling of parity with businesses and understanding the terms of engagement with them. Targeting was seen as a problem where it shifted the power in that deal making towards businesses. This was seen as possible in two ways: targeting might deny someone something they wanted, or it could be used to determine the choices with which they were presented.

In both cases it was acknowledged that this already happens and is to some extent within the rights of a business. However, there was a feeling that there should be limits to the amount of information businesses can have. And more fundamentally, there was a concern that some forms of targeting might mean that a person's choices would be shaped by the targeting in ways they were unaware of, leading either to a narrowing of choice, or more seriously in the eyes of participants, price discrimination. There was a lack of clarity about the extent to which it can and does happen, and who exactly would be affected. But there was a general unease about its effects:

I think discrimination is one of the biggest problems … Demographically I'm thinking I'm only targeting between 25 and 35-year-olds and you're 65, I don't want to sell it to you. It's effectively, it goes back almost to kind of, I don't know, it's just discrimination.[68]

The uncertainty about exactly when and to what degree targeting was technically possible, and how effective it was, led to a desire for transparency about where it was happening. In cases where targeting changes the terms of the deal, it was generally seen as problematic where it happened without people's knowledge and where it unfairly led to some people being denied products or services.

Vulnerable consumers

Participants were in the main comfortable that they could manage the problems of targeted advertising. But there were references to those vulnerable groups who might not be able to. In that respect, targeting was seen as a new channel for old ways to play on people's naivety. In Bradford the presence of targeting was seen as 'like your old-fashioned knock on the door to old folk [who might end up] getting ripped off.'[69] Young people in particular were seen to be vulnerable, despite having grown up with the technology, a debate that one exchange summed up well:

Female: *We didn't have computers at school and now they just do it as a standard thing, so I just think they'll get more savvy and they'll get taught things and so how to look after –*
Male: *I still think they're more likely, just to give themselves away though.*[70]

In discussing how to manage these vulnerabilities, participants felt that while we had some simple solutions in the offline world for managing risks and harms, we had yet to work out digital equivalents. Extending the comparison with traditional offline shopping environments, one person wondered what the equivalent of the magazine 'top shelf' would be in the digital world.

Does informed choice mean anything?

Being able to make an informed choice was seen as essential. But as it stands, this was not seen to give participants an adequate level of control over information use in commercial environments. Inquiry members did not feel that they were aware of how targeted advertising works, what the effects are in reality, and the ways in which people can consent to it or otherwise. Allied to this were concerns about insecurity and the possible effects of targeting, and about those less able to manage an environment of more sophisticated targeting.

In the first half of week two, participants discussed the conditions under which the public interest argument outweighs their capacity to consent to the use of information about their time online. The principle behind the use of data was felt to be legitimate, but there were concerns about how it was applied in practice. But in the second half of week two, the legitimacy of targeted advertising and its use of personal information depended more on meaningful consent and awareness. They expected to know what was happening and how they could make a meaningful choice about whether it was acceptable. They felt that the nature of their relationship with the private sector depended on their ability to enter into deals fully aware of the other parties' knowledge of them. Even though the services that relied on targeting were seen as useful, the use of personal information in these commercial contexts was seen as acceptable only under these conditions.

Key findings

- Targeted advertising was not seen as a serious problem as it stands.
- Participants felt able to manage their choices and saw the potential for targeting to be a good deal.
- The ability to control targeting was seen as essential, including a desire for greater awareness and transparency.
- Third parties and the insecurity of information were deemed to be risks.

- When targeting resulted in price discrimination or determined the choices available to consumers, awareness and consent were seen as especially important.
- Participants were aware that there might be other more vulnerable people who could be exposed to the risks of being drawn into bad deals.

4 Medical records

In the third week of the inquiry, we turned to the issue of medical records. First, we looked at the moves to digitise personal medical records and create a system of access to them across the health service, and secondly, we examined the use of medical information for the purposes of research. In doing so the inquiry members continued to explore the trade-offs between individual control and wider interests and the areas where the two might conflict.

To help introduce these topics in London, we invited Marlene Winfield of the NHS to outline the current state of play with regard to electronic medical records and Stephen Whitehead from the new economics foundation (nef) to set out some of the critiques of the plans. Michael Keegan from the General Medical Council (GMC) spoke about the way medical records are accessed for use in research. In Bradford, we asked Mohammad Al-Ubdayi, of PatientsKnowBest, to speak on the topic of personal medical records, while Stephen Whitehead spoke on the use of medical records for research.

What participants said

I don't think there's a problem really, I mean generally it'll be a trust … thing. As long as everything's explained to me, you wouldn't worry too much.
Session 3, London

The groups saw the intended uses of communications data under RIPA as in the main legitimate, and the idea of targeted advertising, under certain conditions, seemed to them a potentially fair deal. On the subject of medical research, the pattern of debate followed a familiar form. Participants again

identified legitimate justifications for the use of personal information – to deliver more joined-up healthcare, to give people better access to their own records and to further research in the public interest. There was a strong sense that digitising personal medical records has great potential to improve standards of care. Similarly, allowing access to medical records for the purpose of research also found strong support.

Just as the concerns about RIPA were to do with insecurity and unintended use, the concerns about electronic medical records were largely about ensuring that access remained tied to the intended, legitimate uses. The main concerns in this respect related to the vulnerability of information through the channels of access that would be available (through leakage, theft and loss).

At the same time, participants felt that largely legitimate uses were only fully acceptable when associated with control and transparency. These were seen as the threshold conditions for making the use of medical records acceptable. This 'threshold' varied according to the different justifications for and motives behind use, with a stronger desire for control and transparency where information was being used by the private sector or those not involved in providing care.

Legitimate uses for electronic medical records

Inquiry members discussed a number of purposes for electronic medical records, with a general feeling that in a variety of cases its use was legitimate and could potentially lead to many benefits.

'It's a no-brainer'[71]

Participants expressed very strong support for the system of electronic personal medical records that health professionals can access. 'Joined-up' access '…would give you a faster treatment and hopefully diagnose you quicker with your problems. So you've got to condone it.'[72] In addition, 'risks of lost data' in the current system would be reduced: your medical records couldn't

'get lost in the post'.[73] The plans were seen as common sense. There was some incredulity that it had taken so long:

I thought whichever hospital you went to if you had an accident down south or in Scotland you wouldn't have to tell them who you were and they wouldn't … I thought that everybody had access.

In the current system, 'it could take forever to get your paperwork to another [doctor or hospital] … if at all'.[74] One participant in Bradford, who works for the NHS, spoke about the frustrations currently experienced:

I work in a local authority building and I don't have access to the records that I desperately need. So I have to get in my car, drive down to the hospital, go look at the notes then write down everything that I need to write down. Because my system – the computer systems that I work with day-to-day are not connected to the PCT systems.[75]

Some participants saw the attraction of accessing, and in some cases being able to update, their own records. It was felt that this would improve accountability and, as participants in Bradford argued, might apply pressure for quicker processing by GPs and consultants.

Participants were also strongly supportive of the need for medical researchers to use medical information, especially in the discussions about cancer registries and the 'Biobank' project.[76] That response held even where they acknowledged that the research would not be of direct benefit to them. They tended to justify this by pointing out the benefits for people they know, for their children, or for future generations more widely:

We think that the researchers should have access because we hope in the future that there will be cures for cancer, HIV, diabetes, Alzheimer's – any incurable disease. We might be long gone but our children will still be here and hopefully we'll get the benefit from that.[77]

As with some uses of communications data, participants believed the benefits of medical research could outweigh

individual objections if they were raised: 'it's imperative', as one participant put it, to help support medical research.

There was also some support for the use of medical information in other cases not linked to care. For example, participants recognised that insurers and employers have legitimate reasons to use medical information. However, as will be discussed below, there were certain conditions attached to these examples.

The challenges

As with communications data and targeted advertising, inquiry members identified challenges that might lead to these legitimate aspirations being undermined in practice. Some of these were very practical worries about the difficulty in implementing technology successfully. One participant in London argued that 'the whole point of having it is for it to work well and get results … If … it doesn't work properly then it will have terrible effects.'[78] There were fears, for instance, that while the point of electronic records was to increase efficiency, the system would instead lead to more costs and time losses, because of additional training needed to use the technology and problems with it breaking.

Access by the wrong people

While there were clear attitudes on what constitutes legitimate use of medical records, participants were also clear about who should be carrying out those functions.

For example, with regard to people's electronic medical records, the inquiry members felt that access should be restricted to 'those who provide care'.[79] In this context, there were concerns that the systems for ensuring access might not work, leading to the wrong people seeing medical records – either people who simply did not need to have access in order to further legitimate uses, or those with some other commercial or criminal motive. There was a concern about 'every Tom, Dick and Harry' who works in a pharmacy or hospital, with references

to pharmacists and receptionists a signal that boundaries fell around those who were deemed to have a relevant role in helping treatment and providing care.

Likewise, there were fears based on the vulnerability of any electronic system, as 'there's always people out there that are such techno buffs that they could do anything if they really wanted to'.[80]

Underlying these challenges was an acknowledgement that electronic records will ultimately be handled by people, leading to the familiar conundrums of human error and fallibility. Firstly, participants acknowledged that people can be corrupt: 'you're always going to get, within any setting or any profession, people that are going to abuse' their position, 'selling [medical details about a celebrity] to the newspapers', for example. And secondly, inquiry members worried that 'the more people that have got access to them, the more chance of human error'.

The 'role-based' access model was held to be very important: different groups were seen as having legitimate reasons for accessing different amounts of information and keeping within these boundaries was seen as essential. Participants held that the ability to decide for themselves, through specifying conditions directly, who would be able to see what, was an attractive proposition and helped to alleviate fears about unnecessary access. But there were serious concerns with how effective these technologies will be in practice. When learning that the system to hide parts of your medical records was not ready yet, for example, one participant remarked 'that's where the part would come in where people wouldn't … feel comfortable telling their doctor things.'[81]

The public and private sector

As with the use of online information explored in the previous chapters, there were concerns about third parties and the private sector where it was unclear that they had a need to access medical records. This was again put fairly bluntly: 'what we're saying is no third parties. Not the private sector'.[82] This applied when discussions turned to the use of records for research, where

for example participants were concerned that pharmaceutical companies could search through medical records to find acceptable study subjects.

The distinctions between public and private sectors in week three rested on the perceived motives of each group and affected how much control and information people expected. And in a similar way to the other topics, participants felt that the likelihood increased that the medical information would be more widely available if it was held by pharmaceutical companies: 'if we say if we agree to consent, it doesn't mean that they're allowed to just dish out the information to insurance companies and things like that.'

However, there was a less visceral reaction against the private sector when discussing the specific examples of access to personal medical records. It was seen as acceptable for the insurance company, for instance, to request information once an approach had been made by the individual for insurance. The 'direction of travel' of the request was important. Participants were more wary of information about specific conditions speaking for them without their knowledge or consent, for example where insurance companies could trawl through that information without their knowledge: 'if I'm asking BUPA to get involved, yes … Not from the other way round.'

Similarly, in discussing employers' access to records, it was not considered acceptable for employers to request some forms of sensitive information, such as information about mental illness, in an application process. However, there were other kinds of information that were considered legitimate, for example information that organisations might legitimately expect to affect people's capacity to do a job; dyslexia was one example considered.

Participants were concerned in both cases that the potential consequences were inappropriate health profiling, and especially that people would open themselves up to being targeted because of a particularly rare or medically 'interesting' condition. As one exchange in week four in the London group showed:

Male: If you have an unusual medical condition. You could become a target for research, insurance purposes. Donor requests.

Male: So in some way, you need to give some kind of consent … to allow your details to be used for that specific targeting.[83]

This was a similar concern to that raised in the targeted advertising discussion regarding the possible 'deal changing' effects of targeting. Where organisations use personal information to make important decisions affecting the service or products to which they are entitled, participants felt that the information should not speak for them without their knowledge. Familiarity with the information being used and the capacity to make a decision about whether its use was acceptable were considered important.

The relationship between patient and health professionals

A further worry about the switch to the use of electronic records in the provision of care was that there would be a strain on relationships between patients and health professionals, or that changes to these relationships could compromise healthcare delivery. If patients have access to their own medical records, they might be offended by the information doctors write down: 'I've seen some of the letters from various consultants and you have to giggle. I'm glad that's not me they're writing about.'[84] Some feared that it might lead to a more adversarial dynamic: 'there could be a hell of a lot more lawsuits against the NHS'. Doctors might 'hesitate' to record information that 'would have been really useful' to some other professional. And this kind of selectivity could worsen the patient-doctor relationship: 'there's a risk that you will lose trust with your own GP'.[85]

Some participants worried that the record might come to replace the relationship with the health professional rather than enhance it. One manifestation of this was a concern that the sensitivity around test results was respected, and that people were not put in the position of having to process results before speaking to a doctor.

What if policy changes in the future?

Participants were afraid that, however acceptable uses are now, the system could be abused as intentions and policies change. Just as with the concerns about future changes of policy on communications data, participants were realistic about the risks of 'function creep'. One participant warned: 'we've got it all relaxed and all these lovely rules … It only takes a small amount of time and suddenly another administration to come in and go, "In actual fact, we can use all this information…"' Another used the analogy of the donor card to describe the temptation towards function creep: 'I'm pretty sure that they're not going find your card if there's something about you that's particularly attractive to be, yeah, to be 'harvested'. And then it's too late.'[86]

In the context of access to personal medical records, inquiry members discussed how people outside the NHS might gain access if plans change. There were worries in London that, eventually 'they might write the law saying, "We don't have to get the patient's consent now. We can just share the information."' Changes 'once it's set up' could mean 'you don't have the power and the private sector could look at things, or other access could be given'. Where there are not strong rights to say no, participants suggested that it would be hard to enforce consent, or that there may be a risk of function creep.

Threshold conditions: control and transparency

Our participants considered the use of medical information to be valid in some circumstances, but only under certain conditions. For example, in the case of access to access to electronic records for care, audit trails, to make users more accountable and individual control to vet those who have access were considered attractive and important mechanisms. Transparency and control were the threshold conditions under which the use of medical information became acceptable.

The first threshold condition for the use of personal information in a medical context was control. The ability to cloak and restrict access to electronic medical records was seen as extremely important, alongside a robust audit trail of access

requests. A desire for direct control was thought necessary as much for peace of mind as for its practical application.

The second threshold condition was high levels of transparency over exactly what information is used for. As it stands, awareness was thought to be too low: 'You've got a letter … saying if you don't consent then tell us. But we don't know what that means, do we.' Informed consent was quickly defined as knowledge of 'a who, what, where and how … of all your information'[87]

Despite a belief that there are strong public interest arguments behind medical research, awareness was seen as a particular problem in this context: 'I felt frustrated because you think there's lots of things going on that we don't know about.'[88] Another participant felt that 'we do need a lot more visibility of who is responsible for what.' [89] Others specified what they felt people needed to know, including 'transparency on how researchers are approved, [and] how research is used', and 'what's it going to be used for and also feedback on the reliability of what they're [doing]'. An example of the dichotomy of transparency that participants discussed as existing between the public interest and the rights of the individual was apparent once again in the context of Biobank and cancer registries. While inquiry members recognised the benefits of both initiatives, there was disagreement about how they interacted with the rights of the individual. In one group in particular participants argued that the rights of the individual should remain strong and that this required study subjects to be kept up to date about the use of their information, and especially about any findings to do with their own health. This need for transparency on an individual level was seen in this group to outweigh the interests of future generations.

The discussion of these conditions of control and transparency took place in the context of debates about opt-in and opt-out consent. People recognised the practical benefits of an opt-out system for the digitisation of medical records; as one put it, 'I personally have no objection to being on it but I'd never write to say "Yeah put me on it."'[90] But the question of whether opt-in or opt-out is more appropriate tended to be less relevant

than a concern for transparency and clarity. This went hand in hand with participants' wanting to know that reasonable efforts had been made to publicise what is happening so that they were aware of how to make the right choices where possible. This was especially so where the private sector was involved. In medical research, for instance, the willingness to support the public interest argument was undercut by a suspicion of the motives behind information use.

The threshold varied according to who was using the records and their motives for doing so. For example, the need for direct control was lower when health professionals were delivering care than when private sector organisations such as insurers or businesses might look for access. One participant summarised her group's view on whether employers should access electronic records: 'a concern is that employers would like to or love to access employee records … obviously that's the grey area. We think it should be at the discretion of each individual as to whether the employer can access their records.'[91]

It was legitimate for these organisations to request access and involve the individual in deciding if that was appropriate. However, it was considered less appropriate for those not providing care or with a commercial motive to be able to trawl data without people's consent. And, as mentioned above, the need for consent was seen as much stronger when medical information was handled by those with commercial motives. Participants were more cautious about pharmaceutical companies using information for medical research, considering that that the ability to consent to this remained essential wherever possible.

Once again, participants identified legitimate uses of information but identified challenges and risks associated with them. And they once again set out the conditions under which the uses of information could be considered acceptable.

Key findings

- Participants identified legitimate justifications for the use of personal information in a medical context: to

deliver more joined-up healthcare and to further research in the public interest.

- Concerns about electronic medical records were largely about ensuring that access remained tied to these intended, legitimate uses.
- Participants felt that largely legitimate uses are only fully acceptable under certain conditions: control and transparency.
- This 'threshold' varied according to the different justifications for use and the motives for pursuing them, with a stronger desire for control and transparency where there were uses by the private sector or those not providing care.

5 Meaningful consent, stronger regulation and transparency

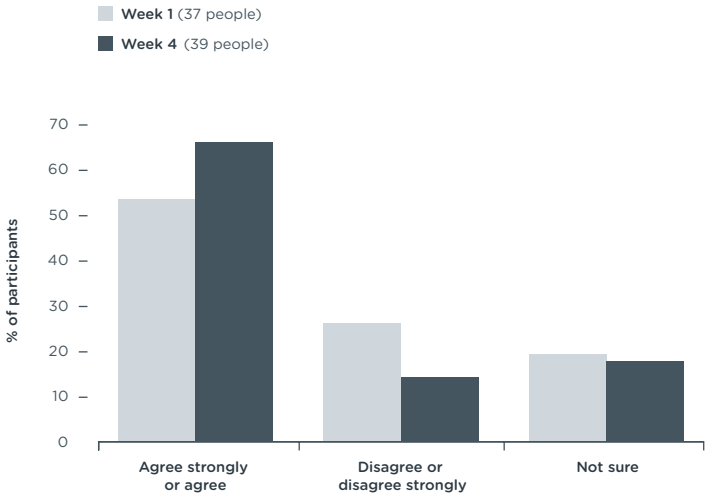
This chapter sets out how participants' attitudes developed over the course of the inquiry, and how through discussing communications data, targeted advertising and the use of medical information, inquiry members took positions on the legitimacy of personal information use and the nature of control over it.

This is partly a story of contrasting attitudes to the public and private sector. We have called the participants' attitudes to the public sector a 'conditional faith', with their relationship to the private sector characterised as a 'wary scepticism'. These attitudes hardened over the course of the inquiry, with participants ultimately considering that meaningful consent, stronger regulation and transparency were required in order to make personal information use more legitimate.

How the inquiry affected attitudes

Over the course of the month-long investigation, participants' attitudes developed in a number of ways. They became more certain through the course of the inquiry about the conditions under which personal information use becomes acceptable, which included: being able to make informed decisions themselves; a faith that organisations would only use the information available for the specified purposes; and transparency about how information is used. Fears about data security, a lack of transparency and function creep contributed to a feeling that people do not have enough control over how information is used. Our survey results show that 23 of the participants disagreed or disagreed strongly at the start of the inquiry that they have enough control over how information about them is used, a feeling that strengthened slightly over the four weeks, rising to 28 of the inquiry members.

Figure 1 **I pay a lot of attention to stories in the press about privacy and personal information (London and Bradford, %)**

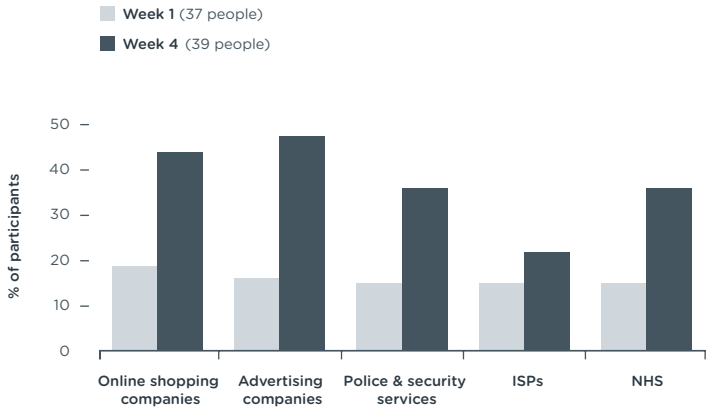


Source: People's Inquiry, London and Bradford

At the same time, there was a disparity revealed in the survey between awareness of the issue of the use of personal information generally and awareness of the specifics of information use. See figures 1 and 2.

Awareness of stories in the press about personal information use was fairly high overall, remaining consistently high in London and rising over the course of the inquiry in Bradford. But awareness of the specifics of data use among inquiry members started off very low. This suggests that participants did not feel that the coverage of privacy issues in the media helped to inform them effectively of how personal information was used and what its use means. That perceived awareness rose significantly over the course of the inquiry. For example, there was an increase from 8 per cent to 36 per cent of participants describing themselves as 'very aware' of information

Figure 2 **How aware are you about the way that your personal information is used by the following organisations? (London and Bradford, % answering 'Very Aware')**



Source: People's Inquiry, London and Bradford

use by ISPs; participants 'very aware' of data use by online shopping companies rose from 19 per cent to 46 per cent; and the number 'very aware' of information use in advertising grew from 21 per cent to 44 per cent. Even so, the number of people describing themselves as 'very aware' was beneath 50 per cent for each of the different uses listed.

It is evident that awareness of privacy issues among participants improved over the month. This was recognised by some of the participants when they reflected on the role of the inquiry itself:

You've seen a lot of the people here have become infinitely more aware or paranoid about their internet usage. Because all of a sudden they're all saying actually "I'm not sure I want to do that now and I'm going to clear my cookies. And I'm going to make sure that there's no tracking cookies on my PC. Because I know now I should press that button." But that's because over the last four weeks whether you pay for it or not this is a bunch of people who've been educated about what is actually happening. And that is a good thing.[92]

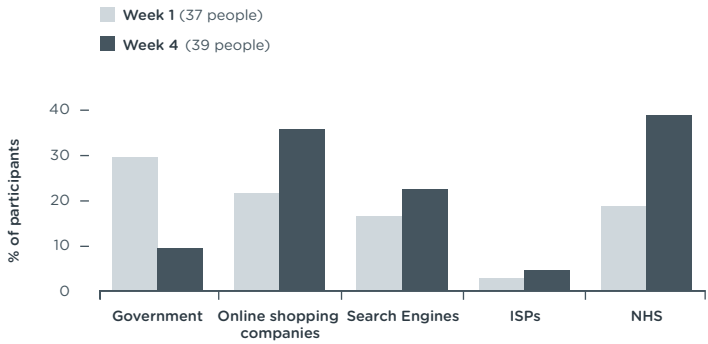
Moreover, inquiry members felt that the process led to them considering the effects of personal information use not only on themselves but also on other people, some of whom they felt could have more pressing reasons to be concerned about information use. This is exemplified by the following quote from London, when one participant expressed how he had come to consider the views of other people who may have something, legitimately, to 'hide':

[Some people might be] saying, "I don't want my medical records available if it means that I'm gonna get hassled because I've got a unique blood group … And I'm constantly going to get hassled to be donating blood." And it's those types of things, where previously I just [didn't consider]… I've ever done anything wrong [and] I'm not worried about anybody seeing what I do on line. I haven't got anything special to do with my [data that] I'm gonna have to worry about. You then realise that people who have something that is different about them, or see the world differently, it's going to be very different for them.[93]

Awareness improved and discussion developed over the inquiry, but this did not make participants start to feel that we have embarked on an inevitable slide towards disempowerment through information use. There was, however, a concern about a lack of awareness among the public, and of a correlative failure on the part of those collecting information to be transparent enough. In this sense, the balance of power, it was felt, was currently weighted towards those who collect information.

But uneasiness about the power of organisations to use information differed across the various contexts studied in the inquiry. There was a greater concern about those with a commercial interest in the use of personal information than about its use by the public sector in the contexts covered in the inquiry. People had more trust in the motives behind public sector use and their intended uses of personal information than in the private sector's motives and potential uses. Our survey of inquiry members tracked the different levels of trust participants had in private and public sector organisations. By the end of the inquiry, the number of people who said that they did not trust

Figure 3 **To what extent do you trust the following organisations to use personal information about you in an acceptable way? (London and Bradford, % answering 'Not At All')**

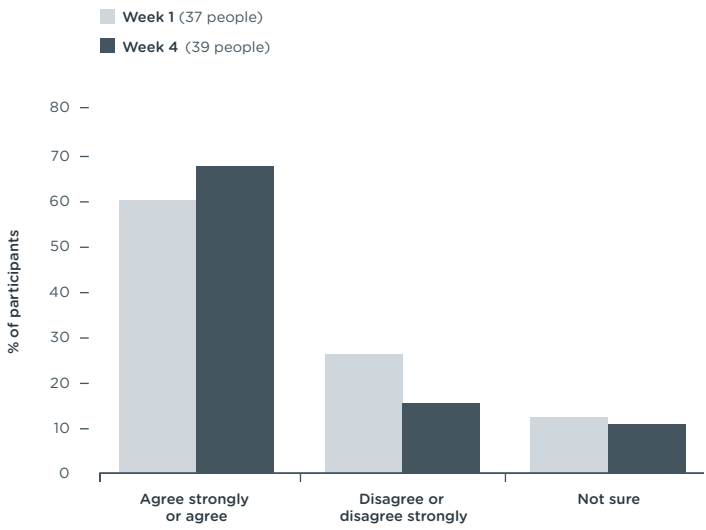


Source: People's Inquiry, London and Bradford

government had dropped by 30 per cent compared to the results at the start. In contrast, those saying that they did not trust ISPs and online shopping companies rose over the four weeks, increasing from 19 per cent to 38 per cent for ISPs and from 22 per cent to 36 per cent for online shopping companies. Trust in the NHS remained strong throughout. See figure 3.

The differing levels of trust people had in public and private sectors were reflected in partipants' perception of a need for a greater level for consent wherever private sector organisations were involved. Participants recognised that in their dealings with the private sector they have to shoulder the responsibility for managing the risks and benefits of sharing information. That meant they wanted an environment to be created in which they could make informed and meaningful decisions. But at the same time, in all contexts, guarding against function creep, human error and insecurity was seen as vital to hold organisations in both public and private sectors to their word. That led participants to call for more meaningful ways to express consent, stronger regulation and greater transparency.

Figure 4 **People understand what they are consenting to when they give permission for their information to be used (London and Bradford, %)**



Source: People's Inquiry, London and Bradford

Meaningful consent

To be considered acceptable under the Data Protection Act, the processing of information has to be fair and lawful.[94] In its guide to data handlers, the Information Commissoner's Office stresses that 'fairness generally requires [users of data] to be transparent – clear and open with individuals about how their information will be used'. They argue that people should have the means to 'make an informed decision' about 'whether to enter into [the] relationship'.[95]

Across all three of the topics the inquiry discussed, the ability to make meaningful choices was seen as important. For example, in the case of access to medical records, people felt that it was crucial that individuals should have the ability to cloak information and take some control over who sees what, given the sensitivities

involved and the fact that different people will be happy with different levels of disclosure. This was summed up by one participant in Bradford:

If you [have] opt-in [for] all the people who are at risk of … [other] people [wanting] to go into their files, then they're the ones that can say, you know "I'm at high risk here. I'm a celebrity or I'm a politician." There are all those people that fit that criteria, they can then opt out. They could say "No I don't want that."

This concern about consent was particularly strong when considering the use of information by the private sector. As one participant in London explained:

I think there's far more problems with the private sector.… I think that this is where the police should be. What the private sector should be allowed to have, how they use it and also make people really aware of when you're giving out information and how much you should give out and know what's going to happen.[96]

For example, in week three, use of records by the NHS was generally endorsed, but it was clear that it was 'not so good that the data the NHS has is available to anybody else.'[97] This was often expressed very bluntly, for example in session three in London:

Female: The benefits definitely outweighed the…
Male: I don't trust the private sector though.

When it came to consumer decisions, participants were often comfortable with private sector organisations' role and the rights the private sector had to use personal information. They saw some of the trade-offs and recognised their own power. But that meant that there was a need for transparency over who was handling personal information and why, and a clear opportunity was needed for individuals to make decisions about whether that use was acceptable. For example, in Bradford one participant agued that 'if you want that content and you're willing to pay for

that content with your personal information, that's a choice only you can make.' Even if it was likely that they would still consent and give information away, doing away with occasions where those conditions of informed choice were not present was seen as extremely important.

But our participants felt that the principles of transparency and control are not being lived up to. Inquiry members were unsatisfied with the kind of choices available to them and the extent of their control over how information about them is used. Our findings suggest that consent or informed choice is sometimes seen as a meaningless procedural event that does not give people the control they expect. There were a number of reasons for this.

There is no real chance to say no

There was a feeling that in reality people are not given the chance to say 'no'. For example, in session one in London, one participant complained that 'sometimes I don't like to give my information [but] I have to because I want something in return. I'm forced to give that information. I'm thinking "God I'm going to have to give this or I can't get what [I want]."'[98] It was often felt that it was inappropriate to make consent to the use of information into part of the terms of a transaction. For example, in session four in London, a participant again emphasised that 'at the moment you haven't got a choice. You normally have to agree or you can't buy what you want to buy.' And while discussing recommendations for action in week four, a group in London stressed that 'at the moment you haven't got a choice. You normally have to agree or you can't buy what you want to buy.'

Excessive collection

It's unbelievable some of the information you have to give over to do certain things these days.

Inquiry member, London[99]

A second problem was the excessive and unnecessary gathering of information. People wondered why organisations needed more information than was necessary for the transaction they were engaged in: 'even for our benefit do they need so much information? Do they?'[100] Participants felt that excess information was asked for because it was useful to the data handlers: 'if you look past it, you think, well they obviously use this information for something, that's why they're asking.'[101]

Awareness

Alongside concerns about excessive collection and problems with consent, participants felt that people are unaware of the reasons for and the consequences of giving away information. In our survey, most participants felt that people do not understand what they are consenting to when they give permission for information to be used. This perception increased slightly over the course of the inquiry, with those disagreeing or disagreeing strongly with the proposition, 'People understand what they are consenting to when they give permission for their information to be used', rising from 59 per cent to 69 per cent. See figure 4.

Part of the fault for this was down to a perceived failure from data handlers to be clear enough, especially with regard to 'third parties'. For example, in London a participant complained:

There needs to be a whole lot more transparency [around] what some of these things actually mean. So when … you sign up for [an online retailer] and [they] say 'you are giving us the right to use your information because you're buying something from us' [it] is fair and reasonable. [But] … then it says '… and anyone we're affiliated with.' Well I want to know who those people are that they're affiliated with.

The 'terms and conditions' associated with exchanges of information were seen as problematic because they do not reveal enough information about what happens to information, and they are hard to understand, so they obscure the real terms of a deal.

Our inquiry participants are not the only ones who have picked up on how problematic privacy statements are as a means

of control. One expert at our roundtables admitted: 'I write these privacy statements and even I don't read them'. Likewise, in an interview with the New York Times the head of the Bureau of Consumer Protection at the Federal Trade Commission, David Vladeck, said: 'I've been practicing law for 33 years. I can't figure out what these consents mean anymore.... I'm not sure that consent really reflects a volitional, knowing act.'[102] When even the lawyers who write privacy statements and those who regulate them say this, the privacy statement ceases to be a legitimate means of regulating information processing. Consumers cannot be expected to become legal experts and it is beyond the limits of our education system to breed a society of mini-lawyers.

Our findings suggest that the conditions for informed choice are currently absent. And further, even where choices do reflect a 'knowing, volitional act', our participants felt that they had little effect on organisations' behaviour.

Stronger regulation

The aspirations behind data use were often seen as worthy, but the problems of third parties, insecurity and human fallibility helped to undermine the belief that personal information use was always legitimate.

Conditional faith in the public sector

In the case of communications data, people had a strong faith in the institutions that use personal information through the RIPA Act. There were often very high levels of trust in the institutions of the public sector that use personal information, including in the organisations' aspiration to enhance security, for example, or improve health care, and in their ambitions to use personal information to do so. As one participant summed up well, 'you have to ... you've got to trust the government, because they're there to be trusted.'[103]

However, we label the attitudes to the public sector expressed throughout the inquiry as 'conditional faith'. Participants did feel that there are limits to the circumstances in

which the public interest argument holds. This was demonstrated in the debate about function creep, communications data and copyright. Concerns were also raised about future governments being less trustworthy, suggesting that this faith is conditional on the perception of the government. One participant in the second week, in a conversation about communications data use for security, used the example of a possible shift away from electoral cycles between centre-left and centre-right governments:

It also depends on who's in government. In this country at the moment we sort of flip between kind of having, centre left and centre right. If, for instance, next the BNP got in, all of a sudden, all this information is like: oh hang on we can't let them have it, because it's really now sensitive … all of a sudden now.[104]

People mainly feared, however, that data insecurity will mean that information will not be used in the intended ways. This applied as much to the private sector as the public. While participants wanted more meaningful consent in their dealings with the private sector, they also recognised that consent by itself was insufficient and that regulation was needed to guarantee that information was used appropriately. Participants recognised that more was needed to make sure data handlers were always held to their word.

Holding data handlers to their word

The two primary concerns for security related to 'third parties' and the problems of 'human error'. These concerns were not seen as trivial but as fundamental problems, as challenges that would be difficult to eradicate and could undermine the validity of the aspirations themselves.

Third parties and the wrong hands

The terms 'third parties' and the 'getting into the wrong hands' were scattered across the discussions. There was very clear sense

that information was, at the moment, almost destined to end up where it was not supposed to be, through insecurity or fallibility: 'the cynical part of me says it doesn't matter whether you tick the box.' This was notable in the discussion regarding the privacy statement of an online retailer, read out in session one. The clause on 'affiliates' was seized upon as problematic: '[Online retailer] and its affiliates, that's what I didn't like. I thought … okay it's only one company I've got that agreement with, one company.'

Human beings

At the same time, a contributing factor in that concern was a constant recognition that human beings make mistakes, that they can be corrupt, and that they can be criminal. As much as the discussion was ostensibly about technology and policy, there were constant references to being realistic about human beings. This was not a case of being overly pessimistic, but realistic, as summed up by one participant in session two in London: 'there are competent and incompetent people in every walk of life. There are honest and dishonest people in every walk of life.'[105] There was a concern running through the inquiry that organisations would either find it difficult to eradicate misuse entirely however much they tried, or that they were not trying hard enough anyway:

And that I think is a big issue – is the extent to which the organisations which have personal data limit the facility to download it onto memory sticks or in any other way for it to be used by dissatisfied employees and parting employees in competitive organisations.[106]

The faith that inquiry members had in the use of personal information was based on their belief in the degree of realism in the aspiration that information would be used only as intended. But participants also felt that information use had to be appropriately transparent.

Transparency and data pragmatism

But it all makes assumptions. The assumption is that this data is only available to the people that it's targeted at – the police, the emergency services, the NHS, whatever. If that was 100 per cent true you don't have any arguments about it.

Session 1, London

Our participants did not define 'personal information' by listing categories of information. Instead, they focused on its possible uses. In this respect, the inquiry members were, in the main, data pragmatists. As one participant described, 'that's like the fundamental point or the focal point … how the information is used.' That helps to explain why transparency was seen as a fundamental concern, as participants looked to have the means to make informed decisions.

There were references to bodily privacy and to ownership of information; for example, 'it's my property; it's me, my body, my details',[107] and 'you don't just come and use my car'.[108] However, the explanation behind that sense of ownership was never far away:

What if it's political or sexually orientated let's say, or the subject matter is a little bit, you know … areas that people might be slightly sensitive to … it could create a whole profile about you that may be would have an effect if it's sold on to certain companies, certain bodies.[109]

In all groups in week one of the inquiry, discussion developed from discussion of *types* of information, to its *use*: 'anything that you could expect [to be used] in a negative way, you know if someone got hold of it.'[110] Often this discussion included such references to gateway information that 'can be used to find out even more about you than maybe ought to be known or it could be used to set up an identity in your name to abuse.'[111] Another participant in Bradford, similarly, stressed that 'I don't mind you knowing who I am … [but] I don't want you to know who I am, where I am, what I do.'[112] Perhaps the attitude towards what 'personal information' meant to participants is summed up best by the following exchange from session one in London:

Male: *All that information under a definition is personal because it's personal to you. But it's how that is used or abused depending on the company or the corporation that are using that information. That's where the damage or the danger is.*

Female: *So there's two sides…one's a criminal element and one's probably an authority element.*

As we saw in the case of communications data, the use of information is context-specific. RIPA was seen as acceptable so long as policy worked in practice as it was intended. But this did not necessarily mean participants found the use of the same information in other contexts legitimate, as the disagreements about copyright enforcement showed.

However, a lack of awareness, both of the specifics of the way information is used in practice and of its tangible effects, meant that it was hard for participants to gauge how serious the risks really were, or how they would affect people in a concrete way. That meant that data insecurity, for instance, was seen as a risk in and of itself, while it was harder to say what its consequences could be. For example, in Bradford, in a discussion about the legislation covering access to communications data, one participant said that 'I don't know how they can use it against anything, they can't use that information. It's mostly for … criminal-type people.'[113]

It was clear that participants were not running scared of the information society, but equally that they certainly cared about how their personal information was used. They were quick to draw limits and boundaries to its use. But despite having felt that their own awareness rose over the course of the inquiry, participants still felt that a lack of transparency meant that they were denied the chance to be fully informed data pragmatists.

It could be that the lack of awareness itself was partly responsible for participants' fears, which were often opaque or intangible in nature. One participant in Bradford expressed this connection well: 'there's a lot of unknowns, aren't there. People are making decisions about what they perceive as acceptable…. So the … actual truth about the information that they're using is so far out of our control.'

Transparency, the option of control and strong oversight were felt to be crucial components of legitimate information use – and in the final week of the inquiry, participants turned their attention to these issues.

6 The inquiry's 'calls to action'

Everyone's sort of coming to terms with it.
Session 4, London

In the final week of the inquiry, we asked participants to discuss how to address some of the issues that they had identified in the previous three weeks. To help with this, we welcomed Stephen McCartney from the Information Commissioner's Office and Lizzie Coles-Kemp, from Royal Holloway University.

Participants emerged from their discussions with 42 practical demands. In this chapter, we outline these 'calls to action'. Transparency, strong regulation and improved conditions for consent feature heavily. As discussed in the previous chapter, it was considered important to give individuals meaningful rights to consent, which means offering them responsibility for how their information is used. But there was a feeling that the responsibility to manage the information world cannot be borne by individuals alone, even if they are fully informed. In the eyes of participants, this conferred responsibilities on the institutions that handle data, on regulators and government who set and enforce the rules for its use, and on the businesses that exploit it.

The calls to action spoke directly to this desire for more meaningful consent and stronger regulation. They betray a concern for basic principles that participants felt are currently not being lived up to. These were principles on which they felt the acceptability of personal information use rests: that people should be able to make informed choices and that regulation should ensure that organisations are held to their word through appropriate regulation and good practice. To reflect this, we have grouped the calls to action into two sections in this chapter. First, we discuss those calls to action that deal with establishing

conditions under which people can make informed choices, and secondly, we look at those designed to hold organisations to their word. We outline a number of the recommendations that fall under these categories, before setting out the discussions that led to them. The full list of recommendations can be found in appendix B.

Making informed choice meaningful

Every day, people have to navigate choices about when and where to share information about themselves. To help make people's choices to give away information more meaningful, participants identified responsibilities for government, public bodies and businesses to raise awareness and transparency.

Responsibilities for government and regulators

- Online information: awareness raising and educating people – teachers and students – through, for example, a smart Health and Safety campaign (London)
- Medical research: confirmation when time-specific opting-in is given (London)
- Targeted adverts: kite-marking for ads – and more information on who companies share information with (like a traffic light system) (Bradford)
- Regulators providing a list of the top 100 'named and shamed' organisations (Bradford)
- Levels of access for medical information (Bradford)
- Education on the safe use of social networks – for young people and parents (Bradford)
- Medical records 'coming of age' consent request (Bradford)
- Medical research opt-out (Bradford)
- Medical records: more information provided when letters are sent – clearly defining who, what, where in lay terms (like the FSA key facts) (Bradford)
- Medical records: a booklet to say where you want your information to go (Bradford)

- A full information campaign for the medical records programme (Bradford)
- Medical records: doctors telling you before using information (Bradford)

Tackling low awareness of the value of personal information and its possible uses was seen as an important task. The government was seen as having an important role in this area. Participants identified space for 'campaigns like you get with health.' Young people were seen as particularly vulnerable, given their propensity to share information and the various peer pressures they are under to do so. Inquiry members also suggested an approach for the personal information environment similar to the one taken in teaching young people about other environmental risks such as road safety. In doing so, inquiry members were keen to dispel any presumptions that young people have any particular wisdom when it comes to the internet– there was a feeling that they may know the technology but, in the words of one participant, 'we have lived a bit longer'.

As well as raising awareness generally, people saw a role for government in enhancing the transparency of information use in people's everyday decisions making. The clearest call to action in this regard was for a kite-marking system through which regulators could signal good and bad practice, with a 'traffic light system' identified as one possibility. People felt that the Food Standards Agency's hygiene rating system could serve as a useful model here, helping people make better consumer decisions through simple messages about how trustworthy particular organisations were. Participants in Bradford considered the possibility that regulators could publish a 'name and shame' list identifying the top 100 organisations who have mishandled data.

There were similar responses in the context of medical records. To alleviate concerns that letter writing would not be enough to raise awareness to a level that would satisfy participants that the 'opt-out' model was sufficient, one solution was to 'do something similar to … the digital switchover with TV, [and] fully advertise this on all … media channels … that this

process is happening, everyone has to be involved and it's going to be the future and the way forward.'[114] As with the other areas, the importance of being kept aware of what was happening was seen to be crucial, signified by the calls for a booklet that explains clearly the details of personal medical records use, but also gives people an opportunity to specify more easily with whom they want information to be shared.

These recommendations were designed to put more emphasis on explaining clearly exactly what will happen to the records, as one participant explained:

Rather than just a letter [the information should]…clearly define who, what, where this information goes, explained in layman's terms…similar to the key facts that [the] financial governing body has.

There were calls to communicate more effectively with young people, in order to give them a very clear opportunity to exercise control. One idea was for a 'coming of age' moment when young people would be given the chance to consent to the use of medical records, with the idea that 'the question should be asked when their national insurance number comes, "Now you could control your own medical records. Do you want to do that, or don't you?"'

Responsibilities for businesses

Participants felt a number of responsibilities rested on businesses using personal information, covering both awareness raising and the provision of tools for control.

1 Clear forms on use of information, with companies specifying who the third-parties are (London)
2 Targeted adverts: standard, clear consent forms and privacy policies (Bradford)

Clarity and raising awareness

Whilst government and regulators were seen as key in raising awareness of the broader issues of personal information,

businesses were also identified as having a role to play. It was recognised that business and government bring with them complementary brand associations. Government involvement signifies that the matter is serious and that there is 'someone to answer to', whilst businesses might have greater 'credibility'. As one participant said, internet businesses would have 'the credibility … to produce media campaigns' and that they would 'therefore [benefit] from advertising from sponsoring some sort of vision.' Many felt that this would require encouragement or intervention from government. One participant summed this up neatly with an analogy: 'the cigarette companies don't volunteer to print "this is going to kill you" on the back of your fag packet.'[115]

To combat a sense that the information use that happens after a transaction is hidden from view, and that this leads to unknown third parties handling data, participants identified a need for some form of clear and standard explanation of subsequent information sharing. As one participant explained, businesses should make a commitment, saying 'we will make this as transparent and as available to you as we physically can. And we will issue directives to say that's what should – your Ts and Cs should look like.'[116] The notion of a standardised consent form was given as a specific call to action in this context: 'when you're agreeing to all that stuff, you want a standardised consent form across it all.'

Providing tools for control

1 Targeted advertising: opt-out for junk mail online (London)
2 Targeted advertising: people's own information profile which they control – deciding who sees what (London)
3 More meaningful control over what information you choose to give (on a one-time basis) (Bradford)
4 Opt-in for marketing (Bradford)
5 Express consent for retaining bank and sensitive information (Bradford)
6 The ability to opt-out in future (Bradford)
7 No DPI (deep packet inspection) without consent (Bradford)

There was a cluster of recommendations calling for more meaningful control over what information goes where. This included making the ability to opt out clearer and confirmation of the minimum amount of information needed for a transaction, so that 'you can click on a website and it comes up and says "to go on this website … this is the minimum that we need: your name and your email address."'[117] This led to a series of quite strict demands, involving being able to visit sites anonymously ('if you say "Oh, no I don't want to give anything"') and having websites confirm what they hold about you when you revisit them: 'something would pop up and say "the last time you visited you chose to give us this information. Is that still okay?"' At the same time, there was a feeling that people should be able to withdraw consent – that 'once you've given it, it doesn't mean [they] get it forever.'[118]

With reference to the discussion from week two, certain forms of targeting were seen to give people less opportunity for control. They were seen to deny people the chance to give consent: 'you've got absolutely no control over your deep packet inspection. If your ISP wants to do that, they are going to do it regardless. So we don't want that to be a possibility.' [119] The call to action was the ability to give express consent to 'deep packet inspection' – the form of targeted advertising mentioned in their discussions as the most worrying, because it involved the 'reading' of content without their consent. The intention is that without that consent, companies 'wouldn't then be able to do the deep packet inspection'.[120]

These calls focused on having an influence over the way that organisations can use information they hold about people, and how transactions involve giving away information. There was a call for a more direct form of control over these through a 'personal information profile' managed by individuals themselves. The idea was to give people a greater direct say over who sees what, and equally to ensure information is accurate. The group described this as meaning that:

Each individual would have their own separate information profile that you were responsible for updating … You choose what information on that profile

you give to whoever you are doing business with … You can select that information on your profile that is shared with other people, third parties and for advertising.

Make the regulation strong enough

Ensuring the conditions were right for people to make informed decisions was seen as essential. Transparency and individual consent were considered necessary to help to ensure data is used as it is intended to be. But the consumer consent model, of individuals being the masters of their information, was not enough. There were requirements for stronger guarantees about the security of information and safeguards against future or unforeseen harms.

Responsibilities for government and regulators

1 Tougher penalties for misuse of information (London)
2 Temporary staff only allowed to access relevant information (London)
3 Regulation for online information needs to be up to date (London)
4 Information Commissioner's Office should introduce tiered fines for misuse of information (Bradford)
5 Information Commissioner's Office should have the power to perform an unannounced audit (Bradford)
6 Regulators must listen to public concerns (Bradford)
7 Regulator should be neutral (Bradford)
8 'Tidying up' the regulation bracket – making sure that the regulators (the ICO, etc) can regulate (Bradford)
9 Regulation for medical records access by pharmaceutical companies (Bradford)
10 Auditing for medical information use (Bradford)

There were clear demands to prevent unnecessary data sharing through mistakes or corruption by using tougher deterrents for misuse. And there was a sense that this should be

about repercussions for individuals as much as for the organisation involved. Participants referenced the NHS Care Record Guarantee in this respect:

At the end of the NHS care guarantee, which I appreciate is [not quite the same], [it says that] if we find someone's deliberately accessed records without the permission [then it involves] ending a contract, firing an employee. That's the only way really – or bringing criminal charges.[121]

The second concern was that there would be points of vulnerability that opened up access to people who did not have a significant investment in keeping the information safe and within certain boundaries. This led to a call for 'multiple levels of authority for information being shared or released,' which would mean, for example, that 'temporary contract staff only to get access to information required for them to do their job.'

This genre of recommendation set quite strong calls for regulators. One participant referred to the necessary oversight as 'intelligent regulation', covering the problem of rapid change and the need for the regulation to keep pace by constantly reviewing its approach. One example of this came in looking at the remit of regulatory bodies, which were called on to 'clarify who is subject to the law in the UK', and clarify the regulation jurisdiction, since participants considered that 'it shouldn't just be about having an office here.' Participants felt that there was a need to extend jurisdiction over those organisations that clearly have a role in the use of personal information in the UK but who may not, in the participants' eyes, have been subject to UK regulation. One idea was to create a business case by revealing those who do and do not fall under certain jurisdictions:

Because obviously, you can't force a company to come in, but what you can do is say 'Look, these companies have a base in Britain. They are regulated and fall under the jurisdiction. Therefore, there's an implicit benefit to using those over competitors.' So you create a business case for Facebook to have a base here and fall under [the UK data protection regime].[122]

In the case of medical records, the most pressing calls involved regulating access by pharmaceutical companies and others with a commercial interest and to help with this, participants called for the auditing of medical information use.

Responsibilities for businesses

1 Mandatory code of practice for targeted advertising with penalties for misuse (London)
2 Compensation for consumers whose information is sold on (London)
3 Independent oversight for targeted advertising (Bradford)
4 Greater oversight for viral marketing (Bradford)

Participants identified some duties on businesses to improve the regulation of the use of personal information, including working with regulators to create an environment of independent oversight.

Inquiry members felt that it would be unwise to continue to let advertising online be completely self-regulatory, exemplified by the conclusion that 'we've all accepted that we can't expect the companies to police themselves because that won't work.'[123] For this reason, participants thought that there should be 'an enforceable code of practice' which was down to 'an external body', an 'ombudsman', 'or even down to the ICO or the government' to police.[124] This required both 'strong guidelines and strong powers', with the 'code of practice' backed up by 'really strong repercussions if you break the guidelines.'[125] This related closely to a call for an independent body to review methods of online marketing and to approve or deny them. So, for instance, 'if companies want to bring deep packet inspection in, a completely independent body would look at that and see if that is acceptable or not.'

Participants further recommended that where these regulations were transgressed in ways that harmed individuals, those consumers should be compensated: 'if we've been forced to tick a box and agree terms and conditions and then the

information gets [misused] ... Then there should be some form of compensation.'

Finally, a concern for viral marketing led people to consider the need for more oversight. This related back to a worry that people would be unaware that advertising was happening, and would not be conversant with the sophistication of various forms of targeting. For example, one participant argued that often:

You don't know if the company who offers that product has put a review on there. Or if the person who reviewed it; you don't know if they're real or not or you don't know if they're viral advertisements. Sometimes you don't even realise it's a viral advertisement whatsoever.

Responsible governing

1 Validating age of users (London)
2 Clearing up the age of consent for online networks (London)
3 Online information: An internet passport (London)
4 Tighter regulation for young people on social networks (Bradford)
5 Social networks: prompts to 'tidy up' information (Bradford)

There were further calls for regulators to take on some of the responsibilities participants felt they had related to social networks and also with regard to targeted advertising. People felt that businesses had a duty to combat the problem of children who are too young accessing social network sites. And in highlighting this option participants again referenced the fact that it is unlikely businesses alone will take action:

Male 1: I don't know if you remember seeing in the voluntary code of conduct ... put out by advertisers ... whether they say in their voluntary code of conduct, 'We will not market to minors.'
Male 2: Rubbish.[126]

This was not a responsibility seen as applying only to online businesses. It stretched across parents, teachers, and

government. Concern about young people using social networks was clear but mechanisms to enforce age restrictions were not. The discussion recognised the appeal of social networks and the peer pressure to use them on young people themselves. One participant said, 'My daughter [is] eight and she actually came back she said "Mum, can I set myself up on Facebook because all my friends are on it."'[127] Technical solutions, boundary setting and good parenting were mentioned as important ways of tackling the problem.

Calls to action included a need to clarify the age of consent on social networks and instituting a consistent policy for trying to enforce it. Further, some form of passport or pincode was suggested, which might be able to regulate more easily what young people were exposed to. There was disagreement about how realistic this recommendation was, centred on how it would work in practice, with some thinking that this type of solution throws open a 'quagmire of issues and problems'. Participants were aware of the risks of an arms race of authentication. Similarly, many recognised the risk of being overly protective and felt that these problems were more about good parenting and allowing young people an appropriate amount of freedom.

There was an awareness of the trade-offs of making people prove their age – that it might require websites to know potentially more revealing and personal information than otherwise. One participant summed this up well by describing it as 'the epitome of a catch 22 situation', asking 'do you want [a social network site] to have the rights to validate the information? Which means they've then got access into a full set of records? Because I don't ... I'd rather somebody lied.'[128]

Lastly, there was a call for those who handle online data, and most specifically for social networks, to provide more ways for people to 'clean up' the information held about them through prompts and tools to manage information.

Controlling information

Over a decade ago, Perri 6 argued that privacy can be seen as 'protection against certain kinds of risk'. He categorised these as

'risks of injustice through such things as unfair inference, risks of loss of control over personal information, and risks of indignity through exposure and embarrassment.'[129] These risks resonated throughout the discussions of our inquiry, with participants identifying harms related to identity fraud, profiling, stigmatising and vulnerability.

Twelve years on, our participants have demonstrated that Perri 6's risks are still live, but that the evolving methods for gathering and using personal information require, in practice, a focus on the principles of awareness, consent and firm regulation.

Conclusion: Democratising the database society

In February 2010, Google launched its social network, Buzz. By basing Buzz in its existing Gmail service, users were able to easily follow and be followed by those in their Gmail contact list. But it led to criticisms that people might be unwittingly sharing information they had previously considered private, and that it was difficult to understand how to manage connections with other Buzz users. US privacy group EPIC filed a complaint with the Federal Trade Commission, claiming that Buzz 'violated user expectations, diminished user privacy, contradicted Google's privacy policy, and may have violated federal wiretap laws.'[130] The company apologised for any mistakes and any harm caused. They also pointed to the consent required to turn Buzz on and the ability provided to turn it off again. And Google's Chief Executive Eric Schmidt argued that the problem was one of communication, saying Google 'did not understand how to communicate Google Buzz and its privacy. There was a lot of confusion when it came out…'[131] The Buzz case exemplifies some of the challenges identified in the people's inquiry.

The desire for transparency and the meaningful capacity to choose shows that the use of personal information becomes problematic, and is seen to involve a problematic transfer of power, where it is used by others either in ways that are unknown to the people that it affects or that deny them a chance to accept or reject it. Our participants were data pragmatists to the extent that they considered information personal wherever there was a perceived harm. That included cases where the consequences were unknown or opaque. Transparency was important not just to improve consent but also to alleviate fears of the unknown.

The presence of transparency and the ability to make informed choices were the conditions under which participants accepted personal information use. The members of this People's

Inquiry into Personal Information have sent a clear message about the best way to take advantage of the benefits of personal information use at the same time as dealing with significant uncertainty about the potential risks involved. They wanted an emphasis on transparency, the capacity to control and mitigate for possible and sometimes unforeseen harms, coupled with more guarantees about security. Our findings suggest that organisations should presume that people want the means to make informed decisions, based on clear and easily understood information about the consequences, about when information about them is shared and how it is used.

The participants' demands are largely for the robust applications of existing principles of data protection. For example, the recent submission from the Article 29 Working Party to the European Commission's consultation on 'the legal framework for the fundamental right to protection of personal data' also advocates a focus on consent and transparency. First, regarding consent, they argue that 'confusion between opt-in and opt-out should be avoided, as well as the use of consent in situations where it is not the appropriate legal basis.' Second, they argue that transparency 'does not necessarily lead to consent but is a pre-condition for a valid consent and the exercise of the rights of the data subject'.[132] The need for transparency from all data handlers is echoed in the ICO guidance on 'fair' processing.

The findings have a number of implications for decisions about how to govern the database society. Firstly, it is time to take the need for greater clarity and transparency seriously. One example would be the relationship between pubic and private sector. The inquiry did not cover the extent to which public and private sectors overlap in practice. But the attitudes to the two, dependent as they were on perceptions of motive, suggests that there is a need to clarify the relationship between government and private sector in the context of personal information use, especially where data handling is undertaken by the private sector on behalf of a public sector body. Not doing so puts at risk the faith people place in the public sector's motives and undermines their ability to decide whether information use is acceptable.

This means being clear about contractual relationships where the private sector is carrying out personal information processing, and it extends to many areas in which public and private overlap, for instance in the case of personal medical records. We did not cover the question of alternative providers for electronic medical records explicitly, but the findings on control and consent suggest that providing access to the private sector in this context should be based on an explicit choice by the patient for those organisations to have access to the records.

The findings also suggest that some of the tools already at our disposal will have an important role to play in helping people control their data. In the commercial sphere, emerging business models that provide people with easier ways to manage their information use directly, such as MyDex and the identity solutions provided by companies like Garlik, will have an important part to play in future personal data management.

Finally, there is a need to keep up to date with how the developing methods for learning about people and their behaviour affects them individually and collectively. That means constantly reviewing methods of personal information use and conducting practical examinations of the benefits, risks and effects. This sets a challenge both for policy makers developing policy for the public sector and for those in the private sector communicating their information use: it is necessary to be clear about the link between information use and the aspirations behind it.

But at the same time, this sets a challenge for privacy advocates and researchers to maintain a solid and clear evidence base of the tangible risks and harms, and in practice, whom they will affect and in what situations. This will help provide evidence of the degree to which principles of privacy are undermined and give a greater weight to arguments for intervention. An up-to-date and clear topology of risk for personal information use would help inform people of the consequences of giving away information and make it easier for policy makers to understand the need for privacy interventions.

Democracy and personal information

Participants believed that there are appropriate ways to use information and they wanted better ways to have a say in what they are. The availability of personal information will only increase, as will the sophistication of the methods used to utilise and analyse it. What is open to question is the extent to which people retain an individual or collective ability to determine its effects. The best defence against the inappropriate use of personal information and the harms associated with it is to make the use of personal information as democratic as possible. That requires a solid governance framework, including giving people the means to make meaningful, informed decisions about when and where to release information when it is in their power to do so. There are many situations in which people will have to shoulder the responsibility to manage the database society themselves. But ensuring people have a hand in their database fates also means recognising the *limits* of people's individual control.

This report offers one way to include public attitudes in the debates about personal information. There are many other opportunities for this. For example, there are tools such as Privacy Impact Assessments (PIA) and Privacy by Design that can help to build privacy thinking into projects from their inception. Of equal importance in using these is recognising what constitutes legitimate use and where in practice people want the boundaries of legitimate use enforced. Involving the public in those substantive questions of legitimacy will help to make sure that the privacy built into projects and research reflects an understanding of the attitudes of those it affects.

Further, there is a welcome vigour behind the drive to release to the public more data held by government. In many cases, the information will not be personal. But this new drive towards releasing public information needs reconciling with privacy concerns. One suggestion to help address this would be an independent board, similar to the National Information Governance Board developed to provide oversight of the use of medical information for research, that could take decisions about the release of information that might be either unintentionally identifiable or have potential adverse privacy consequences.

'Democratising' the collective effects of personal information use is an imperative in the information age. As radical as the demand that principles of transparency and informed choice are taken seriously is the demand that we find better ways to listen to the people that personal information use affects. There is no one way to achieve this. People's inquiries cannot claim to provide the only solution. And one people's inquiry cannot claim to provide the answers by itself. But deliberative methodologies can be part of the solution by revealing informed attitudes and by connecting people more directly with decision making. The results of this project are an example of how useful they can be in involving people more directly in the debate about power and governance in the database society.

Appendix A: How the inquiry worked

The methodology at the heart of this project draws on two parallel streams of work. The first is the recent history of public engagement in technology and science. In looking to address these problems, Demos has had a strong presence in the debate to open up science and technology to public engagement. In the 2004 pamphlet, *See Through Science,* James Wilsdon and Rebecca Willis argued that public engagement in science needed to move 'upstream', allowing the voices of the public to shape the questions that drive scientific enquiry. Scientific and technological innovations can challenge established values or beliefs – for example, should the use of foetal stem cells be permitted where they might lead to significant enhancements in treatments for serious illnesses? Where this is the case, science is 'giving rise to distinct sets of ethical and social dilemmas.'[133]

Public engagement plays a role here in submitting these questions and challenges to public scrutiny. A recent example of the application of this ethical thinking in the context of technological research is the EPSRC's Digital Economy programme. The programme has an Ethics Advisory Panel examining the appropriate way to reconcile cutting-edge research with the ethical questions it poses.

The second stream of work informing this project concerns deliberative democracy, the theory of which has been developing for some time. In its application, it has become a means to the end of involving people in the governance of science and technology. Demos's *Nanodialogues*, for example, reports on a series of experiments connecting the public with the debates around nanotechnology, an emerging area of science with potentially far-reaching applications.[134] Similarly, in 2008, BMRB, with research supported by Demos and sponsored by the research councils, undertook public engagement research into

stem cell research. Running across four cities, with 50 people in each city meeting three times, the aim was to use the findings from a large public dialogue to help guide funding decisions on stem cell research by understanding more about people's attitudes to the ethical challenges of the science.[135]

The value of such deliberative engagement projects comes from appreciating that people's views are not expressions of innate attitudes but are formed in context. This is their key contribution to the governance of technology and science. The way people learn about a topic affects their attitudes to it. So, deliberative methodologies look to create the conditions under which informed conversations can take place. The results do not give a snapshot of 'public opinion' in a singular sense, or of representative positions of particular groups. The principle is not that the participants are the same as the rest of the population, but that they are different because of the deliberation. In that respect, they provide nuanced pictures that should inform and guide policy makers and researchers in ways that simple polling or focus groups do not. They offer an example of how to understand and then listen to people's informed attitudes and opinions, developed through more in-depth engagement with the issues.

Setting up the inquiry

We assembled the inquiry with the intention of exploring people's attitudes to personal information through a robust deliberative methodology. That involved inviting the same participants to return for each of the four weeks and ensuring that their involvement developed over the month from reflection to deliberation to decision making. Each group of 20 participants was split into three smaller groups. The 20 were together for expert presentations and feedback at the end of each week, and in the smaller groups for the deliberation.

The two groups ran in London and Bradford, running between 21 October and 14 November 2009. The venues were chosen to give a geographic spread, but the locations were based on the findings of OFCOM's report 'The Communications

Market 2009: Nations & Regions – England', with London having the joint highest Internet take-up at 79 per cent and Bradford having joint lowest internet take-up, at 60 per cent.[136]

A deliberative process such as this people's inquiry cannot try to reflect every position and opinion or be representative of the population. We made certain decisions about the make-up of the groups to get a spread of backgrounds and attitudes and in order to be transparent about the make-up of the groups. This provides space to speculate how alternative opinions and ideas may have changed the shape of the inquiry and altered the outcomes. We used Criteria to recruit participants of a range of socio-economic backgrounds and within the age range 18–50.

How the inquiry worked

The groups ran for four weeks, meeting once a week with each meeting lasting 3 ¼ hours.

In week one we ensured that there was time for initial reflection and discussion of the broad topic, facilitated by researchers from Demos. In advance of the following weeks, we handed out informative material that consisted of short take-home extracts from news stories covering the relevant topic. In the second week, we set more tasks for the participants, asking them to begin manage conversations themselves by taking on the running of the groups. Over weeks three and four participants took on more of the responsibility for handling the discussion themselves. This involved electing a chairperson from the group who was responsible for managing the conversation, note-taking and feeding back results at the end of the session. The Demos researchers receded to the role of helper, offering research assistance if desired and time-keeping where helpful. In the final week, participants took time deciding on their recommendations, having to take decisions about the action necessary to address the problems they had identified over their previous discussions. These 'calls to action' are summarised in chapter 6 and listed in full in appendix B.

To help to inform the groups we invited a series of experts to offer short introductions. Experts were asked to speak for

5–10 minutes; to set out their topic clearly and for a non-expert audience; and to be clear where they were presenting their opinion and where they were outlining policy, practice or others' attitudes. They were also asked to stay around for the smaller group discussions in order to answer any follow-up questions participants may have had.

Participants were asked to complete a survey at the start of the inquiry and again at the very end. The purpose was to track the change in participants' attitudes to the organisations that use information and to their awareness of the issues under consideration.

Following the inquiry, Demos hosted three expert round-tables, at which initial findings from the deliberation were presented and discussed. The aim was to understand experts' reaction to the inquiry participants' views. The list of experts who attended the roundtables can be found in appendix C.

How we used the results

Following the inquiry we used 'grounded theory' to analyse the results. This involved reviewing transcripts from the inquiry discussions and pulling out 'codes' or themes. These were refined and tested by repeatedly returning to the transcripts, each time refining the coding and testing the analysis. The aim was to reflect the voices of the inquiry members as clearly as possible. We recognise that there may be more to draw from the raw material, different themes to pick out and value in checking the validity of our conclusions. In the interests of open research, therefore, the anonymised transcripts from the inquiry will also be available for download from the Demos website.[13]

Appendix B: The calls to action in full

From London

1 Regulators: tougher penalties for the misuse of information
2 Regulators: temporary staff should only have access to relevant information
3 Targeted advertising: a mandatory code of Practice with penalties for the misuse of information
4 Targeted advertising: people's own information profile which they control, deciding who sees what
5 Targeted advertising: an opt-out for junk mail online
6 Online information: a clear, standard form for the use of online information, with companies specifying who third parties are
7 Online information: compensation for consumers whose information is sold on
8 Online information: validate the age of users online
9 Online information: clarify the age of consent for online networks
10 Online information: awareness raising and education for teachers, parents and students – for example through a smart Health and Safety style campaign
11 Online information: an internet passport or pincode
12 Online information: keep regulation up to date
13 Medical records: more information should be provided when letters are sent, clearly defining who, what, where in lay terms (like the FSA key facts)
14 Medical records: a booklet to help you say where you want your information to go
15 Medical records: a full information campaign
16 Medical records: confirmation when time-specific opt-in is given by the patient

17 Medical records: tt should be easy to access and check your own records
18 Medical records: doctors telling individuals first about test results

From Bradford

1 Targeted advertising: clearer opt-out
2 Targeted advertising: standard, clear consent forms or privacy policies
3 Targeted advertising: kite-marking for advertising and more information on who companies share it with, for example through a traffic light system
4 Targeted advertising: opt-in for marketing
5 Targeted advertising: no deep packet inspection without consent
6 Targeted advertising: independent oversight for targeted advertising
7 Targeted advertising: greater oversight for viral marketing
8 Online information: more meaningful control over what information individuals choose to give
9 Online information: ability to opt out in future
10 Online information: prompts to 'tidy up' information online
11 Online information: tighter regulation for young people on social networks
12 Online information: education on the safe use of social networks – for young people and parents
13 Online information: express consent for retaining bank and other sensitive information
14 Regulators: regulators must listen to public concerns
15 Regulators: regulator should be neutral
16 Regulators: regulators should have a 'top 100 named and shamed' list
17 Regulators: the Information Commissioner's Office (ICO) should be able to administer tiered fines
18 Regulators: the ICO should have powers of unannounced audit

19 Regulators: ‘tidying up’ the regulation bracket and who falls under regulators’ jurisdictions – to make sure that the regulators can regulate
20 Medical records: levels of access for medical information
21 Medical records: medical research opt-out
22 Medical records: auditing for medical information use
23 Medical records: medical records ‘coming of age’ consent request
24 Medical records: the ICO should regulate medical records

Appendix C: Attendees of the expert roundtables

Roundtable 1: The use of communications data, 14 January 2010

Paul Wilson	De La Rue
John Leach	John Leach Information Security
Martin Hoskins	T-Mobile
Ian Brown	Oxford Internet Institute
Philip Virgo	EURIM
Stephen Deadman	Vodafone
Natalie Hunt	Hunton & Williams
Sara Marshall	Identity and Passport Service
Eduardo Ustaran	Field Fisher Waterhouse
Nick Coleman	Author of 'The Coleman Report: An Independent Review of Government Information Assurance'
Clemence Marcelis	Consumer Focus
Linda Weatherhead	Consumer Focus

Roundtable 2: Medical information, 15th January 2010

Harry Cayton	Council for Healthcare Regulatory Excellence
Adrian Sieff	Health Foundation
Marlene Winfield	Department of Health
Niall Monaghan	British Computer Society Health Informatics Forum
Dr Claudia Pagliari	University of Edinburgh
Dr Gillian Braunold	Department of Health
Michael Keegan	General Medical Council
Dr Justin Whatling	BT
Sophie Brannan	British Medical Association
Dr Tony Calland	British Medical Association

Henny Abuzaid	Consumer Focus
Jon Fistein	Tribal
Stephen Whitehead	new economics foundation

Roundtable 3: Targeted advertising, 19th January 2010

Iain Henderson	MyDex
Nick Stringer	Internet Advertising Bureau
Anna Fielder	Consumer rights expert
Cristina Luna-Esteban	Office of Fair Trading
Philip Virgo	EURIM
Jeremy Simon	Virgin Media
Daphne Yao	Virgin Media
Kasey Chapelle	Vodafone
Anthony House	Google

Notes

1 *Hansard*, 20 Nov 2007, vol 467, col 1101, www.publications.parliament.uk/pa/cm200708/cmhansrd/cm071120/debtext/71120-0004.htm#0711205800015 8 (accessed Mar 2010).

2 Information Commissioner's Office, 'Report data breaches or risk tougher sanctions, warns the ICO', 26 Jan 2010, www.ico.gov.uk/upload/documents/pressreleases/2010/data_breaches_260110.pdf (accessed Mar 2010).

3 House of Lords Constitution Committee, *Surveillance: Citizens and the State*, (London: House of Lords Constitution Committee, 2009), www.publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/1803.htm (accessed Mar 2010).

4 Information Commissioner's Office, *Report on the Findings of the Information Commissioner's Office Annual Track 2008*, Dec 2008, www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/ico_annual_tracking_individuals_final_report2008.pdf (accessed Mar 2010).

5 R Woods, 'Facebook's Mark Zuckerberg says privacy is dead. So why does he want to keeps this picture hidden?', *The Sunday Times,* 17 Jan 2010, http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article6991010.ece (accessed Mar 2010).

6 Information Commissioner's Office, *ICM Personal Information Survey,* http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/icm_research_into_personal_information_feb08.pdf (accessed Mar 2010).

7 comScore, Inc, 'Social networking explodes worldwide as sites increase their focus on cultural relevance', August 2008, www.comscore.com/Press_Events/Press_Releases/2008/08/Social_Networking_World_Wide/%28language%29/eng-US (accessed Mar 2010).

8 C Raab and C Bennett, *The Governance of Privacy* (Cambridge, MA: MIT Press, 2006) p 25.

9 DJ Solove, *Understanding Privacy* (Cambridge, MA: Harvard University Press, 2008), p 1.

10 Perri 6, *The Future of Privacy* (London: Demos, 1998), p 215.

11 See for example d boyd, 'Why youth (heart) social network sites: The role of networked publics in teenage social life' in D Buckingham (ed) *Youth, Identity, and Digital Media*, MacArthur Foundation Series on Digital Learning (Cambridge, MA: MIT Press). See also DJ Solove, *The Future of Reputation: gossip, rumor, and privacy on the internet* (New Haven and London: Yale University Press, 2007).

12 T Ilube, 'Where everybody knows your name' in C Fieschi and C Edwards (eds), *UK Confidential*, (London: Demos, 2008).

13 For an outline of the problem of identity online, see K Cameron, *The Laws of Identity*, www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf (accessed Mar 2010).

14 P Bradwell and N Gallagher, *FYI: The new politics of personal information* (London: Demos, 2007).

15 D Lyon, *Surveillance Studies: An overview*, (Cambridge: Polity, 2007), p 26.

16 A Travis, 'Legislation to access public's texts and emails put on hold', *The Guardian*, 10 Nov 2009, www.guardian.co.uk/uk/2009/nov/09/home-office-plan-data-storage (accessed Mar 2010).

17 See, for example, H Porter, 'The dangers of state surveillance', *The Guardian*, 1 Feb 2010, www.guardian.co.uk/commentisfree/henryporter/2010/feb/01/ripa-act-surveillance-authorities (accessed Mar 2010).

18 For the background to the people's inquiry and the lines of research on which it draws, see appendix A.

19 J Stilgoe, *Nanodialogues* (London: Demos, 2007) p 19.

20 Stilgoe, *Nanodialogues*, p 19.

21 For more on the methodology and the profiles of those who attended the inquiry, see appendix A.

22 M Dale, 'Suit: Pa. school spied on students via laptops', *The Associated Press*, 18 Feb 2010, www.google.com/hostednews/ap/article/ALeqM5gdwlE3DpcMD9gNAnFMrQ7iNHCS6AD9DUNV2G1 (accessed Mar 2010).

23 D Drummond, 'A new approach to China', *The Official Google Blog*, 12 Jan 2010, http://googleblog.blogspot.com/2010/01/new-approach-to-china.html (accessed Mar 2010).

24 *BBC News*, 'Man in Facebook paedophile ordeal', 18 Feb 2010, http://news.bbc.co.uk/1/low/england/manchester/8523103.stm (accessed Mar 2010).

25 Experian, 'Mosaic UK: The consumer classification for the UK', www.experian.co.uk/www/pages/what_we_offer/products/mosaic_uk.html (accessed Mar 2010).

26 Home Office, 'Electronic communications: The Data Retention (EC Directive) Regulations 2009' (London: OPSI, 2009), www.opsi.gov.uk/si/si2009/draft/ukdsi_9780111473894_en_1 (accessed Mar 2010).

27 The Regulation of Investigatory Powers Act 2000 (London: Stationery Office, 2000), www.opsi.gov.uk/acts/acts2000/ukpga_20000023_en_1 (accessed Mar 2010).

28 Home Office, *Protecting the Public in a Changing Communications Environment* (London: Home Office, 2009), www.homeoffice.gov.uk/documents/cons-2009-communication-data/cons-2009-communications-data2835.pdf (accessed Mar 2010).

29 *Protecting the Public in a Changing Communications Environment*.

30 Home Office, *Regulation of Investigatory Powers Act 2000: consolidating orders and codes of practice – responses to the consultation* (London: Home Office, 2009), www.homeoffice.gov.uk/documents/cons%2D2009%2Dripa/ripa-cons-response2835.pdf (accessed Mar 2010).

31 Liberal Democrat Voice, 'Huhne attacks RIPA snoopers' charter: "the Government's surveillance society has got out of hand"', 17 Apr 2009, www.libdemvoice.org/huhne-attacks-ripa-snoopers-charter-the-governments-surveillance-society-has-got-out-of-hand-13730.html (accessed Mar 2010).

32 *RIPA 2000: consolidating orders and codes of practice*.

33 P Kennedy, *Report of the Interception of Communications Commissioner 2008*, 21 Jul 2009, www.official-documents.gov.uk/document/hc0809/hc09/0901/0901.pdf (accessed Mar 2010).

34 Open Rights Group, 'Digital Economy Bill: Brief to Lords on Second Reading', www.openrightsgroup.org/ourwork/reports/digital-economy-bill-briefing (accessed Mar 2010).

35 See, for example, the OpenNet Initiative report, *Internet Filtering in China*, 15 Jun 2009, available at http://opennet.net/research/profiles/china (accessed Mar 2010).

36 See, for example, D Waters, 'BT advert trials were "illegal"', *BBC News*, 1 Apr 2008, http://news.bbc.co.uk/1/hi/technology/7325451.stm (accessed Mar 2010).

37 Phorm, 'About us', www.phorm.com/about_us/index.html (accessed Mar 2010).

38 European Commission, 'Telecoms: Commission launches case against UK over privacy and personal data protection', 14 Apr 2009, http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/570 (accessed Mar 2010).

39 European Commission, 'Telecoms: Commission steps up UK legal action over privacy and personal data protection', 29 Oct 2009 http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/1626 (accessed Mar 2010).

40 Internet Advertising Bureau, 'Internet ad spend grows 4.6%', 30 Sept 2009, www.iabuk.net/en/1/adspendgrows300909.mxs (accessed Mar 2010).

41 Office of Fair Trading, 'OFT launches market studies into advertising and pricing practice', 15 Oct 2009, www.oft.gov.uk/news/press/2009/126-09 (accessed Mar 2010).

42 Federal Trade Commission, 'Advertising and marketing on the internet: rules of the road', www.ftc.gov/bcp/edu/pubs/business/ecommerce/bus28.shtm (accessed Mar 2010).

43 Internet Advertising Bureau, 'IAB Good Practice Principles', www.youronlinechoices.co.uk/good-practice-principles (accessed Mar 2010).

44 NHS, 'Summary Care Records', www.nhscarerecords.nhs.uk/summary (accessed Mar 2010).

45 For an example of the discussion of health behaviour change, see D O'Leary (ed), *The Politics of Public Behaviour* (London: Demos, 2008) and the Department of Health's three Health and well-being reports, 1 Feb 2010, www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_111698.

46 For a discussion of the development of online information 'surveillance', see P Ohm, 'The rise and fall of invasive ISP surveillance', University of Illinois Law Review 5 (2009).

47 For more detail on how the people's inquiry worked, see appendix A.

48 Ensuring Consent and Revocation (EnCoRe) is a collaborative IT research project being undertaken by UK industry and academia 'researching how to improve the rigour and ease with which individuals can grant and, more importantly, revoke their consent to the use, storage and sharing of their personal data by others'. See EnCoRe, 'EnCoRe – Ensuring Consent and Revocation', www.encore-project.info.

49 People's Inquiry into Personal Information, Session 2, Bradford.

50 People's inquiry, Session 2, Bradford.

51 People's inquiry, Session 2, London.

52 People's inquiry, Session 2, London.

53 People's inquiry, Session 2. London.

54 People's inquiry, Session 2, Bradford.

55 People's inquiry, Session 2, Bradford.

56 People's inquiry, Session 2, Bradford.

57 People's inquiry, Session 2, Bradford.

58 People's inquiry, Session 2, Bradford.

59 People's inquiry, Session 2, Bradford.

60 People's inquiry, Session 2, Bradford.

61 People's inquiry, Session 2, Bradford.

62 People's inquiry. Session 2, Bradford.

63 People's inquiry, Session 2, London.

64 People's inquiry, Session 2, Bradford.

65 People's inquiry, Session 4, London.

66 People's inquiry, Session 2, London.

67 People's inquiry, Session 2, London.

68 People's inquiry, Session 2, London.

69 People's inquiry, Session 2, Bradford.

70 People's inquiry, Session 2, Bradford.

71 People's inquiry, Session 3, London.

72 People's inquiry, Session 3, Bradford.

73 People's inquiry, Session 3, Bradford.

74 People's inquiry, Session 3, Bradford.

75 People's inquiry, Session 3, Bradford.

76 For information about the UK Biobank project, see www.ukbiobank.ac.uk.

77 People's inquiry, Session 3, Bradford.

78 People's inquiry, Session 3, London.

79 People's inquiry, Session 3, London.

80 People's inquiry, Session 3, Bradford.

81 People's inquiry, Session 3, London.

82 People's inquiry, Session 3, London.

83 People's inquiry, Session 4, London.

84 People's inquiry, Session 3, Bradford.

85 People's inquiry, Session 3, Bradford.

86 People's inquiry, Session 4, London.

87 People's inquiry, Session 4, London.

88 People's inquiry, Session 4, London.

89 People's inquiry, Session 4, London.

90 People's inquiry, Session 4, London.

91 People's inquiry, Session 3, Bradford.

92 People's inquiry, Session 4, London.

93 People's inquiry, Session 4, London.

94 Data Protection Act 1998 (London: Stationery Office, 1998), http://www.statutelaw.gov.uk/content.aspx?LegType=All+Primary&PageNumber=1&BrowseLetter=D&NavFrom=1&activeTextDocId=3190610&parentActiveTextDocId=3190610&showAllAttributes=0&hideCommentary=0&showProsp=0&suppressWarning=1.

95 Information Commissioner's Office, 'Processing personal data fairly and lawfully', www.ico.gov.uk/for_organisations/data_protection_guide/principle_1_processing_personal_data_fairly_and_lawfully.aspx (accessed Mar 2010).

96 People's inquiry, Session 1, London.

97 People's inquiry, Session 1, London.

98 People's inquiry, Session 1, London.

99 People's inquiry, Session 1, London.

100 People's inquiry, Session 1, London.

101 People's inquiry, Session 1, London.

102 *Media Decoder*, 'An interview with David Vladeck of the FTC', *The New York Times*, 5 Aug 2009, http://mediadecoder.blogs.nytimes.com/2009/08/05/an-interview-with-david-vladeck-of-the-ftc (accessed Mar 2010).

103 People's inquiry, Session 1, London.

104 People's inquiry, Session 2, London.

105 People's inquiry, Session 2, London.

106 People's inquiry, Session 1, London.

107 People's inquiry, Session 1, London.

108 People's inquiry, Session 1, London.

109 People's inquiry, Session 1, London.

110 People's inquiry, Session 1, London.

111 People's inquiry, Session 1, London.

112 People's inquiry, Session 2, Bradford.

113 People's inquiry, Session 2, Bradford.

114 People's inquiry, Session 4, Bradford.

115 People's inquiry, Session 4, London.

116 People's inquiry, Session 4, London.

117 People's inquiry, Session 4, Bradford.

118 People's inquiry, Session 4, Bradford.

119 People's inquiry, Session 4, Bradford.

120 People's inquiry, Session 4, Bradford.

121 People's inquiry, Session 4, London.

122 People's inquiry, Session 4, Bradford.

123 People's inquiry, Session 4, London.

124 People's inquiry, Session 4, London.

125 People's inquiry, Session 4, London.

126 People's inquiry, Session 4, London.

127 People's inquiry, Session 4, London.

128 People's inquiry, Session 4, London.

129 Perri 6, *The Future of Privacy*.

130 Electronic Privacy Information Centre, 'Complaint, Request for Investigation, Injunction, and Other Relief in the matter of Google Inc', http://epic.org/privacy/ftc/googlebuzz/GoogleBuzz_Complaint.pdf (accessed Mar 2010).

131 K Fiveash, 'Schmidt defends Google Buzz despite tweaks aplenty', *The Register*, 17 Feb 2010, www.theregister.co.uk/2010/02/17/google_buzz_schmidt (accessed Mar 2010).

132 Article 29 Data Protection Working Party, *The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data* (Brussels: European Commission, 2009), p 8.

133 J Wilsdon and R Willis, *See Through Science* (London: Demos, 2004).

134 Stilgoe, *Nanodialogues*.

135 BMRB, *Stem Cell Dialogue* (London: BMRB, 2008), www.mrc.ac.uk/consumption/idcplg?IdcService=GET_FILE&dID=18081&dDocName=MRC005309&allowInterrupt=1.

136 Ofcom, *Communications market report: English regions 2009* (London: Ofcom, 2009), www.ofcom.org.uk/research/cm/cmrnr09/england/nrcmreng.pdf.

137 See www.demos.co.uk.

References

Article 29 Data Protection Working Party, *The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data* (Brussels: European Commission, 2009).

BBC News, 'Man in Facebook paedophile ordeal', 18 Feb 2010, http://news.bbc.co.uk/1/low/england/manchester/8523103.stm (accessed Mar 2010).

boyd, d, 'Why youth (heart) social network sites: The role of networked publics in teenage social life' in D Buckingham (ed), *Youth, Identity, and Digital Media*, MacArthur Foundation Series on Digital Learning (Cambridge, MA: MIT Press).

BMRB, *Stem Cell Dialogue*. London: BMRB, 2008. www.mrc.ac.uk/consumption/idcplg?IdcService=GET_FILE&dID=18081&dDocName=MRC005309&allowInterrupt=1.

Bradwell, P and Gallagher, N, *FYI: The new politics of personal information* (London: Demos, 2007).

Cameron, K, *The Laws of Identity*, www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf (accessed Mar 2010).

comScore, Inc, 'Social networking explodes worldwide as sites increase their focus on cultural relevance', August 2008, www.comscore.com/Press_Events/Press_Releases/2008/08/Social_Networking_World_Wide/%28language%29/eng-US (accessed Mar 2010).

Dale, M, 'Suit: Pa. school spied on students via laptops', *The Associated Press*, 18 Feb 2010, www.google.com/hostednews/ap/article/ALeqM5gdwlE3DpcMD9gNAnFMrQ7iNHCS6AD9DUNV2G1 (accessed Mar 2010).

Data Protection Act 1998. London: Stationery Office, 1998. http://www.statutelaw.gov.uk/content.aspx?LegType=All+Primary&PageNumber=1&BrowseLetter=D&NavFrom=1&activeTextDocId=3190610&parentActiveTextDocId=3190610&showAllAttributes=0&hideCommentary=0&showProsp=0&suppressWarning=1.

Drummond, D, 'A new approach to China', *The Official Google Blog*, 12 Jan 2010, http://googleblog.blogspot.com/2010/01/new-approach-to-china.html (accessed Mar 2010).

Electronic Privacy Information Centre, 'Complaint, Request for Investigation, Injunction, and Other Relief in the matter of Google Inc', http://epic.org/privacy/ftc/googlebuzz/GoogleBuzz_Complaint.pdf (accessed Mar 2010).

European Commission, 'Telecoms: Commission launches case against UK over privacy and personal data protection', 14 Apr 2009, http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/570 (accessed Mar 2010).

European Commission, 'Telecoms: Commission steps up UK legal action over privacy and personal data protection', 29 Oct 2009, http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/1626 (accessed Mar 2010).

Experian, 'Mosaic UK: The consumer classification for the UK', www.experian.co.uk/www/pages/what_we_offer/products/mosaic_uk.html (accessed Mar 2010).

Federal Trade Commission, 'Advertising and marketing on the internet: rules of the road', www.ftc.gov/bcp/edu/pubs/business/ecommerce/bus28.shtm (accessed Mar 2010).

Hansard, 20 Nov 2007, vol 467, col 1101, www.publications.parliament.uk/pa/cm200708/cmhansrd/cm071120/debtext/71120-0004.htm#07112058000158 (accessed Mar 2010).

Home Office, 'Electronic communications: The Data Retention (EC Directive) Regulations 2009'. London: OPSI, 2009. www.opsi.gov.uk/si/si2009/draft/ukdsi_9780111473894_en_1 (accessed Mar 2010).

Home Office, *Protecting the Public in a Changing Communications Environment* (London: Home Office, 2009), www.homeoffice.gov.uk/documents/cons-2009-communication-data/cons-2009-communications-data2835.pdf (accessed Mar 2010). The summary of responses to the consultation is available at www.homeoffice.gov.uk/documents/cons-2009-communication-data/cons-2009-comms-data-responses2835.pdf.

Home Office, *Regulation of Investigatory Powers Act 2000: consolidating orders and codes of practice – responses to the consultation*. London: Home Office, 2009. www.homeoffice.gov.uk/documents/cons%2D2009%2Dripa/ripa-cons-response2835.pdf (accessed Mar 2010).

House of Lords Constitution Committee, *Surveillance: Citizens and the State*. London: House of Lords Constitution Committee, 2009. www.publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/1803.htm (accessed Mar 2010).

Ilube, T, 'Where everybody knows your name' in C Fieschi and C Edwards (eds), *UK Confidential* (London: Demos, 2008).

Internet Advertising Bureau, 'IAB Good Practice Principles', www.youronlinechoices.co.uk/good-practice-principles (accessed Mar 2010).

Internet Advertising Bureau, 'Internet ad spend grows 4.6%', 30 Sept 2009, www.iabuk.net/en/1/adspendgrows300909.mxs (accessed Mar 2010).

Information Commissioner's Office, 'Processing personal data fairly and lawfully', www.ico.gov.uk/for_organisations/data_protection_guide/principle_1_processing_personal_data_fairly_and_lawfully.aspx (accessed Mar 2010).

Information Commissioner's Office, *ICM Personal Information Survey,* http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/icm_research_into_personal_information_feb08.pdf (accessed Mar 2010).

Information Commissioner's Office, *Report on the Findings of the Information Commissioner's Office Annual Track 2008*, Dec 2008, www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/ico_annual_tracking_individuals_final_report2008.pdf (accessed Mar 2010).

Information Commissioner's Office, 'Report data breaches or risk tougher sanctions, warns the ICO', 26 Jan 2010, www.ico.gov.uk/upload/documents/pressreleases/2010/data_breaches_260110.pdf (accessed Mar 2010).

Kennedy, P, *Report of the Interception of Communications Commissioner 2008*, 21 Jul 2009, www.official-documents.gov.uk/document/hc0809/hc09/0901/0901.pdf (accessed Mar 2010).

Liberal Democrat Voice, 'Huhne attacks RIPA snoopers' charter: "the Government's surveillance society has got out of hand"', 17 Apr 2009, www.libdemvoice.org/huhne-attacks-ripa-snoopers-charter-the-governments-surveillance-society-has-got-out-of-hand-13730.html (accessed Mar 2010).

Lyon, D, *Surveillance Studies: An overview* (Cambridge: Polity, 2007).

Media Decoder, 'An interview with David Vladeck of the FTC', *The New York Times*, 5 Aug 2009, http://mediadecoder.blogs.nytimes.com/2009/08/05/an-interview-with-david-vladeck-of-the-ftc (accessed Mar 2010).

NHS, 'Summary Care Records', www.nhscarerecords.nhs.uk/summary (accessed Mar 2010).

Ofcom, *Communications market report: English regions 2009*. London: Ofcom, 2009. www.ofcom.org.uk/research/cm/cmrnr09/england/nrcmreng.pdf.

Office of Fair Trading, 'OFT launches market studies into advertising and pricing practice', 15 Oct 2009, www.oft.gov.uk/news/press/2009/126-09 (accessed Mar 2010).

Ohm, P, 'The rise and fall of invasive ISP surveillance', University of Illinois Law Review 5 (2009).

O'Leary, D (ed), *The Politics of Public Behaviour* (London: Demos, 2008).

OpenNet Initiative, *Internet Filtering in China*, 15 Jun 2009, http://opennet.net/research/profiles/china (accessed Mar 2010).

Open Rights Group, 'Digital Economy Bill: Brief to Lords on Second Reading', www.openrightsgroup.org ourwork/reports/digital-economy-bill-briefing (accessed Mar 2010).

Perri 6, *The Future of Privacy* (London: Demos, 1998).

Phorm, 'About us', www.phorm.com/about_us/index.html (accessed Mar 2010).

Porter, H, 'The dangers of state surveillance', *The Guardian*, 1 Feb 2010, www.guardian.co.uk/commentisfree/henryporter/2010/feb/01/ripa-act-surveillance-authorities (accessed Mar 2010).

Raab, C and Bennett, C, *The Governance of Privacy* (Cambridge, MA: MIT Press, 2006).

Regulation of Investigatory Powers Act 2000. London: Stationery Office, 2000. www.opsi.gov.uk/acts/acts2000/ukpga_20000023_en_1 (accessed Mar 2010).

Solove, DJ, *Understanding Privacy* (Cambridge, MA: Harvard University Press, 2008).

Stilgoe, J, *Nanodialogues* (London: Demos, 2007).

Travis, A, 'Legislation to access public's texts and emails put on hold', *The Guardian*, 10 Nov 2009, www.guardian.co.uk/uk/2009/nov/09/home-office-plan-data-storage (accessed Mar 2010).

Waters, D, 'BT advert trials were "illegal"', *BBC News*, 1 Apr 2008, http://news.bbc.co.uk/1/hi/technology/7325451.stm (accessed Mar 2010).

Wilsdon, J and Willis, R, *See Through Science* (London: Demos, 2004).

Woods, R, 'Facebook's Mark Zuckerberg says privacy is dead. So why does he want to keeps this picture hidden?', *The Sunday Times,* 17 Jan 2010, http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article6991010.ece (accessed Mar 2010).

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 filesharing 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.

The database society is not inherently good or bad. The best we can hope for is that it is as democratic as any of the institutions, markets, and regulatory and legal mechanisms that exert power over our lives. The rules governing information use will determine our power as individuals in the database society and the powers that the state, businesses and other people have over us. As the infrastructure of the database society passes through a formative stage, it is important to understand more about how in practice the use of personal information is understood by the people it affects.

Democratising personal information does not only mean giving people a voice in the debate. It also means finding better ways of listening to what they say. This pamphlet is about what people think about the use of their personal information. It sets out the findings of Demos' 'People's Inquiry into Personal Information', revealing the opinions and ideas expressed over 13 hours of deliberation. The inquiry demonstrates how to engage in the conversations that bring personal information decision-making closer to the people it affects.

Peter Bradwell is a researcher at Demos.

Consumer Focus
Campaigning for a fair deal

ico.
Information Commissioner's Office

ISBN 978-1-906693-36-7 £10