

“The public must be  
at the heart of any  
new settlement on  
data sharing...”

---

## THE DATA DIALOGUE

Jamie Bartlett



Demos is a think-tank focused on power and politics. Our unique approach challenges the traditional, 'ivory tower' model of policy making by giving a voice to people and communities. We work together with the groups and individuals who are the focus of our research, including them in citizens' juries, deliberative workshops, focus groups and ethnographic research. Through our high quality and socially responsible research, Demos has established itself as the leading independent think-tank in British politics.

In 2012, our work is focused on four programmes: Family and Society; Public Services and Welfare; Violence and Extremism; and Citizens. Alongside and connected with our research programmes, Demos has political projects focused on the burning issues in current political thinking, including the Progressive Conservatism Project, the Centre for London at Demos and Demos Collections, bringing together topical essays by leading thinkers and commentators.

Our work is driven by the goal of a society populated by free, capable, secure and powerful citizens. Find out more at [www.demos.co.uk](http://www.demos.co.uk).

First published in 2012  
© Demos. Some rights reserved  
*Magdalen House, 136 Tooley Street,  
London, SE1 2TU, UK*

ISBN 978 1 909037 16 8  
Series design by modernactivity  
Typeset by Chat Noir Design, Charente  
Printed by Lecturis, Eindhoven

Set in Gotham Rounded  
and Baskerville 10  
Cover paper: Flora Gardenia  
Text paper: Munken Premium White



# THE DATA DIALOGUE

Jamie Bartlett

## Open access. Some rights reserved.

As the publisher of this work, Demos wants to encourage the circulation of our work as widely as possible while retaining the copyright. We therefore have an open access policy which enables anyone to access our content online without charge.

Anyone can download, save, perform or distribute this work in any format, including translation, without written permission. This is subject to the terms of the Demos licence found at the back of this publication. Its main conditions are:

- Demos and the author(s) are credited
- This summary and the address *www.demos.co.uk* are displayed
- The text is not altered and is used in full
- The work is not resold
- A copy of the work or link to its use online is sent to Demos

You are welcome to ask for permission to use this work for purposes other than those covered by the licence. Demos gratefully acknowledges the work of Creative Commons in inspiring our approach to copyright. To find out more go to *www.creativecommons.org*



## Contents

Acknowledgements	7
Foreword	9
Executive summary	11
1 Background	19
2 Results	29
3 Conclusion	47
Annex: methodology	53
Notes	61
References	69



## Acknowledgements

This paper would not have been possible without the support of O2, for which we are very grateful. In particular, we would like to thank Emma Hart and Paul James for their support throughout.

The polling for the research was conducted by Populus – Laurence Stellings from Populus ensured we had all the data and analysis we requested. We would also like to thank, of course, all the participants who took part in the survey and the workshops.

At Demos, Duncan O’Leary provided useful feedback, and Ralph Scott made sure the report went smoothly through the publication process. As ever, Susannah Wight copy-edited the work quickly and accurately. Hedda Bjorge Soremshaugen produced a series of excellent background documents and briefing notes.

Any errors or omissions rest entirely with me.

Jamie Bartlett  
September 2012



# Foreword

The onset of the digital age necessitates that people share their data every day with other citizens, businesses and the Government, be it billing information, preferences or location. This information is used legitimately in many business models and to deliver public services, just as a mobile phone company must use the location information of its customers to connect mobile calls. It's a responsibility we take extremely seriously.

This is just the tip of the iceberg as more and more services become digitised and businesses and government become more aware of the opportunity in what has become known as 'Big Data'. The new services that will help make Britain digital depend upon the collection and analysis of data, including personal information, to deliver value. There is tangible citizen benefit as well as future revenue opportunity.

But the reality, and increasingly our challenge, is that people are fearful of sharing their data largely because companies and government haven't been good at clearly explaining how they use it. In order for the UK to realise the potential in the use of customer data, for the benefit of citizens themselves, there needs to be a certain level of trust established and a fair value exchange realised.

We believe in having open and honest conversations with our customers and that by asking the right questions we will be able to bring their perspective to every juncture of the digital services journey. But to do this, it is important to understand the ground from which we are starting from, which is why we commissioned what we believe to be the most in-depth research to date on the public's attitudes toward the sharing of information.

This report acts as a window through which we can view the world through the eyes of the consumer. The findings offer a

unique opportunity for us all to evolve the way we engage with citizens in the *Data Dialogue*. It tells us that as we delve deeper into this discussion, the voice of the consumer must not be lost.

There needs to be a unified push on transparency. Otherwise there will always remain confusion and concern amongst the public about inconsistent practices and standards. Whilst we don't have all the answers, we believe that by starting the conversation, asking the right questions and working collectively, we will be in a better place to get it right.

We want others to join us in exploring ways to offer transparency and control to consumers. Not just by complying with legislation but by working together to establish trust – for the benefit of UK citizens and our future business success.

Ronan Dunne  
CEO  
O2

# Executive summary

We live in an age of sharing. For reasons of security, convenience, necessity or choice we either are required – or choose – to share and disclose more information about ourselves than ever before. As more of us go online, and in more varied ways, this will continue.

The information we share tends to be one of two types:

- As we shop and subscribe on and offline, we provide ‘personal information’, which directly identifies us: bank details, telephone number, home address and so on.
- As we spend more time connected to the internet, we create more ‘behavioural data’: information that may be generated by individuals but which is anonymised and aggregated when stored and analysed. This information includes location and browsing or purchasing history.

Businesses and government are increasingly aware of the value of this information; it is now a significant asset. New ways of accessing and analysing these data can result in better (and cheaper) services for customers, innovative solutions and new sources of income. Some services – such as location based apps and network access – cannot be provided at all without sharing data. It is worth billions to the UK economy, and can also help improve public services.

As with most innovations, there are tensions and trade-offs. The question of who owns this information, and how it is collected, stored and used, is becoming a major consumer rights issue. None of the potential gains of the information revolution can be realised unless people are at the heart of any new settlement.

Finding the right balance between guaranteeing the economic and social benefits of information sharing and ensuring consumer concerns are respected requires a sophisticated understanding of what people know and think about the subject. Knowing where the public stands, therefore, is vital to companies and policymakers, particularly in fields with a fast pace of change in technology and business models.

To help inform these decisions, O2 commissioned the polling company Populus to conduct the largest ever survey looking into the public's attitudes towards personal information. It is a representative sample of over 5,000 members of the public aged 18 and over, undertaken in March 2012 (see chapter 2 for full details). The results provide new insight into the public's attitudes towards sharing information.

## Research findings

### **Finding 1 There is no single attitude to sharing personal information: the public has a very varied and diverse set of attitudes and behaviours**

Members of the public fall into one of five categories each characterised by a distinct set of views about personal information:

- *Around 30 per cent of the population are 'non-sharers'.* They are knowledgeable about data protection, view much of their data as personal and take measures to protect it.
- *Around 22 per cent of the population are 'sceptics'.* They do not have a single view about whether data are personal or impersonal – but they are sceptical about whether or not government and companies can be trusted. Unlike the non-sharers, they do not use online services much. They share data and information if the personal benefits of doing so are clear to them, but they want measures to give them simple, direct and regular control over their data.
- *Around 20 per cent of the population are 'pragmatists'.* They do not know all the details of how their data are used, but take small measures to protect their privacy. They prefer efficient services to complete privacy.

- *Around 19 per cent of the population are ‘value hunters’.* They understand the value of their data, and the benefits of sharing it. They are not overly concerned about risks to personal information being shared – but want to get the most in return.
- *Around 8 per cent of the population are ‘enthusiastic sharers’.* They categorise a lot of their information as impersonal, and subsequently are comfortable with sharing it. They are amenable to sharing more information in future, but are concerned about the ways in which those data could be misused.

These groups have often very different views about issues relating to privacy and personal information. Some general themes emerge, with variations across the different groups set out where significant.

### **Finding 2 The public does not have a clear understanding of how personal data or information is defined**

What constitutes ‘personal’ information varies from person to person: there is no clear set of principles or ideas that marks certain types of information as personal or non-personal. However, in general terms, the public tends to consider information that might allow someone to be personally identifiable or details about their personal lives – such as phone numbers or how many children one has – as personal: 83 per cent of the public consider health records as personal; 62 per cent consider a landline number as personal.

By contrast, the public tends to view information about behaviour – often generalisable or aggregatable – as less personal: 45 per cent of the public believes that your current location is personal, and only 30 per cent agree that information about the products and services you buy is personal.

Different segments have highly diverse views, however: 73 per cent of non-sharers felt that location details were personal, whereas just 12 per cent enthusiastic sharers thought so. Similarly, only one per cent of enthusiastic sharers felt the films, books and music you like is personal information, compared with 42 per cent of non-sharers.

**Finding 3 The public is aware that personal information and behavioural data are used for commercial purposes, although understanding about what this means in practice is limited**

The results suggest that knowledge about the general principles of data use is fairly widely known. For example, 85 per cent are aware that online purchasing history data are collected and used, and 81 per cent are aware of supermarket loyalty schemes. Knowledge about Gmail-based advertising is lowest, although over two-thirds (67 per cent) of the public are aware of it.

However, in the workshop, participants knew and understood less about the specific ways in which personal information is collected and used.

**Finding 4 In general, the public sees only limited benefits of sharing personal information and behavioural data**

When asked about the benefits to consumers of sharing personal information and behavioural data, members of the public are fairly negative. Only 41 per cent could see the benefits of supermarket loyalty schemes, while only 19 per cent could see the benefits of Gmail-content-based advertising, despite the fact that users can sign up to accounts for free.

Similarly to all the other findings, these results mask significant differences across the segments: 71 per cent of enthusiastic sharers compared with only 25 per cent of non-sharers could see the benefits of online purchasing data being used to suggest future purchases.

**Finding 5 People are sharing more than ever, but there is a ‘crisis of confidence’ in the way that personal information and behaviour data are being used**

Populus asked respondents a series of questions about the extent to which they were comfortable with how personal information and behavioural data are being used. The highest level of comfort is for supermarket loyalty schemes: 27 per cent of the public are comfortable with Tesco Clubcards, but only 10 per cent are comfortable with Gmail scanning email content for the purposes of targeted advertising.

This is notwithstanding that significant numbers of people share information anyway, and expect to share more in future. Indeed, 85 per cent of the public use store loyalty cards, despite these worries. Nearly one in two (48 per cent) adults expect to be sharing more personal data with companies in ten years' time (and 47 per cent expect to do so with the government). Fewer people expect to be sharing less data with private companies (19 per cent) and the government (15 per cent) by 2022. The results are very similar to the range of data people expect to be sharing in a decade's time.

### **Finding 6 Losing control of personal information is the most significant concern for the public**

For example personal data being used without permission (80 per cent) or being lost (76 per cent). Scores for government data were roughly the same.

Value hunters were markedly less concerned than other groups. Only 13 per cent of this group were concerned about companies losing personal information, compared with 76 per cent overall.

### **Finding 7 The public will welcome measures to give them more control over personal information and behavioural data, especially knowing what is held about them, and the ability to withdraw it if they wish.**

The overall results suggest the public have some significant worries about the status quo. The public recognise that sharing personal information is important – and that there are some benefits – but there is a lot of discomfort and unease about the terms on which that is currently taking place.

There was high demand for a variety of reassurance measures overall. Of particular value was the 'ability to withdraw data' (73 per cent) and to 'see what information is held on me' (70 per cent).

### Finding 8 There is no single policy solution

Public views about personal information and behavioural data are highly varied. Unsurprisingly, therefore, measures to protect personal information did not command universal support. Educating people worked well for some groups, but not for others. No single solution works well for everyone.

We set out these findings in full below, and place the research in the context of current debates surrounding personal information and privacy. Taken together, we propose the following conclusions.

### Conclusion

*There is a crisis of confidence in information sharing; regulators and companies need to respond in a dynamic and flexible way that reflects the diversity of views held by the public.*

Data and information sovereignty is the next big consumer issue. The Populus survey suggests that people share an increasing amount of information about themselves – and expect to share even more in the future. However, there is a crisis of confidence: the public is uncomfortable about the way personal information and behavioural data are collected by government and commercial companies. There is a danger that this loss of confidence will lead to people sharing less information and data, which would have detrimental results for individuals, companies and the economy.

The solution is to ensure individuals have more control over what, when and how they share information. Privacy is not easily defined. It is a negotiated concept that changes with technology and culture. It needs continually updating as circumstances and values change, which in turn requires democratic deliberation and a dialogue between the parties involved. Single, blanket solutions are not likely to work. Consumers are a highly diverse group, with very different attitudes towards information sharing, different types of concerns, and different degrees of willingness to share information. Some people want to share more than others, because they believe they will benefit from a ‘value exchange’ transaction. Others are happy to share a huge amount of

information about themselves, irrespective of personal benefits. As the demographics of internet use continue to expand, this diversity of opinions will also grow.

Regulators and businesses need to find a flexible, dynamic framework, which recognises the diversity of views on the issue, and consider how people can customise and negotiate their relationship with organisations, so that it is and feels mutually beneficial.

We believe that three key principles can help establish this approach to data sharing: offering informed choice, having meaningful options and elucidating the mutual benefit of doing so.

### Informed choice

People want to make informed decisions that make a difference to how their information is used. This demands simplicity and transparency. Informed decisions are based on knowledge about how data and information are collected, who it might be shared with, and under what conditions, so this information must be provided in a clear and simple way. This includes making distinctions between information that is personal – for example, anything that might identify them personally – and generic behavioural data, which can be aggregated and anonymised. This demand honesty about the ways in which data are collected – such as how the technology works – and how they are used.

### Meaningful options

Concerns relating to the sharing of personal data are not about the principle of sharing data *per se*, but about losing control over who accesses it and what it is used for. Information policies must be designed around the principle of consumer control – creating a spectrum of meaningful options about how much, when, and to whom consumers share information. This needs to be realistic: some products depend on information sharing, such as mobile network access services. A spectrum of options must go beyond ‘opt-in’ or ‘opt-out’, which do not reflect the shifting scale and

variety of views about information sharing held by the public. Simple dichotomies could result in too little or too much information being shared, which is bad for consumers and businesses.

### **Mutual benefit**

Consumers and companies can both benefit from sharing information. People recognise that there are potential benefits to them, but at present do not see how they are realised for consumers. As a result, consumers may not be making informed decisions about withholding their data and protecting their privacy, or sharing data and obtaining benefits. It is important to make 'value exchange' transactions between consumers and companies more explicit. At the moment people are entering into an exchange but are not always sure what they are trading. It is vital to make the currency of the exchange more explicit to all parties, so that trust is established. Any information policy must be based on fully elucidating the benefits of sharing information for individuals and companies.

Companies and organisations that take information sharing concerns seriously will be rewarded by consumers. The research suggests that people are willing to share information, but have doubts and concerns about how this is done at present. Consumers worry that commercial companies cannot always be trusted with their personal information or behavioural data.

Consumers make decisions about what to share based on trust: they will share information with companies and brands they have confidence in. To gain that trust, businesses must recognise and respond to the concerns that the UK public has about information sharing. Then they will benefit from greater consumer loyalty – and reap an economic reward, too, as consumers share more.

# 1 Background

Over the past decade, personal information and data have become an extremely important political, economic and social issue, because of four important trends:

- Citizens recognise that sharing personal information and behavioural data is an important, valuable (and inevitable) part of modern life, and are sharing more as a result.
- Companies are waking up to the potential this ‘information revolution’ has for improved services, growth and innovation.
- There are growing concerns from the public – reflected by regulatory bodies – about the way this information is being collected and used.
- Some companies are responding to these concerns, reflecting both a desire to do the right thing by their customers and gain a competitive advantage.

## The age of sharing

UK citizens recognise that sharing information is an increasingly important part of modern life. In a recent survey undertaken by Ofcom, two-thirds of respondents said they thought that technology has changed the way we communicate, and this results in us sharing more information about ourselves than ever before.<sup>1</sup> In another 2012 survey four-fifths of respondents agreed that disclosing personal information is an increasing part of modern life.<sup>2</sup>

Certainly, most of us accept that both private and public bodies – from Tesco through its Clubcards to Amazon, Oyster and Google – learn and record a vast amount about us daily. When we want to find something, we search online: Google Search now has around 30 million unique UK visitors each

month.<sup>3</sup> When we shop or bank, we increasingly do that online, too – 73 per cent of people with internet access at home use it to purchase goods online, while almost two-thirds use online banking services and social networking sites. New technology is also encouraging new ways to share information: 39 per cent of phone users have smartphones, compared with 27 per cent a year ago, which has resulted in a growth in what is known as location data.<sup>4</sup> In our personal lives, too, social media are changing what we consider personal and public: McKinsey Global Institute has calculated that 30 billion pieces of content are shared on Facebook each month, many of them personal.<sup>5</sup>

As sharing information becomes an increasingly important part of modern society, attitudes about personal information and behavioural data also evolve. In a recent Eurobarometer poll, a bare majority of UK respondents considered photos of themselves to be personal; less than half considered ‘who your friends are’ to be personal; 41 per cent thought that details of the websites they visit were personal; and only 32 per cent thought their tastes and opinions were personal. In contrast, large majorities regarded financial data as personal.<sup>6</sup> Nevertheless, around two-thirds of those banking online or visiting government websites said they ‘are happy to enter their personal details’, and just over half of people shopping online said that ‘they are happy to do so’.<sup>7</sup>

Of course, these figures vary according to the experience, age and demographic of the user. Ofcom’s annual survey on internet use and attitudes shows significant differences by age and socio-economic groups, an example being that those in the younger online demographic are more likely to feel more confident using online services.<sup>8</sup>

One of the reasons we now share more data is because there are considerable benefits in doing so. Providing personal information and behavioural data can result in services and applications that are more tailored to users’ needs, for example an improved shopping experience when buying goods online, better network coverage, greater security when online, and free applications and services.<sup>9</sup>

According to Ofcom, almost six in ten people think new communication methods have made their lives easier – whether through using online banking, having a better, more tailored shopping experience by buying goods online or through the provision of improved services in general.<sup>10</sup>

## The value of data

Personal information and behavioural data are valuable to companies, and many are willing to provide free services in order to access them. The ability of most of the free social network providers and internet companies to provide free or improved services depends on accessing and then using or selling personal information. Encouraging users to share their information is therefore central to these companies' business plans and lies at the heart of the commercial competition between tech giants like Google and Facebook.<sup>11</sup>

The explosion of available data and sophisticated software to analyse these new types of data, especially behavioural data, has stimulated several lucrative commercial sectors. This is partly being driven by remarkable – and very rapid – improvements in big data analytics. The data now available to companies are unprecedented: quintillions of bytes and growing at around 50 per cent a year, and aggregated webs of information rather than discrete databases.<sup>12</sup> According to the World Economic Forum, 'personal data represents an emerging asset class, potentially every bit as valuable as other assets such as traded goods, gold or oil'.<sup>13</sup>

This is especially true in the UK, where the internet economy is estimated to be worth well over one hundred billion pounds – the highest proportion of GDP of any G20 country.<sup>14</sup> Online advertising makes up a significant proportion of that, being the second biggest source of advertising revenue after TV, and constitutes a larger share of the overall advertising mix in the UK than in any other developed country.<sup>15</sup>

The Government has recognised the benefits of information sharing, and has recently announced a new Open Data Initiative, which aims to share more of the data held by

government, in order to open government up to greater accountability and help realise economic benefits by ‘enabling businesses and non-profit organisations to build innovative applications and websites using public data’.<sup>16</sup> According to a recent Demos pamphlet, *The Data Dividend*, this could help improve public services too.<sup>17</sup>

## Concerns about sharing personal information

The rapid growth – and increasing sophistication – of sharing information has resulted in a growing number of concerns about how, when and why personal information and behavioural data are being accessed and used. These have been in part driven by a number of recent privacy related cases. In 2012, Google was issued its largest ever fine for intentionally tracking and monitoring users’ web activity through cookie use, which avoided Safari’s usual block on cookies from third party sites.<sup>18</sup> Indeed, Google’s new privacy policy is being investigated by the Commission nationale de l’informatique et des libertés (CNIL), because, the Commission claims, the users of Google services are unable to identify exactly which purposes, collected data, recipients or access rights are relevant to their use of Google services.<sup>19</sup>

Concerns about personal information are not only about online security. Over the last five years, a series of lost or missing data files have seriously damaged public confidence in the government’s ability to ensure data security. This occurred most notably in 2007, when a file holding the personal details of 25 million individuals went missing.<sup>20</sup>

As privacy and data protection become a growing subject of public debate, a number of polls and surveys have suggested that there is growing concern among the public with the way personal information and behavioural data are held. The World Economic Forum claims that evidence points to a decline in trust in the ‘personal data ecosystem’.

The Eurobarometer survey *Data Protection in the European Union: Citizens’ perceptions* has asked European citizens – including UK citizens – periodically about their views on data protection. In 2003, 60 per cent of UK respondents were

concerned about data protection; this figure rose to 68 per cent in 2008. In 2003, 73 per cent of UK respondents said, were concerned about leaving information on the internet more often than before, and this figure had increased to 79 per cent by 2008. Furthermore, the poll has found a large increase in the number of people in the UK who think current legislation is unable to deal with personal information on the internet.<sup>21</sup>

Although the subject is still in a state of flux – it is a quickly moving field – the chief concerns surrounding personal information sharing tend to relate to two specific sets of issues:

- not knowing how and why personal data are being collected
- losing control over what happens to it, who has access to it and what they do with it

We call this ‘control loss’ – as it is predominantly about the individuals losing control over their information, rather than the fact of actually sharing it *per se*. Research shows that the public is increasingly aware that information is collected, but not clear about how. This is partly driven by the way technology and privacy concerns interact. The ways in which people’s personal information are collected and shared are sophisticated; this can be done in ways that the individual might not reasonably expect or even understand.

One good example is the way ‘cookies’ are collected and stored. Cookies allow pages like Facebook to divert traffic onto their partners’ websites. A survey conducted by PricewaterhouseCoopers LLP found that only 13 per cent of respondents fully understood how cookies worked, although 37 per cent had heard of them.<sup>22</sup> Similarly, Ofcom’s *Adults’ Media Use and Attitudes Report* found that just over half (53 per cent) knew how to delete cookies from a PC, laptop, netbook or tablet website browser.<sup>23</sup> The Communications Consumer Panel (CCP) – an independent group of experts that provides advice to Ofcom – found that there was less awareness that mobile phone apps can also collect personal data (45 per cent knew they did).<sup>24</sup>

Some privacy groups argue that legal protections over personal data – such as the Data Protection Act – can be

routinely breached by ‘surveillance by design’, in which surveillance is established as a design element of new hardware and systems. Privacy International, for example, accuses the UK Government of failing to promote a culture of secure protection of personal information data. It claims that personal data from government computers are routinely being revealed and passed on, at the expense of privacy, suggesting that this is done for profit-making purposes.<sup>25</sup>

Concerns over the Coalition Government’s recently proposed communications bill reflect these worries. The bill proposes to force network and telecommunications providers to store at least six months’ worth of telephone and internet usage data on all customers, in order to assist police and security services maintain law and order and undertake criminal prosecution. Privacy groups have argued that this would be an unacceptable level of surveillance, and that the technology involved would allow for longer-term data collection in a way that has not been taken into account by the bill itself.

More prosaically, privacy and data-sharing agreements are sometimes non-existent, misleading, or overly technical and jargon-ridden, which makes them difficult to understand. The CCP argued in 2011 that companies need to improve consumers’ awareness of how their data are collected and used, and provide straightforward information for them. Although the majority of people are aware of website terms and conditions, most of us barely or never read them when downloading apps or uploading information.<sup>26</sup> As a result, consumers may not be making informed decisions about withholding their data and protecting their privacy, or sharing data and obtaining benefits.<sup>27</sup>

The second aspect of control loss relates to *who* has access to personal information. One 2011 poll showed that nine out of ten consumers in the UK would like control over the personal information they share with companies and the manner in which it is stored.<sup>28</sup> Other research supports this position; the Information Commissioner’s Office (ICO) found that six in ten ‘feel they have lost control over the way their information is collected and processed’.<sup>29</sup>

Third party access ranks among people's highest concerns about information sharing, especially when it is used for targeted advertising. Nearly half (48 per cent) of UK adults say they are not comfortable with websites using their information in this way (which contrasts with a more positive attitude to companies using personal information to generate more business or develop new services).<sup>30</sup> This survey also found that the loss of personal data to unknown third parties 'was less acceptable than companies using the information themselves'.<sup>31</sup> Consumer Empowerment Tracker research from 2011 found that nine out of ten consumers believe that they should 'be able to control what information organisations collect about me and what they use this information for'.<sup>32</sup> This is also true of cloud computing, the rapidly growing data storage system whereby data are not stored on devices, but on the web. The World Economic Forum believes that users are mainly concerned about business competitors or government authorities being able to access their personal data without their knowledge or consent.<sup>33</sup>

Regulators are responding, seeking a suitable balance between the economic and social imperative of sharing information, while ensuring there is sufficient protection to the public. The shift is clearly one towards regulators giving consumers more control over their personal data – including historic data – and making consent over data sharing more explicit. However, the fundamental tension remains between the need for stimulating economic growth and innovation, and taking measures to protect internet users from the risks concerning use of personal information.<sup>34</sup> It is an extremely difficult balance to strike.<sup>35</sup> To that end, the European Commission is currently working to establish a reformed data protection act, establishing a unified law for the entire European Union. The aim is to increase accountability and responsibility for those processing personal information, to ensure explicit consent of the user or consumer (sometimes called 'opt-in'), and to make it easier for people to access (and if desired, delete) the data that are held on them. The Commission also intends to strengthen the power of national independent data protection

authorities, enabling them to enforce rules and punishments of companies in breach of European Union legislation.<sup>36</sup>

In 2011 the UK Government launched a ‘midata’ initiative, a voluntary programme with industry, which will give consumers increased access to their personal data in a portable, electronic format. The Government is also currently consulting on creating new powers which would compel suppliers of services and goods to provide to their customers, on request, historic transaction and consumption data in an open standard machine-readable format.

There are also a number of issue-specific reforms being proposed or adopted. The EU directive on cookies – dubbed the ‘cookie law’ – was adopted by all EU countries (including the UK) in May 2011. This directive requires implied consent when visiting a web page, and more clear and concise language in cookie policy guidelines: there must be a clear statement on web pages explaining that although users consented to cookies, they are still able to withdraw this consent, and must be made fully aware of how this withdrawal of consent may affect their future use of the website.<sup>37</sup>

### **Commercial response: the privacy dividend**

Alongside the regulatory bodies, private companies themselves have started to take a more nuanced and consumer focused approach to personal data collection. This is partly driven by a recognition that there is a commercial interest in them doing so. Some internet companies – such as Google – have recently been experimenting with ways to allow for users to have more control over the information they share.<sup>38</sup>

Indeed, according to the ICO there is a ‘privacy dividend’ – a commercial case – for private companies to offer more control over personal information to consumers.<sup>39</sup> Research shows that brand trust is extremely important to consumers when making decisions about sharing personal information. People are often ready to embrace communications services – recognising the benefits – but only if and when they trust the holders of those data to treat their information with care.<sup>40</sup>

Certainly, the growth in consumer confidence to shop online, especially among new internet users, has accelerated online shopping revenue. The risks internet users face when shopping online are reduced by assessing the reputation of online sellers, as well as promoting their fair and truthful behaviour.<sup>41</sup>

As the value of personal information and behavioural data continues to grow, organisations with open, transparent and clear information-sharing relationships with customers will have significant advantage.<sup>42</sup> This is good news for consumers too.



## 2 Results

### Existing survey data

The concept of privacy cannot be defined by experts; it is a negotiated concept that changes with technology and culture. A generation ago a phone call or photo album might have been widely considered to be private. Today that is not necessarily the case. Knowing where the public stands, therefore, is vital to companies and policymakers, particularly in fields with a fast pace of change in technology and business models.

As public interest in personal information and privacy has grown, more polls and surveys have gauged public attitudes. They are of varying quality and detail, ranging from small focus group discussions to targeted demographic polls and nationally representative survey data.<sup>43</sup> Among the latter, the CCP, the ICO and the Oxford Internet Institute have produced survey data based on between 1,000 and 2,000 respondents, with quotas and weightings to ensure representivity.<sup>44</sup> This work has been invaluable in improving our understanding of the attitudes and concerns of the public.

### New Populus poll

This survey is the largest of its type. Populus interviewed a random sample of 5,010 adults living in Great Britain aged 18 and over online between 9 and 14 March 2012. Interviews were conducted across the country and the results have been weighted to the profile of all adults aged 18 or over. It is therefore a representative poll of the public and we feel confident making statements about its findings on Great Britain as a whole.

The size of this new survey means we are able to break down and analyse the data sets with a degree of granularity and specificity that has not been possible in previous surveys.

Populus asked participants 31 questions about their online behaviour, knowledge of data sharing, and attitudes, and a small number of demographic-based questions.

In addition to the polling, Populus conducted four focus groups in London among members of the public on the 30 and 31 May 2012.<sup>45</sup> Quotes from participants of these focus groups are included throughout for the purposes of illustrating the survey findings.

The annex at the end of this report sets out the demographic background of the respondents, and specific gender, age, social economic group and regions of the sample and the various segments.

The main results are set out below.

### **Finding 1 There is no single attitude to sharing personal information: the public has a very varied and diverse set of attitudes and behaviours**

Populus asked respondents a series of attitudinal and behavioural questions on four key areas relating to data sharing:

- how personal or impersonal they regard their data to be
- how comfortable they are in sharing their data
- whether they believe they gain something from sharing their data
- how receptive they are to ideas that increase data safeguards

Based on these responses, Populus placed respondents into one of five categories (see annex for details), spanning a range of views and attitudes about personal data: non-sharers, sceptics, pragmatists, value hunters and enthusiastic sharers.

#### ***Non-sharers (30 per cent)***

Nearly one in three (30 per cent) of adults – 14.19 million people – are non-sharers. They are very cautious about technology and sharing their personal data, and tend not to be experienced at using modern technology.

They view their data as personal, and take proactive measures to keep them private: unsubscribing, deleting their

browsing history, and alerting companies to possible violations. This attitude towards privacy is not just internet specific: non-sharers often list their number as ex-directory and place a 'no junk mail' sign outside their door.

As a group, they are knowledgeable about data protection and receptive to ideas that allow them to withdraw their data.

### *Sceptics (22 per cent)*

Just over one in five (22 per cent) of the population – 10.41 million – are sceptics. They do not have a single view about whether information is personal or impersonal in principle, but are sceptical about whether or not government and companies can be trusted. Unlike the non-sharers they do not use online services much, and tend to be older – so there is little scope for them to build up trust through experience.

Those in this group are cynical about a range of issues –including the benefits of sharing data. Although they sometimes buy into 'value exchange' transactions when the personal benefits are clear, they would welcome measures to give them simple, direct and regular control over their data.

### *Pragmatists (20 per cent)*

One in five (20 per cent) of the population – 9.4 million people – are pragmatists. They do not know all the details of how their data are used, but take small measures to protect their privacy, such as retaining ownership over their data even after they have been shared with third parties.

They prefer efficient services to complete privacy – seeing benefits from the sharing of personal information – so their trust in the companies or institutions that hold their data is key.

### *Value hunters (19 per cent)*

Just under one in five (19 per cent) of the population – 8.99 million people – are value hunters. This group understands the financial value of their personal data, and recognises that sharing them can save money and time, and thus have a beneficial outcome.

They tend to be young, and are often early adopters of technology and on the lookout for new advances that can make a practical difference to their lives – they are not overly concerned about risks to personal information being shared, and are reasonably comfortable with their data being used. They are knowledgeable and understand the value of the data they are giving up.

### *Enthusiastic sharers (8 per cent)*

Some 8 per cent of the population – 3.78 million people – are enthusiastic sharers, who categorise a lot of the information about them as impersonal, and subsequently are comfortable with sharing it.

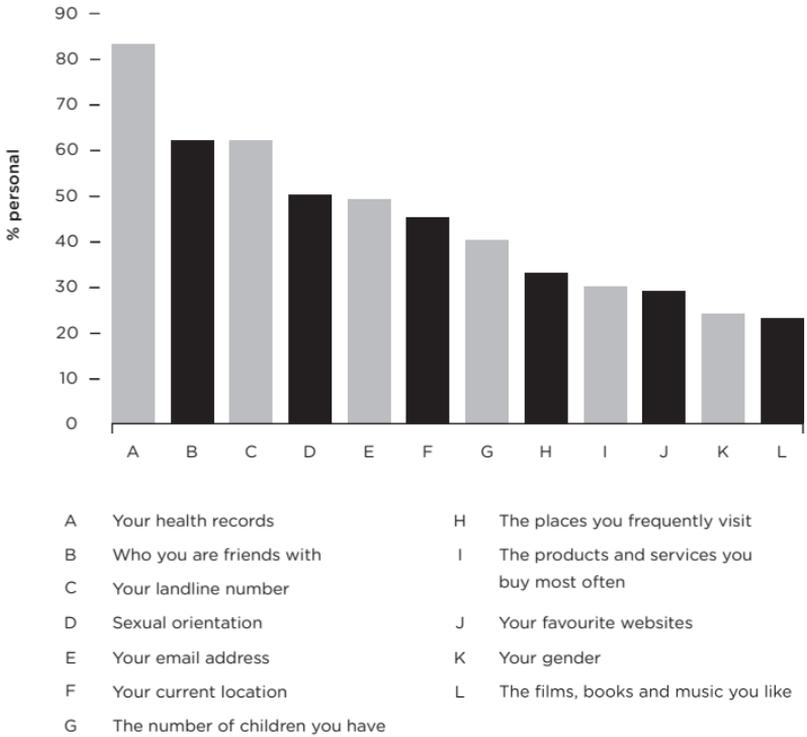
They understand ‘value exchange’ transactions, seeing the benefits of sharing information, and are amenable to sharing even more in the future. They have some concerns about the ways in which their data might be misused, but are comfortable if data use is specified.

### **Finding 2 The public does not have a clear understanding of how personal data or information is defined<sup>46</sup>**

What people consider personal or impersonal is changing. What constitutes ‘personal’ information varies from person to person: there is no clear set of principles or ideas that mark certain types of information as personal or public, but the public tends to consider information that might allow someone to be personally identifiable or details about their personal lives – such as phone numbers or how many children one has – as personal: 83 per cent of the public consider health records as personal; 62 per cent consider a landline number as personal; and half consider sexual orientation as personal.

By contrast, views about behavioural data are significantly more relaxed. The public tends to view information about behaviour – often generalisable or aggregatable – as less personal: overall, only 45 per cent of the public believe that your current location is personal; only 30 per cent agree that the products and services you buy are personal; and 29 per cent

Figure 1 Are the following personal or impersonal?



believe your favourite website constitutes personal information. This suggests there is some difference in people's attitudes towards *personal information* and *behavioural data*.

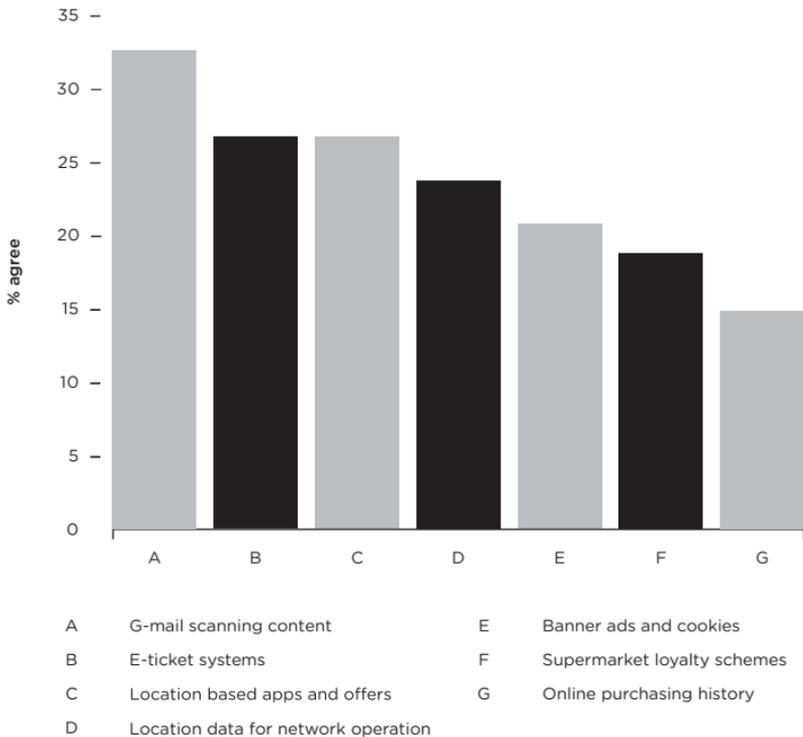
However, these findings mask significant differences between the groups. For example, 73 per cent of non-sharers felt that location details were personal, whereas just 12 per cent of enthusiastic sharers thought so. Similarly, only 1 per cent of enthusiastic sharers felt the films, books and music you like is personal information compared with 42 per cent of non-sharers.

Just 8 per cent of enthusiastic sharers consider the number of children you have to be personal, compared with 55 per cent of pragmatists.

**Finding 3 The public is aware that personal information and behavioural data are used for commercial purposes, although understanding what this means in practice is limited<sup>47</sup>**

The results suggest that knowledge about the general principles of data use is fairly widely known. For example, 85 per cent are aware that online purchasing history data is collected and used,

Figure 2 I did not know my data were used in this way



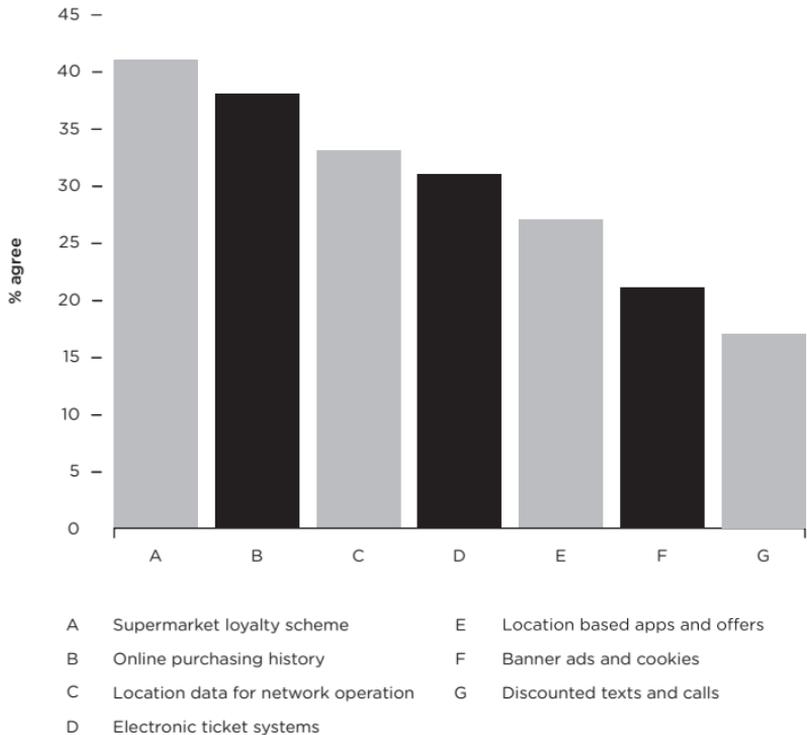
and 81 per cent are aware of supermarket loyalty schemes. Knowledge about Gmail-based advertising is lowest, at 67 per cent.

Workshop participants knew and understood much less about how data were collected and used.

#### Finding 4 In general, the public sees only limited benefits of sharing personal information and behavioural data<sup>48</sup>

Participants were asked whether they could see what consumers gained from personal data being used in a number of ways.

Figure 3 I can see what consumers gain from data being used in this way



There were low scores for every measure tested. In none of the categories could more than 50 per cent of the public see what consumers gained from the way personal information and behavioural data are used.

In the workshops, it was often noted that the reason for not recognising the benefits from sharing information was that those benefits are not always clearly stated:

*It just feels like I don't gain anything from letting companies use my data, none of them have ever told me how I benefit.*

Sceptic

The public could see the benefits most clearly (although still a minority) in what might be described as 'purchasing related data use': 41 per cent could see the benefits of supermarket loyalty schemes; 38 per cent could see the benefits of online purchasing history being used to suggest future purchases; but only 19 per cent could see the benefits of Gmail-content-based advertising – despite the free email service.

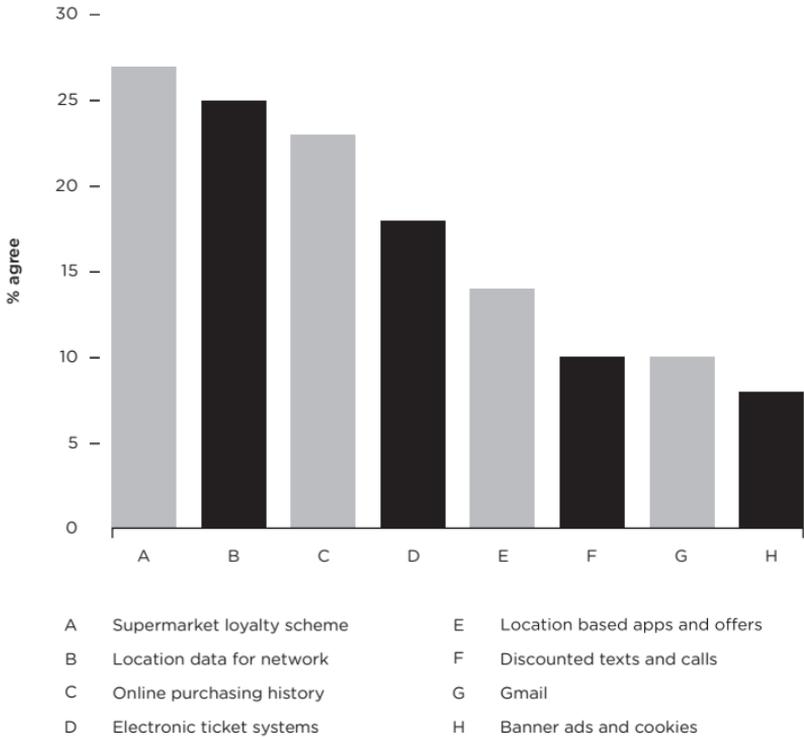
Similarly to all the other findings, these results mask significant differences across the segments: 71 per cent of enthusiastic sharers but only 25 per cent of non-sharers could see the benefits of online purchasing data being used to suggest future purchases.

### **Finding 5 People are sharing more than ever, but there is a public 'crisis of confidence' in the way that personal information and behavioural data are being used**

Populus asked respondents a series of questions about the extent to which they were comfortable with the way personal information and behavioural data are being used. Overall, the public is uncomfortable about every type of information and data use they are asked about.<sup>49</sup>

The highest level of comfort was with supermarket loyalty schemes: 27 per cent of the public are comfortable with Tesco Clubcards, but only 10 per cent of the public is comfortable with

Figure 4 I am comfortable with my data being used in this way



Gmail scanning email content for the purposes of targeted advertising.

This is notwithstanding the fact that millions of people use loyalty schemes anyway. It has been estimated that 85 per cent of people in the UK have at least one store loyalty card, while Gmail is used by around 10 million people.<sup>50</sup>

The variation between groups was considerable. Sceptics and non-sharers recorded extremely low levels of comfort – (0 per cent of non-sharers were comfortable with banner ads and

cookies). Enthusiastic sharers and pragmatists reported fairly high levels of comfort: 67 per cent of enthusiastic sharers (and 50 per cent of pragmatists) were comfortable with supermarket loyalty schemes, while 64 per cent (and 42 per cent of pragmatists) were comfortable with companies collecting the online purchasing history of individuals to recommend products.

In the workshop discussions there was considerable concern about the ways in which companies explain their information sharing policies, with many feeling they were intentionally opaque. One participant from the value hunter groups said:

*Some companies seem to sit down there and devise as difficult a way as possible to stop you unsubscribing.*

Male, 45–59, value hunter

Another mentioned the way email offers can be misleading:

*They ask you in a really sneaky way; they say click here if you do not want to receive emails from us and click here if you do want to receive emails from selected parties.*

Female, 30–44, value hunter

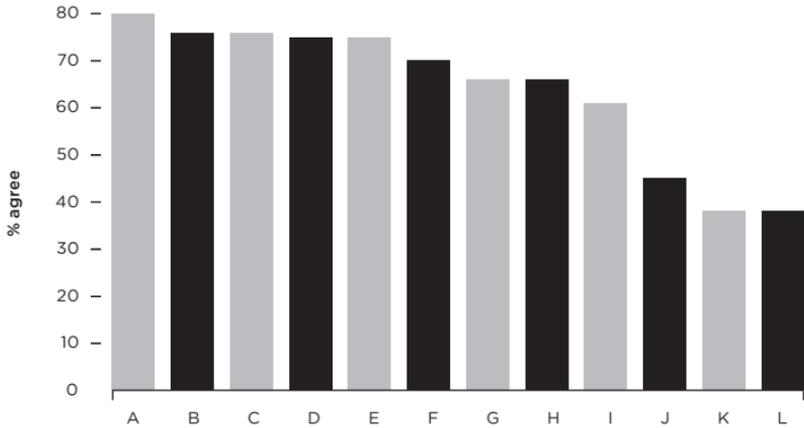
### **Finding 6 Losing control of personal information is the most significant concern**

Populus asked respondents to rate what concerns they had relating to sharing personal information in 12 circumstances.<sup>51</sup>

Overwhelmingly, the most significant set of concerns related to ‘loss of control’ – such as data being used without permission or being lost. Overall, 80 per cent were worried about companies using data without their permission; 76 per cent were worried about companies losing their personal data (scores for government were roughly the same); 76 per cent were concerned about data being shared with third parties; and 70 per cent were worried about ID theft.

In the workshop discussion, loss of control emerged as a key theme, in particular the risk of information being passed to

Figure 5 I have concerns about my data being used in this way



- A Companies using data without permission
- B Your data being sold to third parties
- C Companies losing your personal information
- D The Government using data without permission
- E The Government losing your personal information
- F ID theft
- G Your data leaving the UK
- H Your data leaving the EU
- I Automated marketing phone calls
- J Spam text messages
- K Unsolicited post
- L Spam email

the third parties. Many participants appeared happy to share information with brands they trust, but did not want it to be passed on without their permission:

*Amazon having my data is fine, as long as it stays within Amazon*  
 Male, 45–59, sceptic

A respondent from the pragmatist group asked:

*I think it's OK to give away location data, but who else apart from the company will get hold of it?*

Female, 45–59, pragmatist

By contrast, other concerns were not as significant: 61 per cent were worried about automated marketing phone calls; 45 per cent about spam text messages; and 38 per cent about spam email.

Similar to other results, there were considerable differences across segments. Value hunters were markedly less concerned than other groups. Only 23 per cent worry about companies using data in a way that they haven't given permission for; and only 13 per cent of this group were concerned about companies losing personal information; compared with 70 per cent overall.

### **Finding 7 The public expects the amount of data sharing to increase in future**

The Populus survey asked respondents whether they share more data now than ten years ago – and if they expect that to continue.

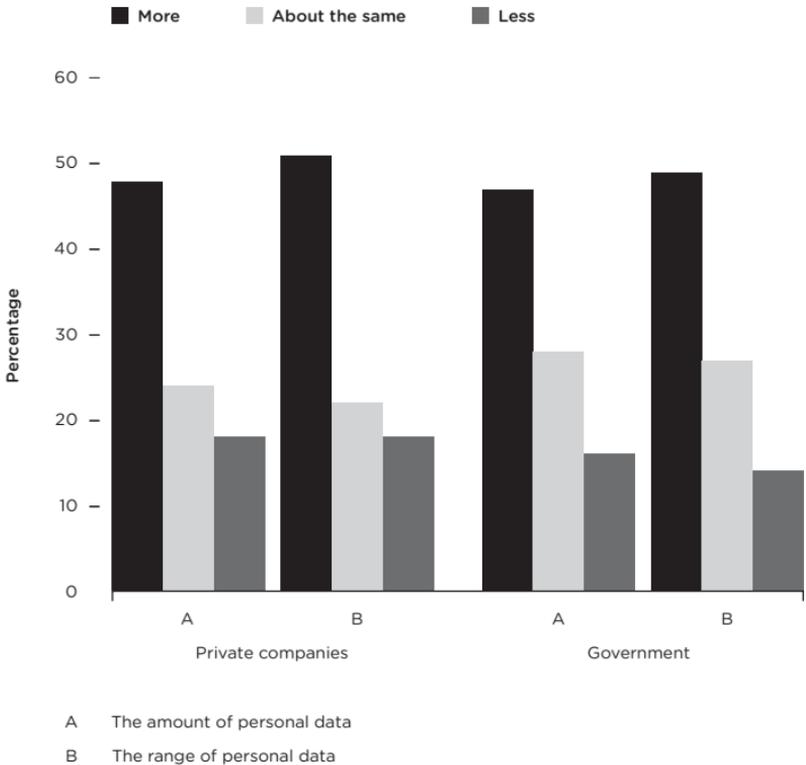
The public (including those within each of the five segments within the Populus survey) think that they already share more information today with companies and the government than they did ten years ago. They expect the amount of shared information to increase still further over the next decade. One of the reasons for this is the growth of social networks:

*You're getting more and more social networks, we're all sharing more data with them, and I just see the amount of information other people know about me increasing and increasing.*

Enthusiastic sharer

Nearly half (48 per cent) of adults expect to be sharing more personal data with companies in ten years' time (and 47 per cent expect to do so with the Government). Fewer people expect

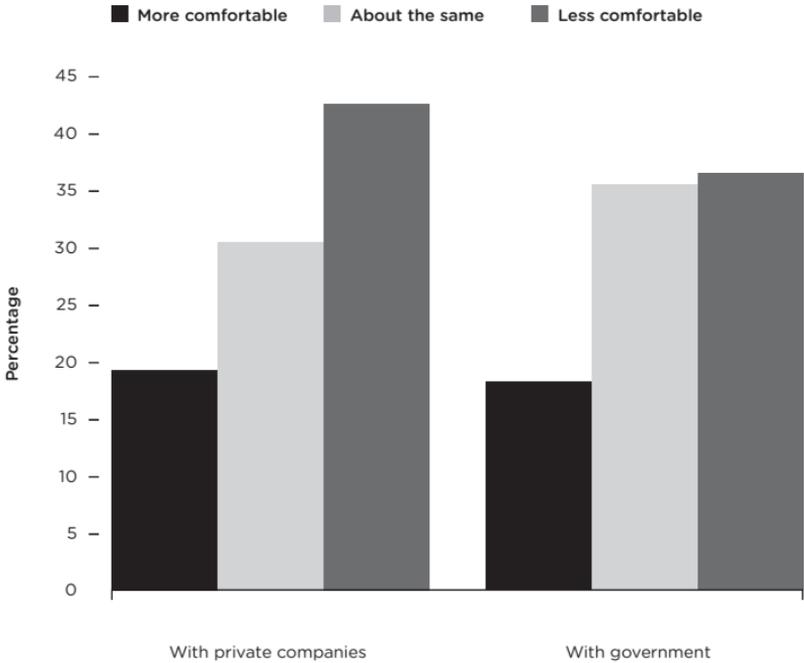
Figure 6 **How much data do you expect to share in ten years' time?**



to be sharing less data with private companies (19 per cent) and the Government (15 per cent) by 2022. The results are very similar for the range of data people expect to be sharing in a decade's time.

These findings show that people strongly expect to be sharing more information and data in the next ten years, but overall they are not comfortable with doing so: 45 per cent expect to feel less comfortable, and 20 per cent expect to feel more comfortable with sharing information with private companies; and 39 per cent expect to feel less comfortable, 17 per cent expect to feel more comfortable with sharing information with government.

Figure 7 **How comfortable do you expect to feel about sharing your data in ten years' time?**

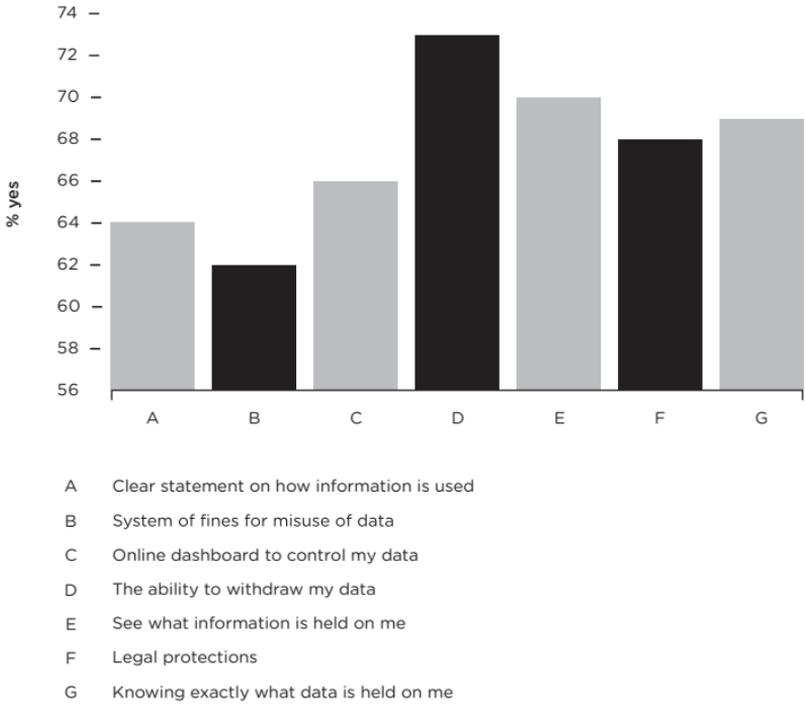


**Finding 8 The public will welcome measures to give them more control over personal information and behavioural data, especially knowing what is held about them, and to withdraw it if they wish**

The overall results suggest some significant worries about the status quo. The public recognises that sharing personal information is important – and that there are some benefits to it – but that there is a lot of discomfort and unease about the terms on which such sharing is currently taking place.

Populus asked respondents whether they would support particular measures to reassure them about sharing personal information and behavioural data.<sup>52</sup> As might be expected, there was high demand for a variety of reassurance measures overall. Of particular value was the 'ability to withdraw data' (73 per

Figure 8 **Would the following make you more comfortable with sharing information?**



cent) and to ‘see what information is held on me’ (70 per cent), but each measure scored over 62 per cent overall. The results are not uniform: value hunters and pragmatists reported a much lower degree of agreement over reassurance measures: for all measures asked about, value hunters scored between 37 per cent and 47 per cent.

In the workshop discussion, there was considerable agreement that companies taking a proactive approach to the subject would be rewarded by consumers. One participant – a sceptic – noted how a simple way of controlling the information held on him would be very welcome.

*I'd really like it if websites and companies would tell me, in simple terms, what they know about me and what they do with it. I'd like the chance to control that information.*

Sceptic

### Finding 9 There is no single policy solution

Educating people does not necessarily make people more likely to share information or data, or to have more confidence.

Overall, when various types of data use were explained, comfort levels were increased very slightly, but not dramatically.

In fact, having more information about the specific methods and techniques increased confidence and comfort among some groups, but reduced it for others. In some groups,

Figure 9 I am comfortable with my data being used in this way

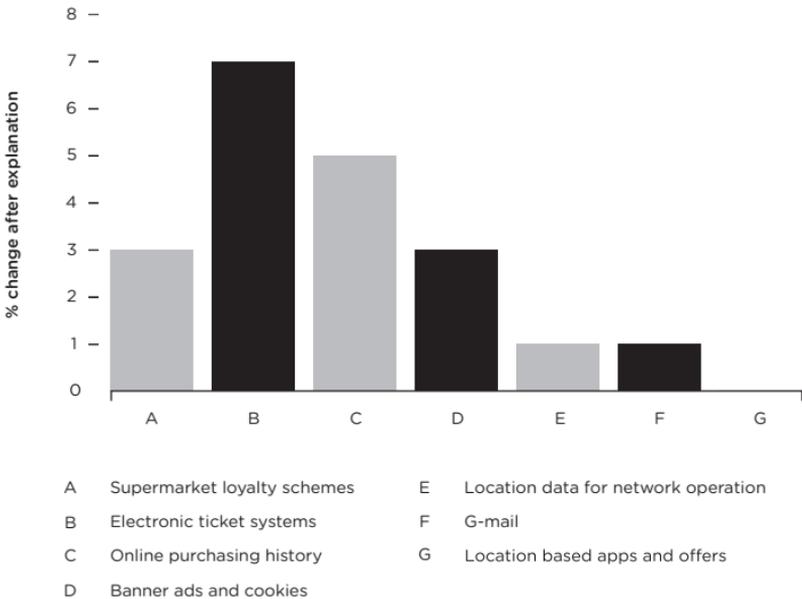
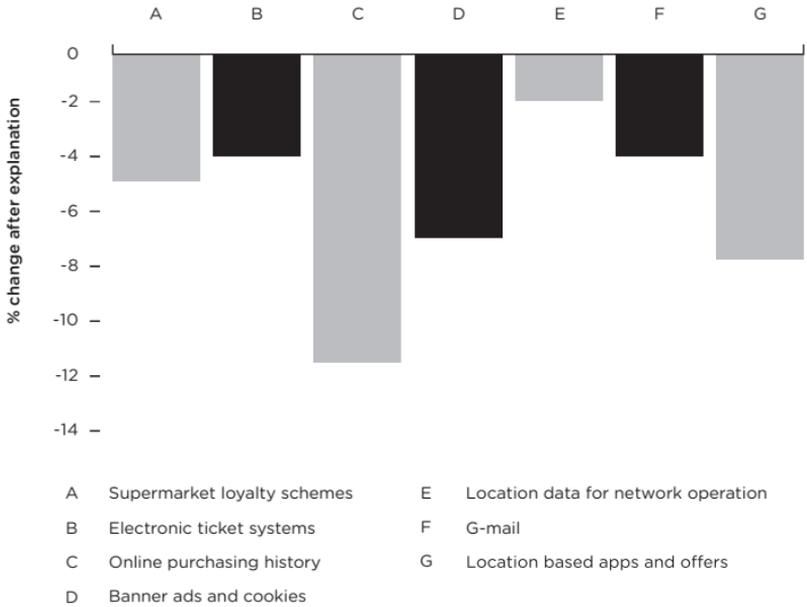


Figure 10 I am comfortable with my data being used in this way (value hunters only)



confidence *fell* overall following further explanation. For the enthusiastic sharers, value-hunters and pragmatists there was a net fall in comfort (see figure 10).



## 3 Conclusion

Personal information and behavioural data offer immense potential to businesses, society and individuals. Having access to personal information and behavioural data is an extremely important part of modern companies' business models. It drives new and better services, innovative solutions, and is an important income stream. It is worth billions to the UK economy, and a source of future economic growth. The UK is already a world leader in information access and analytics, and it is vital this is encouraged.

The information sharing revolution can also lead to better services for consumers and citizens. Some services – such as location based apps and mobile network coverage – are not possible without sharing information about where you are. Sharing personal information and behavioural data allows companies to provide better – or free – services, an improved shopping experience, better telephone coverage, greater online security and much more. As other research by Demos has argued, this data revolution can also help improve public services by making services more personalised and responsive to citizens, and more accountable to tax payers and users.<sup>53</sup>

However, as with any new and evolving area of society – especially where rapidly developing technology is involved – there are tensions and trade-offs. Alongside the remarkable development and growing sophistication of data collection and analysis tools is a recognition that information and data matter to people too: there are concerns about how information is collected, used and shared. Ultimately, none of these gains can be realised unless people are involved.

*There is a crisis of confidence in information sharing: regulators and companies need to respond in a dynamic and flexible way that reflects the diversity of views held by the public.* Data and information

sovereignty is the next big consumer issue. The Populus survey suggests that people share an increasing amount of information about themselves, and expect to do so in the future. However, there is a crisis of confidence: the public is uncomfortable about the way personal information and behavioural data are collected by government and commercial companies. There is a danger that this loss of confidence will lead to people sharing less information and data, which would have detrimental results for individuals, companies and the economy.

The answer is to ensure individuals have more control over what, when and how they share information. Privacy is not easily defined. It is a negotiated concept that changes with technology and culture. It needs continually updating as circumstances and values change, which in turn requires democratic deliberation and a dialogue between the parties involved.

Single blanket solutions are not likely to work. The public is concerned about the use of personal information and behavioural data, but not in the way that is commonly believed. Consumers are a highly diverse group, with very different attitudes towards information sharing, different types of concerns, and different degrees of willingness to share information. Some people want to share more than others, because they believe they will benefit from 'value exchange' transactions. Others are happy to share a huge amount of information about themselves, irrespective of personal benefits. As the demographics of internet use continue to expand, this diversity of opinions will also grow.

Regulators and businesses need to find a flexible, dynamic framework, which recognises the diversity of views on data sharing, and consider how people can customise and negotiate their relationship with organisations so it is and feels mutually beneficial.

We believe that three key principles can help establish this approach to data sharing: offering informed choice, having meaningful options and elucidating the mutual benefit of doing so.

## Informed choice

The modern consumer believes that the sharing of personal information is an important part of contemporary society, and will become even more so in future. Our research indicates there is a lack of understanding about the benefits of data sharing, and the mechanisms of how personal data are collected and used.

People want to make informed decisions that make a difference to how their information is used. This demands simplicity and transparency. Informed decisions are based on knowledge about how data and information are collected, who it might be shared with, and under what conditions, so this information must be provided in a clear and simple way. This includes making distinctions between information that is personal – for example, anything that might identify people personally – and generic behavioural data, which can be aggregated and anonymised. This demands honesty about the ways in which data are collected – such as how the technology works – and how they are used.

## Meaningful options

Concerns relating to the sharing of personal data are not about the principle of sharing data *per se*, but about losing control over who accesses it and what it is used for. Information policies must be designed around the principle of consumer control so a spectrum of meaningful options is created about how much, when and to whom consumers share information.

Some people want to share more than others, because they think they will benefit from a ‘value exchange’ transaction. Others are happy to share a huge amount of information about themselves, irrespective of personal benefits. Some are concerned about specific risks to sharing information, and are highly sceptical about governments’ or companies’ ability to measure and manage those risks. The research does not suggest the decision is whether ‘to share versus not to share’ but about a spectrum of views, each unique to the individual.

Options need to be realistic: some businesses depend on information sharing, such as network access services. The choice of options must go beyond ‘opt-in’ or ‘opt-out’, which do not

reflect the shifting scale and variety of views about information sharing held by the public. Simple dichotomies could result in too little or too much information being shared, which is bad for consumers and businesses.

### Mutual benefit

People recognise that there are potential benefits to information sharing, but presently do not see how they are realised for consumers. As a result, consumers may not be making informed decisions about withholding their data and protecting their privacy, or sharing data and obtaining benefits. It is important to make 'value exchange' transactions between consumer and company more explicit. At the moment people are entering into an exchange but are not always sure what they are trading. It is vital to make the currency of the exchange more explicit to all parties, so that trust is established. Any information policy must be based on fully elucidating the benefits of sharing information for the individual and the company.

*Companies and organisations that take information sharing concerns seriously will be rewarded by consumers.* The research suggests that people are willing to share information, especially with brands they trust to manage that information responsibly and transparently, but they have doubts and concerns about how that is done at present. Consumers worry that commercial companies cannot always be trusted with their personal information or behavioural data. They are worried about losing control over them, or not knowing how they are collected and used.

The key component is trust. Consumers make decisions about what to share based on trust; they will share information with companies and brands they have confidence in. Gaining that trust means recognising and responding to the concerns that the UK public has about information sharing. Taking this issue seriously – as seriously as the public does – is good not only for consumers but also for businesses, which will reap economic rewards, as consumers will share information with them. This is important because personal data are a significant growth area, and will become even more so in future.

Attitudes and behaviours about personal information are changing, and will probably continue to change in future. Many groups have a stake and an important contribution to this continuing debate, sometimes with quite different concerns and perspectives. Ultimately, any settlement that seeks to find a balance between competing social, economic, privacy-related, issues must be based on a detailed understanding of what the public thinks about the subject. From that basis, governments and businesses can establish a trust-based relationship among public policy makers, private businesses and consumers. These report findings provide new insight and detail that can help to inform this critical task.



# Annex: methodology

## Survey data

Populus interviewed a representative sample of 5,010 adults living in Great Britain aged 18 and over online between 9 and 14 March 2012, across the country. The results have been weighted to the profile of all adults aged 18 or over.

Populus asked participants 31 questions about their online and offline behaviour, knowledge of data sharing, attitudes, and a small number of demographic-based questions. Several of the questions had a number of sub-questions.

## Segments

Populus devised the segments based on respondents' replies to options grouped under four questions. The report author devised the titles for each of the segments.

These were the four questions:

*Please read these different ways in which information is currently used or might be used in future and, for each, say whether you agree or disagree using a 0–10 scale where 10 means completely agree and 0 means completely disagree that 'I'm comfortable with it being used in this way'. If you don't know, please say so.*

*Your shopping history for loyalty card schemes*

*Your travel habits for electronic ticketing systems*

*Your past purchases for online store recommendations*

*Your website browsing history stored in cookies for personalised online adverts*

*Free e-mail service funded by adverts based on the content of e-mails*

*Your location for location-relevant special offers on your mobile phone*

*Discounted calls and text messages funded by adverts based on the content of text messages and e-mails*

*Your mobile phone's location so that calls and texts can be made and received*

*Please read the following types of reassurances that could be provided by government or private companies who hold data about you and, for each, say whether it makes you more comfortable about your data being held or if it makes no difference using a 0–10 scale, where 10 means makes you much more comfortable and 0 means makes no difference. If you don't know, please say so.*

*Clear statement on how information is used*

*The ability to withdraw my data*

*Legal protections*

*System of fines for misuse of data*

*See what information is held on me*

*Knowing exactly what data are held on me*

*Online dashboard to control my data*

*Please read the following statements about this use of your data and, for each, please say whether you agree or disagree using a 0–10 scale where 10 means completely agree and 0 means completely disagree. If you don't know, please say so ('I can see what consumers gain from data being used in this way').*

*Supermarket loyalty schemes*

*Electronic ticket systems*

*Online purchasing history*

*Banner ads and cookies*

*Gmail*

*Location based apps and offers*

*Discounted texts and calls*

*Location data for network operation*

*To what extent do you regard each of the following pieces of information about you as personal or impersonal? (0–10 scale, 0 means not at all personal and 10 means very personal)*

*The details of the people you're friends with*

*The films, books and music you like*  
*The places you frequently visit*  
*The products and services you buy most often*  
*Your age*  
*Your current location*  
*Your date of birth*  
*Your educational attainment*  
*Your e-mail address*  
*Your employer's name*  
*Your ethnicity*  
*Your gender*  
*Your health records*  
*Your home/landline phone number*  
*Your postal address*  
*Your relationship status*  
*Your religion*  
*Your salary/income*  
*Your sexual orientation*  
*Passport number*  
*National insurance number*  
*Criminal record*  
*Your favourite websites*  
*Your interests and hobbies*  
*The number of children you have*  
*Your working status*

## **Main findings**

All figures, unless otherwise stated, refer to the survey results of all respondents. Some of the key variations across the five segments are set out for the purposes of illustrating the differences across segments.

In findings 2–6, 8 and 9, Populus asked respondents to rank their responses on a scale of 0–10. The percentages cited reflect the respondents responding with 8, 9 or 10.

In findings 3, 4 and 5, respondents were given short pen-portraits of the following types of information sharing before being asked to give their views about them. In finding 9,

respondents were asked to rate their levels of comfort about each type of data sharing, before and after being given the pen-portraits below.

This report does not include all the survey results, for reasons of brevity. Demos was given access to the full data set, and the report author decided which findings to present.

### Supermarket loyalty schemes

Like Tesco Clubcard and Nectar – allow supermarkets to record shoppers' transactions and build a detailed understanding of what type of people buy which products. Supermarkets can use these data to provide their customers with targeted special offers and money-off vouchers that match each customer's buying history. Supermarkets can also sell these data to third parties.

### Gmail scanning content

Gmail, the free email service offered by Google, is paid for by adverts. To run the service, Google automatically scans the content of emails sent to and from each account and the adverts shown to each user are tailored based on the content of their emails. A user with recent emails about planning a holiday, for example, is likely to see increased adverts for holidays, flights and hotels.

### Electronic ticket systems

These, like London's Oyster card system – allow travellers to avoid having to pay in cash. The systems build records of users' journey history, which can make it easier to claim compensation for delays or print personal travel histories, while the transport companies who run such schemes gain a greater understanding of how their services are used and who uses them.

### Online purchasing history

Online shops like Amazon record your purchasing history. This

allows online shops to tailor their website and recommend products to you based on those you've purchased in the past and those that other customers, like you, have. This can take the form of email recommendations, banner adverts on the website or suggestions for other products to buy.

### **Banner ads and cookies**

Online advertising systems – like banner adverts – often work by tracking the websites you visit and your interests via 'cookies'. Cookies are very small files created by websites and stored in your web browser. Cookies mean the adverts you see are tailored to your interests or past web browsing history – if you have been visiting holiday websites, for example, subsequent adverts you see on other sites will be for holidays. This system is designed to make sure web users see more relevant adverts and, in turn, increases the chance users will click on adverts making money for the advertising companies. Cookies also mean websites can remember that you have visited them before, so they can show you the UK version of a webpage, for example.

### **Location data for network operation**

All mobile phone networks know the location of each mobile device connected to their network. This information is needed so that the mobile phone network is able to send and receive phone calls, text messages, and internet data from handsets.

### **Location based apps and offers**

Many mobile phone companies offer location based apps and special offer services to their customers. These services use the current location of a mobile phone to find special offers, discounts, or other deals in close location to the mobile phone user. These special offers can then be used by showing an on-screen voucher code or barcode to shop or restaurant staff, rather than carrying paper vouchers.

## Focus groups

In addition to the polling, Populus conducted four focus groups among members of the public in London on 30 and 31 May 2012. Between 10 and 15 participants were recruited as members of four of the segments identified in the research: sceptics, enthusiastic sharers, non-sharers and value hunters; each group had a broad mix of ages (table 1), gender (table 2) and social grades (table 3). Quotes from participants of these focus groups are included throughout to illustrate the survey findings.

Table 1 **All respondents, breakdown by age**

Age	Total	Non-sharers	Sceptics	Pragmatists	Value hunters	Enthusiastic sharers
18-24	12%	6%	8%	15%	22%	13%
25-34	16%	12%	12%	20%	24%	13%
35-44	19%	19%	15%	21%	21%	21%
45-54	17%	19%	15%	17%	15%	17%
55-64	15%	16%	21%	13%	8%	16%
65+	21%	27%	29%	14%	10%	20%

Table 2 **All respondents, breakdown by gender**

Gender	Total	Non-sharers	Sceptics	Pragmatists	Value hunters	Enthusiastic sharers
Male	49%	43%	51%	47%	53%	59%
Female	51%	57%	49%	53%	47%	41%

Table 3 **All respondents, breakdown by social grade**

Gender	Total	Non-sharers	Sceptics	Pragmatists	Value hunters	Enthusiastic sharers
A	7%	6%	5%	8%	9%	6%
B	19%	18%	18%	20%	21%	17%
C1	28%	30%	22%	27%	33%	24%
C2	20%	16%	20%	24%	20%	25%
D	4%	3%	4%	5%	4%	5%
E	18%	21%	24%	14%	11%	19%
Refused	4%	5%	6%	2%	2%	4%



# Notes

- 1 Ofcom, *Communications Market Report 2012*, Jul 2012, [http://stakeholders.ofcom.org.uk/binaries/research/cmr/cmr12/CMR\\_UK\\_2012.pdf](http://stakeholders.ofcom.org.uk/binaries/research/cmr/cmr12/CMR_UK_2012.pdf) (accessed 8 Aug 2012).
- 2 DMA, *Data Privacy: What the consumer really thinks 2012*, Direct Marketing Association, 2012, <http://tinyurl.com/bnsxxhq> (accessed 21 Aug 2012).
- 3 Ofcom, *Communications Market Report 2012*.
- 4 Ofcom, *Internet Use and Attitudes: 2012 Metrics Bulletin*, Jul 2012, [http://stakeholders.ofcom.org.uk/binaries/research/cmr/cmr12/2012\\_metrics\\_bulletin.pdf](http://stakeholders.ofcom.org.uk/binaries/research/cmr/cmr12/2012_metrics_bulletin.pdf) (accessed 8 Aug 2012); Ofcom, *Communications Market Report 2012*.
- 5 S Sengupta, 'Zuckerberg's unspoken law: sharing and more sharing', *New York Times*, 23 Sep 2011, <http://bits.blogs.nytimes.com/2011/09/23/zuckerbergs-unspeaken-law-sharing-and-more-sharing/> (accessed 17 Apr 2012).
- 6 European Commission, *Attitudes on Data Protection and Electronic Identity in the European Union*, 2011.
- 7 Ofcom, *Adults' Media Use and Attitudes Report*, Mar 2012, <http://tinyurl.com/czbzovo> (accessed 8 Aug 2012).
- 8 Ofcom, *Internet Use and Attitudes: 2012*.
- 9 CCP, *Online Personal Data: The consumer perspective 2011*, Communications Consumer Panel, [www.communicationsconsumerpanel.org.uk/Online%20personal%20data%20final%20240511.pdf](http://www.communicationsconsumerpanel.org.uk/Online%20personal%20data%20final%20240511.pdf) (accessed 21 Aug 2012).

- 10 Ofcom, *Communications Market Report 2012*; M Wind-Cowie and R Lekhi, *The Data Dividend*, London: Demos, 2012, [www.demos.co.uk/files/The\\_Data\\_Dividend\\_-\\_web.pdf](http://www.demos.co.uk/files/The_Data_Dividend_-_web.pdf) (accessed 9 Aug 2012)
- 11 J Jarvis, 'Mark Zuckerberg's masterplan for the "sharing economy"', *Guardian*, 2 Feb 2012, [www.guardian.co.uk/technology/2012/feb/02/mark-zuckerberg-sharing-economy](http://www.guardian.co.uk/technology/2012/feb/02/mark-zuckerberg-sharing-economy) (accessed 17 Apr 2012).
- 12 This is an estimate of IDC, a technology research firm. See S Lohr, 'The age of big data', *New York Times*, 12 Feb 2012, [www.nytimes.com/2012/02/12/sunday-review/big-datas-impact-in-the-world.html?\\_r=1&scp=1&sq=big%20data&st=cse](http://www.nytimes.com/2012/02/12/sunday-review/big-datas-impact-in-the-world.html?_r=1&scp=1&sq=big%20data&st=cse) (accessed 17 Apr 2012). For a powerful if controversial description of the 'Petabyte Age', see C Anderson, 'The end of theory: the data deluge makes the scientific method obsolete', *Wired*, 23 Jun 2008, [www.wired.com/science/discoveries/magazine/16-07/pb\\_theory](http://www.wired.com/science/discoveries/magazine/16-07/pb_theory) (accessed 17 Apr 2012).
- 13 World Economic Forum, *Rethinking Personal Data: Strengthening trust*, May 2012, [www3.weforum.org/docs/WEF\\_IT\\_RethinkingPersonalData\\_Report\\_2012.pdf](http://www3.weforum.org/docs/WEF_IT_RethinkingPersonalData_Report_2012.pdf) (accessed 8 Aug 2012)
- 14 C Kalapesi, S Willersdorf and P Zwillenberg, *The Connected Kingdom: How the internet is transforming the UK economy*, Boston Consulting Group, 2010, [www.connectedkingdom.co.uk/downloads/bcg-the-connected-kingdom-oct-10.pdf](http://www.connectedkingdom.co.uk/downloads/bcg-the-connected-kingdom-oct-10.pdf) (accessed 21 Aug 2012).
- 15 Ofcom, *International Communications Market Report*, 2010.
- 16 C David, 'Letter to government departments on opening up data', HM Government, 31 May 2010, [www.number10.gov.uk/news/letter-to-government-departments-on-opening-up-data/](http://www.number10.gov.uk/news/letter-to-government-departments-on-opening-up-data/) (accessed 9 Aug 2012).

- 17 Wind-Cowie and Lekhi, *The Data Dividend*, London: Demos, 2012, [www.demos.co.uk/files/The\\_Data\\_Dividend\\_-\\_web.pdf](http://www.demos.co.uk/files/The_Data_Dividend_-_web.pdf) (accessed 9 Aug 2012).
- 18 C Arthur, 'Google to pay record \$22.5m fine to FTC over Safari tracking', *Guardian*, 9 Aug 2012, [www.guardian.co.uk/technology/2012/aug/09/google-record-fine-ftc-safari](http://www.guardian.co.uk/technology/2012/aug/09/google-record-fine-ftc-safari) (accessed 13 Aug 2012).
- 19 I Falque-Pierrotin, letter to Google CEO Larry Page from president of CNIL, 27 Feb 2012, <http://tinyurl.com/8yxepsq> (accessed 16 Mar 2012); I Falque-Pierrotin, letter to Google CEO Larry Page from president of CNIL, 16 Mar 2012, <http://tinyurl.com/7ar8xtp> (accessed 16 March 2012).
- 20 'UK's families put on fraud alert', BBC News, 20 Nov 2007, [http://news.bbc.co.uk/1/hi/uk\\_politics/7103566.stm](http://news.bbc.co.uk/1/hi/uk_politics/7103566.stm) (accessed 13 Aug 2012).
- 21 European Commission, *Data Protection in the European Union: Citizens' perceptions*, European Commission Analytical Report, Eurobarometer 225, Feb 2008, [http://ec.europa.eu/public\\_opinion/flash/fl\\_225\\_en.pdf](http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf) (accessed 13 Aug 2012).
- 22 PricewaterhouseCoopers LLP, *Research into Consumer Understanding and Management of Internet Cookies and the Potential Impact of the EU Electronic Communications Framework*, commissioned by the Dept for Culture, Media and Sport, 2011.
- 23 Ofcom, *Adults' Media Use and Attitudes Report*.
- 24 CCP, *Online Personal Data*.
- 25 Privacy International, EPIC and CMCS, *European Privacy and Human Rights*, Privacy International, Electronic Privacy Information Center and Center for Media and Communications Studies, 2010, <https://www.privacyinternational.org/sites/privacyinternational.org/files/file-downloads/ephr.pdf> (accessed 13 Aug 2012).

- 26 See D Boyd and E Hargittai, 'Facebook privacy settings: who cares?', *First Monday* 15, no 8, 2010, <http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3086/2589> (accessed 17 Apr 2012); C Edwards and C Fieschi (eds), *UK Confidential*, London: Demos, 2008, p 20, [www.demos.co.uk/publications/ukconfidential](http://www.demos.co.uk/publications/ukconfidential) (accessed 17 Apr 2012); European Commission, *Attitudes on Data Protection and Electronic Identity in the European Union*; R Henry and C Flyn, 'Tap, tap, tapping us all up – mobile apps invade privacy', *Sunday Times*, 26 Feb 2012. This is related to the Eurobarometer data that found that 58 per cent of UK respondents read privacy statements on the internet.
- 27 CCP, *Online Personal Data*.
- 28 Ctrl Shift, *Tracking the Control Shift*, briefing report, 2011, [www.ctrl-shift.co.uk/about\\_us/news/2011/06/02/tracking-the-control-shift-the-consumer-view/](http://www.ctrl-shift.co.uk/about_us/news/2011/06/02/tracking-the-control-shift-the-consumer-view/) (accessed 28 Aug 2012).
- 29 SMSR and ICO, *Report on the Findings of the Information Commissioner's Office Annual Tract 2011 – Individuals, Social and Market Strategic Research and the Information Commissioner's Office*, Oct 2011.
- 30 Ofcom, *Adults' Media Use and Attitudes Report*.
- 31 CCP, *Online Personal Data*.
- 32 Ctrl Shift, *Tracking the Control Shift*.
- 33 World Economic Forum, *Advancing Cloud Computing: What to do now? Priorities for industry and governments*, 2011, [www3.weforum.org/docs/WEF\\_IT\\_AdvancedCloudComputing\\_Report\\_2011.pdf](http://www3.weforum.org/docs/WEF_IT_AdvancedCloudComputing_Report_2011.pdf) (accessed 8 Aug 2012).
- 34 World Economic Forum, *Rethinking Personal Data: Strengthening trust*, May 2012, [www3.weforum.org/docs/WEF\\_IT\\_RethinkingPersonalData\\_Report\\_2012.pdf](http://www3.weforum.org/docs/WEF_IT_RethinkingPersonalData_Report_2012.pdf) (accessed 8 Aug 2012).

- 35 V Reding, 'The EU data protection reform 2012: making Europe the standard setter for modern data protection rules in the digital age', speech, Innovation Conference Digital, Life, Design, Munich, 22 Jan 2012, [http://ec.europa.eu/commission\\_2010-2014/reding/pdf/speeches/s1226\\_en.pdf](http://ec.europa.eu/commission_2010-2014/reding/pdf/speeches/s1226_en.pdf) (accessed 9 Aug 2012).
- 36 European Commission, *Proposal for a Regulation of the European Parliament and on the of the Council of the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data*, Brussels, Jan 2012, [http://ec.europa.eu/justice/data-protection/document/review2012/com\\_2012\\_11\\_en.pdf](http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf) (accessed 9 Aug 2012); Reding, 'The EU data protection reform 2012'.
- 37 ICO, *Guidance on the Rules on Use of Cookies and Similar Technologies*, Privacy and Electronic Communications Regulations, Information Commissioner's Office, May 2011.
- 38 J Shapiro, 'Google Dashboard changes our thinking about privacy', blogpost, 10 Nov 2009, <http://tinyurl.com/ckhyarz> (accessed 14 Aug 2012); 'Facebook u-turns on phone and address data sharing', BBC Technology, 18 Jan 2011, [www.bbc.co.uk/news/technology-12214628](http://www.bbc.co.uk/news/technology-12214628) (accessed 14 Aug 2012).
- 39 ICO, *The Privacy Dividend: The business case for investing in proactive privacy protection*, Information Commissioner's Office, 2010, [www.ico.gov.uk/news/current\\_topics/privacy\\_dividend.aspx](http://www.ico.gov.uk/news/current_topics/privacy_dividend.aspx) (accessed 21 Aug 2012).
- 40 CCP, *No One Should Miss Out: Consumers say what they want from the digital future*, Communications Consumer Panel, 2009, <http://preview.tinyurl.com/bsv6txx> (accessed 21 Aug 2012).
- 41 Ctrl Shift, *The New Personal Data Landscape*, Nov 2011, <http://ctrl-shift.co.uk/wordpress/wp-content/uploads/2011/11/The-new-personal-data-landscape-FINAL.pdf> (accessed 9 Aug 2012); Ofcom, *Communications Market Report 2012*.
- 42 Ctrl Shift, *The New Personal Data Landscape*.

- 43 One example is the Department for Children, Schools and Families' 2009 study *Parents and Internet Safety: Report from HCI discussion groups 27 April – 1 May 2009*, 2009, <http://tinyurl.com/d43p4m2> (accessed 21 Aug 2012), which was based on ten in-depth discussion groups.
- 44 ICO, 'Information rights research', Information Commissioner's Office, 2012, [www.ico.gov.uk/about\\_us/research/information\\_rights.aspx](http://www.ico.gov.uk/about_us/research/information_rights.aspx) (accessed 22 Aug 2012). A few significant, large-scale, representative polls have been undertaken on the subject. CCP's 'Online Personal Data', for example, is based on a representative sample of 1,000 UK adults (aged 16+), while the Oxford Internet Institute's annual and occasional polls, such as WH Dutton and G Blank's *The Next Generation Users: The internet in Britain*, 2011, are usually based on large representative samples (in this case 2,000 adults aged 16+). The ICO also produces an annual tracker survey, based on a representative sample of over 1,000 UK adults. For example, PricewaterhouseCoopers LLP's 2011 study *Research into Consumer Understanding and Management of Internet Cookies and the Potential Impact of the EU Electronic Communications Framework* was based on an online survey of 4,116 children of primary school and secondary school age. Again, this is extremely valuable for developing insight into those populations, but less good at setting out the broader picture. Other polls, although providing some insightful data, were not based on representative samples, sometimes skewed towards intensive internet users, which is often the case with internet-based polls.
- 45 Participants were recruited as members of four of the segments identified in the research: sceptics, enthusiastic sharers, unsubscribers, and 'make me an offer' and included a broad range of age, gender and social grade.

- 46 Populus asked respondents to rank on a scale of 0–10 the extent to which they agreed with the following statement: ‘the information involved here isn’t really private data’ in reference to each of the options given, on a scale where 0 means ‘completely disagree’ and 10 means ‘completely agree’. Participants who responded with 8, 9 or 10 were classified as viewing the option as ‘personal’.
- 47 Populus asked respondents to rank on a scale of 0–10 the extent to which they agreed with the following statement: ‘I did not know data were used in this way’ in reference to each of the options given, on a scale where 0 means ‘completely disagree’ and 10 means completely agree. Participants who responded with 8, 9 or 10 were classified as having answered that they did know.
- 48 Populus asked respondents to rank on a scale of 0–10 the extent to which they agreed with the following statement: ‘I can see what consumers gain from data being used in this way’ in reference to each of the options given, on a scale where 0 means ‘completely disagree’ and 10 means completely agree. Participants who responded with 8, 9 or 10 were classified as having answered that they could see what consumers gained.
- 49 Populus asked respondents to rank on a scale of 0–10 the extent to which they agreed with the following statement: ‘I’m comfortable with my data being used in this way’ in reference to each of the options given, on a scale where 0 means ‘completely disagree’ and 10 means completely agree. Participants who responded with 8, 9 or 10 were classified as having answered that they were comfortable with their data being used in that way.
- 50 V Trench, ‘Who wins with supermarket loyalty cards?’, BBC News, 8 Feb 2010, <http://news.bbc.co.uk/1/hi/business/8505031.stm> (accessed 21 Aug 2012); ‘UK and France most engaged with email sites in Europe’, comScore Data Mine, 26 Jun 2012, [www.comscore.com/2012/06/uk-and-france-most-engaged-with-email-sites-in-europe/](http://www.comscore.com/2012/06/uk-and-france-most-engaged-with-email-sites-in-europe/) (accessed 21 Aug 2012).

- 51 Populus asked respondents to think about data and privacy, and rank on a scale of 0–10 how large or small a concern each of 12 concerns were to them personally, where 10 means it is a very major concern, and 0 means it is not at all concerning. Participants who responded with 8, 9 or 10 were classified as viewing the option as a concern.
- 52 Populus asked respondents to rank on a scale of 0–10 whether each measure would make them more comfortable about their data being used, where 10 means ‘makes you much more comfortable’ and 0 means ‘makes no difference’. If respondents answered 8, 9, or 10 they were classified as being reassured by the measure in question.
- 53 Wind-Cowie and Lekhi, *The Data Dividend*.

## References

Anderson C, 'The end of theory: the data deluge makes the scientific method obsolete', *Wired*, 23 Jun 2008, [www.wired.com/science/discoveries/magazine/16-07/pb\\_theory](http://www.wired.com/science/discoveries/magazine/16-07/pb_theory) (accessed 17 Apr 2012).

Arthur C, 'Google to pay record \$22.5m fine to FTC over Safari tracking', *Guardian*, 9 Aug 2012, [www.guardian.co.uk/technology/2012/aug/09/google-record-fine-ftc-safari](http://www.guardian.co.uk/technology/2012/aug/09/google-record-fine-ftc-safari) (accessed 13 Aug 2012).

Boyd D and Hargittai E, 'Facebook privacy settings: who cares?', *First Monday* 15, no 8, 2010, <http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3086/2589> (accessed 17 Apr 2012).

CCP, *No One Should Miss Out: Consumers say what they want from the digital future*, Communications Consumer Panel, 2009, <http://preview.tinyurl.com/bsv6txx> (accessed 21 Aug 2012).

CCP, *Online Personal Data: The consumer perspective 2011*, Communications Consumer Panel, [www.communicationsconsumerpanel.org.uk/Online%20persona1%20data%20final%20240511.pdf](http://www.communicationsconsumerpanel.org.uk/Online%20persona1%20data%20final%20240511.pdf) (accessed 21 Aug 2012).

Ctrl Shift, *The New Personal Data Landscape*, Nov 2011, <http://ctrl-shift.co.uk/wordpress/wp-content/uploads/2011/11/The-new-personal-data-landscape-FINAL.pdf> (accessed 9 Aug 2012).

Ctrl Shift, *Tracking the Control Shift*, briefing report, 2011, [www.ctrl-shift.co.uk/about\\_us/news/2011/06/02/tracking-the-control-shift-the-consumer-view/](http://www.ctrl-shift.co.uk/about_us/news/2011/06/02/tracking-the-control-shift-the-consumer-view/) (accessed 28 Aug 2012).

## References

David C, 'Letter to government departments on opening up data', HM Government, 31 May 2010, [www.number10.gov.uk/news/letter-to-government-departments-on-opening-up-data/](http://www.number10.gov.uk/news/letter-to-government-departments-on-opening-up-data/) (accessed 9 Aug 2012).

DCSF, *Parents and Internet Safety: Report from HCI discussion groups 27 April – 1 May 2009*, Department for Children, Schools and Families, 2009, <http://tinyurl.com/d43p4m2> (accessed 21 Aug 2012), which was based on ten in-depth discussion groups.

DMA, *Data Privacy: What the consumer really thinks 2012*, Direct Marketing Association, 2012, <http://tinyurl.com/bnsxxhq> (accessed 21 Aug 2012).

Dutton WH and Blank G, *The Next Generation Users: The internet in Britain*, Oxford Internet Institute, 2011.

Edwards C and Fieschi C (eds), *UK Confidential*, London: Demos, 2008, p 20, [www.demos.co.uk/publications/ukconfidential](http://www.demos.co.uk/publications/ukconfidential) (accessed 17 Apr 2012).

European Commission, *Attitudes on Data Protection and Electronic Identity in the European Union*, 2011.

European Commission, *Data Protection in the European Union: Citizens' perceptions*, European Commission Analytical Report, Eurobarometer 225, Feb 2008, [http://ec.europa.eu/public\\_opinion/flash/fl\\_225\\_en.pdf](http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf) (accessed 13 Aug 2012).

European Commission, *Proposal for a Regulation of the European Parliament and on the Council of the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data*, Brussels, Jan 2012, [http://ec.europa.eu/justice/data-protection/document/review2012/com\\_2012\\_11\\_en.pdf](http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf) (accessed 9 Aug 2012).

'Facebook u-turns on phone and address data sharing', BBC Technology, 18 Jan 2011, [www.bbc.co.uk/news/technology-12214628](http://www.bbc.co.uk/news/technology-12214628) (accessed 14 Aug 2012).

Falque-Pierrotin I, letter to Google CEO Larry Page from president of CNIL, 27 Feb 2012, <http://tinyurl.com/8yxepsq> (accessed 16 Mar 2012).

Falque-Pierrotin I, letter to Google CEO Larry Page from president of CNIL, 16 Mar 2012, <http://tinyurl.com/7ar8xtp> (accessed 16 March 2012).

Henry R and Flyn C, ‘Tap, tap, tapping us all up – mobile apps invade privacy’, *Sunday Times*, 26 Feb 2012.

ICO, *Guidance on the Rules on Use of Cookies and Similar Technologies*, Privacy and Electronic Communications Regulations, Information Commissioner’s Office, May 2011.

ICO, ‘Information rights research’, Information Commissioner’s Office, 2012, [www.ico.gov.uk/about\\_us/research/information\\_rights.aspx](http://www.ico.gov.uk/about_us/research/information_rights.aspx) (accessed 22 Aug 2012).

ICO, *The Privacy Dividend: The business case for investing in proactive privacy protection*, Information Commissioner’s Office, 2010, [www.ico.gov.uk/news/current\\_topics/privacy\\_dividend.aspx](http://www.ico.gov.uk/news/current_topics/privacy_dividend.aspx) (accessed 21 Aug 2012).

Jarvis J, ‘Mark Zuckerberg’s masterplan for the “sharing economy”’, *Guardian*, 2 Feb 2012, [www.guardian.co.uk/technology/2012/feb/02/mark-zuckerberg-sharing-economy](http://www.guardian.co.uk/technology/2012/feb/02/mark-zuckerberg-sharing-economy) (accessed 17 Apr 2012).

Kalapesi C, Willersdorf S and Zwillenberg P, *The Connected Kingdom: How the internet is transforming the UK economy*, Boston Consulting Group, 2010, [www.connectedkingdom.co.uk/downloads/bcg-the-connected-kingdom-oct-10.pdf](http://www.connectedkingdom.co.uk/downloads/bcg-the-connected-kingdom-oct-10.pdf) (accessed 21 Aug 2012).

Lohr S, ‘The age of big data’, *New York Times*, 12 Feb 2012, [www.nytimes.com/2012/02/12/sunday-review/big-datas-impact-in-the-world.html?\\_r=1&scp=1&sq=big%20data&st=cse](http://www.nytimes.com/2012/02/12/sunday-review/big-datas-impact-in-the-world.html?_r=1&scp=1&sq=big%20data&st=cse) (accessed 17 Apr 2012).

## References

Ofcom, *Adults' Media Use and Attitudes Report*, Mar 2012, <http://tinyurl.com/czbzovo> (accessed 8 Aug 2012).

Ofcom, *Communications Market Report 2012*, 2012, [http://stakeholders.ofcom.org.uk/binaries/research/cmr/cmr12/CMR\\_UK\\_2012.pdf](http://stakeholders.ofcom.org.uk/binaries/research/cmr/cmr12/CMR_UK_2012.pdf) (accessed 8 Aug 2012).

Ofcom, *International Communications Market Report*, 2010.

Ofcom, *Internet Use and Attitudes: 2012 Metrics Bulletin*, Jul 2012, [http://stakeholders.ofcom.org.uk/binaries/research/cmr/cmr12/2012\\_metrics\\_bulletin.pdf](http://stakeholders.ofcom.org.uk/binaries/research/cmr/cmr12/2012_metrics_bulletin.pdf) (accessed 8 Aug 2012).

PricewaterhouseCoopers LLP, *Research into Consumer Understanding and Management of Internet Cookies and the Potential Impact of the EU Electronic Communications Framework*, commissioned by the Dept for Culture, Media and Sport, 2011.

Privacy International, EPIC and CMCS, *European Privacy and Human Rights*, Privacy International, Electronic Privacy Information Center and Center for Media and Communications Studies, 2010, <https://www.privacyinternational.org/sites/privacyinternational.org/files/file-downloads/ephr.pdf> (accessed 13 Aug 2012).

Reding V, 'The EU data protection reform 2012: making Europe the standard setter for modern data protection rules in the digital age', speech, Innovation Conference Digital, Life, Design, Munich, 22 Jan 2012, [http://ec.europa.eu/commission\\_2010-2014/reding/pdf/speeches/s1226\\_en.pdf](http://ec.europa.eu/commission_2010-2014/reding/pdf/speeches/s1226_en.pdf) (accessed 9 Aug 2012).

Sengupta S, 'Zuckerberg's unspoken law: sharing and more sharing', *New York Times*, 23 Sep 2011, <http://bits.blogs.nytimes.com/2011/09/23/zuckerbergs-unspoken-law-sharing-and-more-sharing/> (accessed 17 Apr 2012).

Shapiro J, 'Google Dashboard changes our thinking about privacy', blogpost, 10 Nov 2009, <http://tinyurl.com/ckhyarz> (accessed 14 Aug 2012).

SMSR and ICO, *Report on the Findings of the Information Commissioner's Office Annual Tract 2011 – Individuals, Social and Market Strategic Research and the Information Commissioner's Office*, Oct 2011.

Trench V, 'Who wins with supermarket loyalty cards?', BBC News, 8 Feb 2010, <http://news.bbc.co.uk/1/hi/business/8505031.stm> (accessed 21 Aug 2012).

'UK and France most engaged with email sites in Europe', comScore Data Mine, 26 Jun 2012, [www.comscoredata.com/2012/06/uk-and-france-most-engaged-with-email-sites-in-europe/](http://www.comscoredata.com/2012/06/uk-and-france-most-engaged-with-email-sites-in-europe/) (accessed 21 Aug 2012).

'UK's families put on fraud alert', BBC News, 20 Nov 2007, [http://news.bbc.co.uk/1/hi/uk\\_politics/7103566.stm](http://news.bbc.co.uk/1/hi/uk_politics/7103566.stm) (accessed 13 Aug 2012).

Wind-Cowie M and Lekhi R, *The Data Dividend*, London: Demos, 2012, [www.demos.co.uk/files/The\\_Data\\_Dividend\\_-\\_web.pdf](http://www.demos.co.uk/files/The_Data_Dividend_-_web.pdf) (accessed 9 Aug 2012).

World Economic Forum, *Advancing Cloud Computing: What to do now? Priorities for industry and governments*, 2011, [www3.weforum.org/docs/WEF\\_IT\\_AdvancedCloudComputing\\_Report\\_2011.pdf](http://www3.weforum.org/docs/WEF_IT_AdvancedCloudComputing_Report_2011.pdf) (accessed 8 Aug 2012).

World Economic Forum, *Rethinking Personal Data: Strengthening Trust*, May 2012, [www3.weforum.org/docs/WEF\\_IT\\_RethinkingPersonalData\\_Report\\_2012.pdf](http://www3.weforum.org/docs/WEF_IT_RethinkingPersonalData_Report_2012.pdf) (accessed 8 Aug 2012).

## 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 authorised 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, dramatisation, fictionalisation, 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 here under. You may not sublicense 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 Licensor 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 towards 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 towards 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 utilising 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 licenced 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.



This project was supported by:

O<sub>2</sub>

We live in an age of sharing. As consumers and online, we regularly share personal information, and generate new data through our browsing or purchasing history. Businesses and government are increasingly aware of the value of this information, which can result in better and cheaper services for customers, new sources of income for businesses and improved public services. But the question of who owns this information, and how it is collected, stored and used, is becoming a major consumer rights issue. It is crucial, therefore, that people are at the heart of any new settlement.

*The Data Dialogue* sets out the results of the largest ever poll of public attitudes on personal information and data-sharing. Based on a representative sample of 5,000 adults, the report finds a growing crisis in consumer confidence over how government and business handle personal data, and discomfort about the way in which personal information and data are currently being used.

The report argues that this loss of confidence could have a knock-on effect on the economy and on the quality of services available to consumers. However, it also finds that views about sharing change when people are given more control and choice about what data is shared, and when the benefit of sharing that data is made clear to them. It therefore suggests that consumers should be engaged in an honest dialogue about how data are collected and used, and be given meaningful choice and control over the information they share. That will be good for business and consumers alike.

Jamie Bartlett is a senior researcher at Demos.

ISBN 978-1-909037-16-6 £10

© Demos 2012

