citizens
advice
bureau

# Personal data empowerment

## Time for a fairer data deal?

## Our aims

- Provide the advice people need for the problems they face.
- Improve the policies and practices that affect people's lives.

## Our principles

The Citizens Advice service provides free, independent, confidential and impartial advice to everyone on their rights and responsibilities.
We value diversity, promote equality and challenge discrimination.

Written by Liz Coll
April 2015

**If you require this publication in an alternative format please contact us**

3rd Floor North
200 Aldersgate
London EC1A 4HD
Tel: 03000 231 231

www.citizensadvice.org.uk

For more information contact: liz.coll@citizensadvice.org.uk

Citizens Advice is an operating name of
The National Association of Citizens Advice Bureaux.

Registered charity number 279057
Published April 2015

## Contents

**Executive summary** ..........4

**1 Introduction** ..........6

1.1 Document purpose ..........6

1.2 Document map ..........6

1.3 Audience ..........6

1.4 Scope of report ..........7

**2 The new data context: a changing personal data landscape** ..........9

2.1 The data-driven economy from a consumer perspective ..........9

2.2 What this means for consumers ..........13

2.3 Consumer perspective on the current situation ..........14

**3 Defining the problem** ..........21

3.1 Limits of consent tools .......... ......21

3.2 Lack of consumer voice ..........24

**4 Emerging alternatives to the status quo** ..........26

4.1 Personal data empowerment ..........26

4.2 Opportunities and risks of personal data empowerment ..........37

4.3 Implications of a new approach ..........45

**5 Articulating a new approach** ..........50

5.1 The need for a new vision ..........50

5.2 A new vision and guiding principles ..........51

5.3 Realising the vision ..........52

**6 Conclusion** ..........53

**7 Methodology of research** ..........54

**8 Bibliography** ..........56

## Executive summary

Personal data issues have risen in complexity and scale over the last 5-10 years. Aggregation, sharing and analysis are becoming readily available to organisations and individuals via new tools and services. There are opportunities for consumers to apply insight from personal data to become more empowered, as well as exercise their rights to privacy and control. Yet the personal data explosion brings huge risks too, and campaigners are all too often left playing catch up with the powerful companies who are pushing at the boundaries with new developments and dominating the conversation about our understanding of consumer attitudes and responses to change.

The attention of consumer and privacy advocates has rightly been focused on identifying and mitigating risks, and we wholeheartedly support the resolute consumer advocacy during the negotiation process over EU data protection regulations, making sure crucial lines are held and key protections are strengthened. However, while focusing on mitigating current risks, we must not lose sight of the potential for consumers to utilise and share their data in new ways to unlock value and enable better outcomes.

Our work with consumers, businesses and regulators makes us acutely aware that a new vision for personal data empowerment, built around consumer attitudes and values, is required. The key factors driving this are:

- disillusionment with the status quo and lack of faith in the notice and consent model to reassure trust
- ties to the dominant business model of data gathering and sale as the only way to run digital services
- the potential for data to empower consumers towards better outcomes
- the consumer appetite for data sharing under particular conditions
- the complexities of consumer attitudes towards privacy and personal data, and the lack of means to express this
- low awareness of more imaginative ways to control and manage personal data.

We feel that now is the right time to articulate a fresh vision of personal data empowerment: one that sees the value of data shared more evenly amongst both the consumers who generate data and the organisations that use it; one that balances safeguards with the ability to innovate and one that contributes towards a more stable personal data ecosystem that better serves consumers in the 21st century.

This report will present an analysis of the data-driven economy from a consumer perspective, together with the results of qualitative research undertaken with leading thinkers, regulators, policy makers and practitioners, and an analysis of new emerging trends in personal data empowerment.

All of this insight has culminated in the development of the new vision and approach to personal data detailed overleaf, which we hope will start to make a fairer data deal for consumers a reality.

## Personal data empowerment: vision and guiding principles

**Vision:**

Consumers are able to exert meaningful control over their personal data.
They can determine how data about them and created by them is used and the benefits they wish to derive, within a trusted and safe system.

**Guiding principles:**

- Personal data can empower consumers towards better individual and collective outcomes – this should be given as much attention as the potential risks and detriments.
- Consumers have an appetite for greater personal data sharing and aggregation but they want a fair value exchange – they should be able to get a clear benefit from sharing their personal data.
- The ability and means to gain a benefit from sharing personal data should be accessible to all consumers, and contribute towards challenging wider detriment
- Consumers want to control how their data is used and by whom – these choices should be organised around an individual's personal preferences, not the organisation's needs.
- Organisations should be transparent in their use of data - information should be accessible and clear so consumers can easily understand what is happening with their data
- Organisations should recognise the importance of transparency in showing they can be trusted to handle personal data – their business model, security standards and lines of accountability should be obvious so that consumers can easily establish whether they meet their trust requirements.
- Consumers' information and data protection rights must be properly enforced and upheld
- Mechanisms to manage privacy and consent should be designed to reflect actual behaviours, not those of the legislators' and regulators' idealised consumer, or data gatherers' convenience.

# 1 Introduction

## 1.1 Document purpose

The purpose of this report is to articulate a vision and set of guiding principles and ideas for the consumer-centred use of personal data. The vision is based on the concept of ‘personal data empowerment’. This concept allows for a wider consideration of the relationship between consumers and their personal data, looking beyond the basic need for mitigating risks to consider the potential for innovative opportunities, with appropriate safeguards designed around consumers’ individual rights, trust requirements, and informed choices about data use. The guiding principles are drawn from insights within the report. Together, the vision and guiding principles form a new approach to personal data; one that we believe will bring benefits to consumers, businesses and governments alike.

## 1.2 Document map

The report will begin by setting the context with an overview of the data-driven economy, followed by an attempt to distil the core problems for consumers in managing their personal data. It will also consider why the existing policy and regulatory mechanisms have been unable to provide an adequate solution to these.

It then explores the emerging tools and services offering personal data empowerment to consumers, and considers the alternative solutions these may offer for the future of personal data and privacy management. This is followed by a review of the risks and opportunities of the current market and new alternatives, based on original qualitative research with policy makers, regulators, practitioners and campaigners. It concludes with the articulation of a vision and guiding principles, rooted in the consumer interest, to guide activity and thinking on personal data, and considers what the roles for key players in this space might be, in order to bring this vision to fruition.

## 1.3 Audience

This report calls on interested companies and those working in the consumer interest via regulation, advocacy or policy to consider a new way to understand and manage the value of personal data, and the importance of trust relationships within that. It is primarily aimed at:

- Businesses: forward-thinking businesses wanting to engender better, deeper relationships with their customers in the new data-driven era can use the vision and guiding ideas to shape their strategy and activity towards a more balanced value exchange.
- Policy makers and regulators: new solutions to personal data issues are required, this report sets out the consumer case for these and a vision and set of guiding ideas that can form the basis of policy discussions.

- Organisations working in the consumer interest: consumer advocates have an excellent opportunity to enable consumers to take a bigger share in the value of their data. However, in order to do this, they will need to understand and communicate the risks of new technology, and how to balance privacy rights with innovation, within the wider context.

## 1.4 Scope of report

Multiple aspects of data use and management will inevitably impact on consumers, given the depth and breadth of the data-driven economy. These include:

- access to and application of insights from open data, with previously closed data sets opened up as a resource for consumers to hold companies to account (see, for example, the UK Regulator Network's paper, *The use of data publication to enable reputation regulation*)[1]
- the analysis of big data, combining information and aggregated data on consumption to derive insights and make decisions
- the increasing consciousness and concern around the way our personally identifiable information is collected and re-used.

There is an almost endless flow of ideas, surveys, visions and apocalyptic or utopian scenarios around these aspects, but in the interests of focus and clarity, this paper is focused on the final point. In particular, it will consider the intersection where consumers can be empowered by their data to better serve their individual and collective interests, whilst also remaining confident that their privacy choices will be upheld.

The focus on empowerment was driven by the recent work by Consumer Futures on consumers in the digital age, which ran from 2011 to 2014. This research and insight programme looked at the opportunities and risks of the new digital economy and explored how people might realise their consumer rights within this new context. Key insights can be found in *Realising Consumer Rights: from JFK to the digital age*,[2] and are summarised here:

**Increased individual access to computing and processing power**: Consumer-centred tools and services are much more widely available, thanks to an exponential growth in computing and processing power coupled with an inversely proportional fall in costs to consumers. This gives consumers powerful technology at their fingertips whenever it is required.

**Alternatives to regulation**: New and emerging forms of digital consumer empowerment can offer fresh ways to assert consumer rights that complement or even offer an alternative to traditional regulation and legislation routes.

[1] UK Regulators Network (2014)
[2] Coll L and Bates R (2014)

**Concept of technological change:** Technology has always created new contexts and disruptions, only now the pace of change is much more rapid. Dealing with risks and issues as they arise will no longer be enough to uphold consumer rights in the long term. Placing consumers at the centre of conversations about how technology and disruption can work in their interests is lacking.

**Changing roles for consumer bodies:** Those working in the consumer interest need to think carefully about their role in this new context and have a broader understanding about how they can best make an impact in the rapidly changing playing field on which citizens, consumers, businesses and government find themselves.

Of course, as the UK's leading consumer organisation, Citizens Advice must go beyond advocating for a policy and delivery approach that will achieve a fairer and more balanced data settlement. All our bureaux deal with personal data on a daily basis and our large central organisation is a data controller, subject to the data protection act with information and data policies, and in a position to set a high standard for data management.[3]

There is also a potential role for new activity with consumers that applies some of the personal data empowerment tools and services to give people better outcomes. These corporate and data application elements are not covered in this report but will be part of our ongoing development.

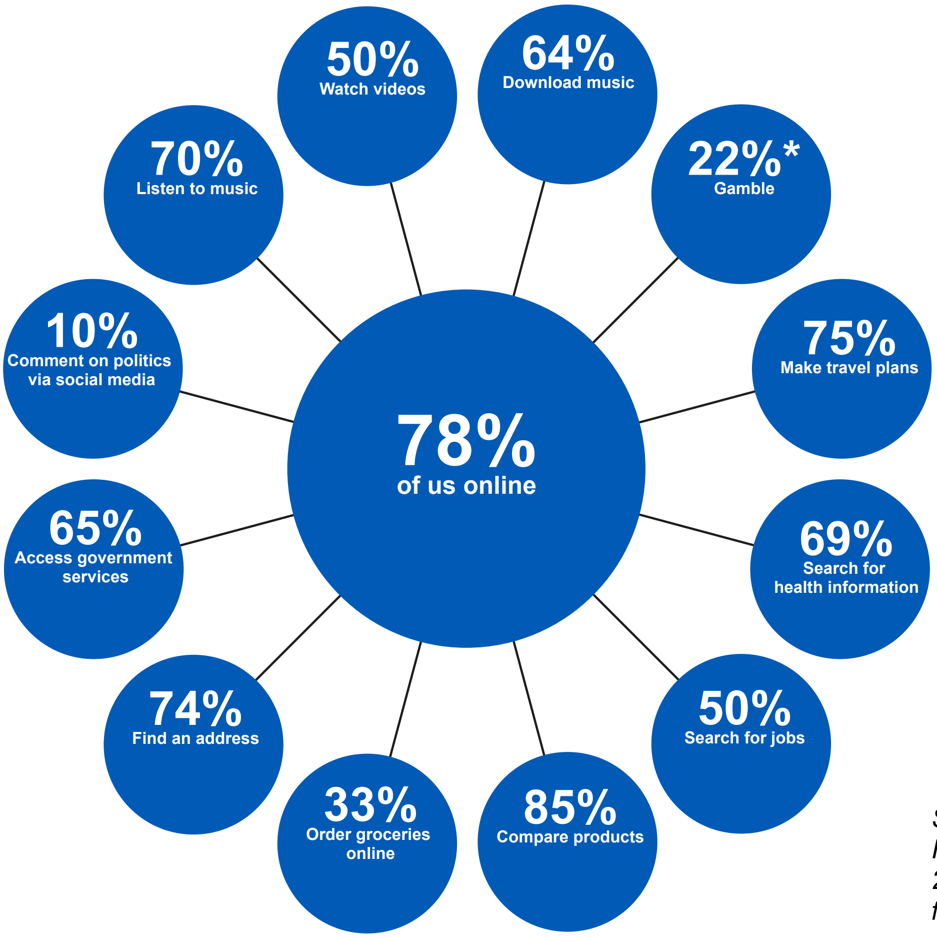
[3] http://www.citizensadvice.org.uk/index/disclaimer_copyright_privacy_cookies/privacy_cookies/information_charter.htm

# 2 The new data context: a changing personal data landscape

## 2.1 Overview of the data-driven economy from a consumer perspective

The personal data landscape has changed dramatically in recent years. More consumers are connected to the internet for more of the time, and for a wider range of activities. According to the latest Oxford Internet Survey, 78 per cent of the UK population aged over 14 accesses the internet, many of them via a mobile or tablet device.[4] Globally, 40 per cent of the world's population are predicted to be online by the end of 2014.[5] We are a nation of voracious researchers, purchasers, planners, creators, commentators and socialisers online.[6] Consumers are vocal, and are able to form useful alliances to demand more from providers, but they are also more visible, leaving a rapidly expanding digital footprint. Consumer activity leaves a far-reaching data trail, with mobile online access becoming the norm, and important location and app usage data is added to this trail.

**Figure 1: Regular online activity that leaves a data trail**

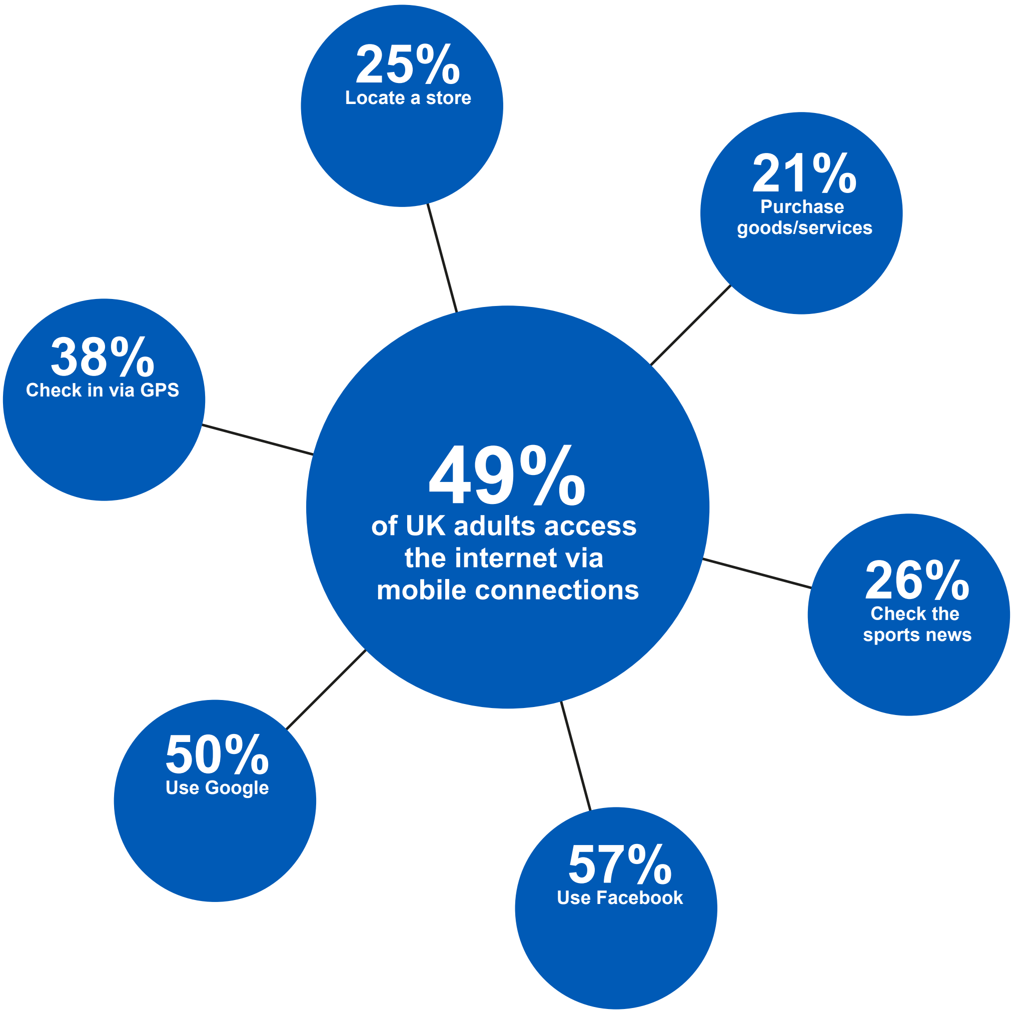


*Source: OXIS Cultures of the Internet Survey, 2013[1] survey of 2,657 UK respondents weighted for UK demographics*

** Self-reported figure*

[4] Oxford Internet Institute (2013)
[5] International Telecommunications Union (2014)
[6] Oxford Internet Institute (2013)

**Figure 2: Mobile connections: online access via mobile and smartphones**



*Source: Ofcom, The Communications Market 2013*[7]

The reduced costs of increased computing capability that put such powerful, social technology in our pockets have also cut down the cost for companies of processing information. This means that it is now possible for more types of businesses to collect and analyse a much deeper range of data on their customers. Take regulated industries in the UK as an example:

- In energy, the imminent arrival of smart meters is turning an industry that, in terms of customer data at least, has been relatively poor into one that is data-rich. This affects not only the value of the data but also its volume and sensitivity. Data about total

[7] Ofcom (2013)

energy use over a day or month is very different to data about energy use minute by minute, which can say a lot about people's lives and lifestyles.

- In the mobile sector, the proportion of consumers with a smartphone has doubled to 51 per cent in the last two years. That is creating an explosion of new data sources: not just about voice and text messages, but uses of data, app usage, online behaviours, transactions and, of course, location data.
- In banking there is the long-term shift from cash and cheques to plastic, to contactless and other payment systems: banking is being digitised, and the volume and variety of digital data that banks can now collect is expanding rapidly.

But beyond the expansion of the data that individual industries can collect about their customers, there is a more fundamental shift going on in relation to the way in which people use digital technology, primarily via the internet, that warrants attention. While the social, participatory web (or web 2.0) has empowered consumers in many ways (making more information available, giving consumers the ability to share their views and experiences), it has also *dis*-empowered them at the same time.[8] This is because most web 2.0 business models are predominantly advertising driven – built on the monetisation and commoditisation of personal data to improve targeting of adverts. Whilst there are growing questions around the effectiveness of this type of advertising (for example, almost half of the UK population are unhappy with targeted advertising),[9] the growth of this model coupled with an increase in the range of customer data has caught the attention of traditional players.

*Previously the supporting act of traditional product/ service provision, the collection and use of data is now the star of the show. This places the entire debate about personal data collection and use on a new footing.*

Whereas before, suppliers collected and used data for mainly operational reasons, such as service provision, billing and customer service, with elements of analytics and advertising/direct marketing built on top, we now see a reversal of emphasis with more and more traditional players attracted to the business opportunities of web 2.0 data monetisation models. The limitations of current regulations in managing this in the consumer interest are dealt with in section 3.

Looking ahead, we can establish a few firm possibilities for the future. We can expect to see the data explosion blurring old industry boundaries. For example, many now believe the future of payment systems lies with the mobile wallet, which points to some sort of convergence between the banking and telecommunications industries. Apple recently secured a banking licence, so it’s not too hard to imagine a smartphone taking on the function of a bank and payment system in the near future. The concept of the ‘smart home’, where every device is connected into a single home management system, brings together device manufacturers, utilities, software and communications companies in a battle to ‘own’ the customer relationship (with Google’s acquisition of automated home energy system *NEST* as a case in point). [10]

[8] Coll L and Bates R (2014), see part 1 for a full exploration of this
[9] Economist Intelligence Unit (2013)
[10] http://www.bbc.co.uk/news/business-25722666

## 2.2 What this means for consumers

### 2.2.1 Opportunities and potential

Mainstream access to digital technology has made new forms of consumer empowerment possible. The flood of data created by consumers, coupled with the opening up of information and easier access to powerful analytical tools, makes for a new space for services that enable consumers to achieve better outcomes.

These could mean making existing processes work better, for example, an assessment of spending patterns to meet new mortgage regulations based on permissioned access to bank account data. Or black box recorders in young drivers' cars that analyse driving behaviour, which can be reflected in appropriate insurance premiums. Or it could mean an intermediary stepping in to offer permissioned, automated switching to the best tariff at any one time, meaning an end to the time-consuming search and administration of switching providers.[11]. We're now well used to things like Amazon's recommendations based on other customers' searches, but this opening up of transactional data to push sales suggestions was once a novelty.

Such new forms of data-driven empowerment could be an additional tool for consumer advocates and advisors wanting to help drive better decisions. Services making use of personal data analysis could work alongside information and advice to relieve consumers of many of the choice burdens involved in complex markets. *Billmonitor* already offers a service that takes your actual usage data and recommends the cheapest tariff based on real-time use.[12]

Or it could create new possibilities; services could match personal data with other public administrative information such as criteria for benefits. For example, the *midata* i*nnovation lab* has produced a visual to show how personal information from energy suppliers, HMRC, DECC and DWP could help simplify access to energy entitlements such as discounts or subsidised insulation schemes.[13] This might help to increase the number of people accessing particular schemes, as barriers to entry are lowered.

At a macro level, the benefits of aggregating large amounts of open data such as travel patterns or health outcomes can bring deeper understanding of behaviours and better information on which to base investments or improve service planning. However, there is debate around whether the promised levels of privacy via anonymisation are actually possible, given the limited amount of information required to re-identify someone.[14]

So for consumers, this creates a dilemma: new data sources open up rich new opportunities for different types of services that could make decisions or actions easier, but the complexities and pitfalls of managing this data creates the potential for new forms of risk,

[11] Bates R (2014)
[12] www.billmonitor.com
[13] www.midatalab.org.uk
[14] Ohm P (2009)

inconvenience and disadvantage. These might include people with a poor credit or insurance history being more easily flagged and therefore finding it hard to access services.

### 2.2.2 Risks and detriments

There is a broad set of real and potential detriments that now routinely affect consumers or cause them concern. We'll look in detail at consumer awareness and attitudes with regards to the current data set-up and these detriments in section 2.3.2, but for now the focus will be on the actual issues. Detriments go far beyond personal data being exchanged in an opaque way, and other issues include: having to remember multiple passwords for different sites and services, having to re-enter the same information repeatedly for different providers, fear of data getting into the wrong hands and the consequences of data breaches, for example, financial loss due to identity fraud. Frauds where criminals misuse the personal data of victims affect around 150,000 consumers each year, and account for 60 per cent of all fraud in the UK.[15] While there is currently no correlation between data breaches and identity theft for the UK,[16] in the US there is research suggesting that up to 35 per cent of known identity thefts are caused by corporate data breaches.[17]

These detriments are not just a problem for affluent digital natives, signing up to apps and tools online. Poor access and control of personal data can affect everyone through things like credit scoring or accessing means-tested state entitlements, or targeting for cold calling and deliberate mis-selling of inappropriate products to susceptible people.

The question of future detriments and risks must also be addressed; without knowing exactly what's possible in the future, we are now very familiar with the speed at which technology moves and new uses emerge, and this causes anxiety. Young people are already finding out the consequences of a visible social life when moving into positions of more responsibility.[18] We are also familiar with 'mission creep', such as surveillance powers being used in circumstances for which they were not designed. An example of this is the case of a local council using the Regulation of Investigatory Powers Act (RIPA) 2000 legislation to determine whether families were in the declared catchment area for a school.[19]

## 2.3 Consumer perspective on the current situation

### 2.3.1 Challenges in identifying the consumer perspective

"*The internet is the one technology above all others that has enabled the transformation of the consumer experience in unprecedented ways*"[20]

Simultaneously empowering and disempowering, it is the deep-rooted shift in context brought about by the digital age that makes it so difficult to pull out a neat distillation of the consumer perspective.

[15] CIFAS (2014)
[16] ICO are planning research along these lines in 2015
[17] Romanosky S, Telang R and Acquisti A (2011)
[18] http://www.bbc.co.uk/news/uk-england-22083032
[19] http://www.lawgazette.co.uk/law/local-authorities-and-surveillance/57531.fullarticle
[20] Coll L and Bates R (2014)

Drawing out the consumers attitudes and perspectives on personal data against this backdrop is even trickier, given the nature of the subject and sweeping changes to the way in which data is used. Attitudes towards privacy and personal information are complex; people have very different perceptions of what even constitutes personal data in different circumstances. People's general attitude (neatly segmented in Demos' Data Dialogue work – see blue box) are contextual and dependent on the circumstances, organisations, types of data, links with other data and purpose of use. In short, privacy is a personal setting, with only the individual knowing what they are comfortable sharing on what basis. For example, many people regard health data as different to other types of data, both for its individual importance and sensitivity, and for the potential for aggregated health data to benefit the wider society.[21]

**Data Dialogue:**
Demos (2012)

There is no single attitude to sharing personal information: the public has a very varied and diverse set of attitudes and behaviours. People fall into one of five categories:

**Non-sharers** (30 per cent): knowledgeable about data protection, view much of their data as personal and take measures to protect it.

**Sceptics** (22 per cent): no single view about whether their data is personal or impersonal – but they are sceptical about whether 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.

**Pragmatists** (20 per cent): 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.

**Value hunters** (19 per cent): 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.

**Enthusiastic sharers** (8 per cent): 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 concerned about the ways in which data could be misused.

*NB: the research methodology was a combination of polling and focus groups, so we might assume that some participants with no previous knowledge of data collection and sharing practices would have had their understanding of this built throughout the process.*

#### 2.3.1.1 Support for entrenched positions

Given the difficulty in surmising clear attitudes on personal data, it is common to see research and evidence used to validate quite different positions on consumers' acceptance of data sharing and collection. This is not unique to this research topic, of course, but it does mean that research evidence is often used to support entrenched, opposing positions, and not necessarily applied in a way that might move the debate on personal data forward into a more productive space. For example:

*Position 1: "Consumers are very concerned about loss of control of their data."*

- The ICO's annual survey of consumer attitudes reports 88 per cent of respondents saying that they are concerned about the protection of personal information – ranking second place only to unemployment (89 per cent).[22]
- Ipsos Mori's annual survey of what G20 consumers feel most threatened by puts consumers' fear that their personal data could be compromised ahead of any other man-made or natural hazard or disaster. The last Global Threat Assessment, carried out in September 2012, shows 73 per cent of people expressing this concern.[23]

*Position 2: "Consumers' behaviour shows they are pretty relaxed about the use of their data."*

The number of users and level of penetration of services based on data sharing and commodification can be interpreted as acceptance or even comfort with the current data set-up on offer. For example, Facebook has 1.36 billion active users,[24] which is well over a third of the world's current online population of 3 billion,[25] with 27 million users in the UK.[26] Of course, we can't say for certain how aware users are of the exact terms of the exchange by which they receive services such as Facebook. Research from 2012 by Consumer Futures[27] found that one in ten consumers had not realised any data was collected on them via online services, and a further fifth thought that the provider only collected the minimum amount required to make the service work better.

#### 2.3.1.2 The say/do discrepancy

At the heart of this is the familiar issue of what consumers *say* they care about not necessarily being reflected in what they *do*. This discrepancy came out strongly in Consumer Futures' research from 2012, which found that despite a limited understanding of what is collected and why, 84 per cent of people want more control over what information organisations collect about them and how it is used, yet 87.5 per cent do not use any kind of control.[28]

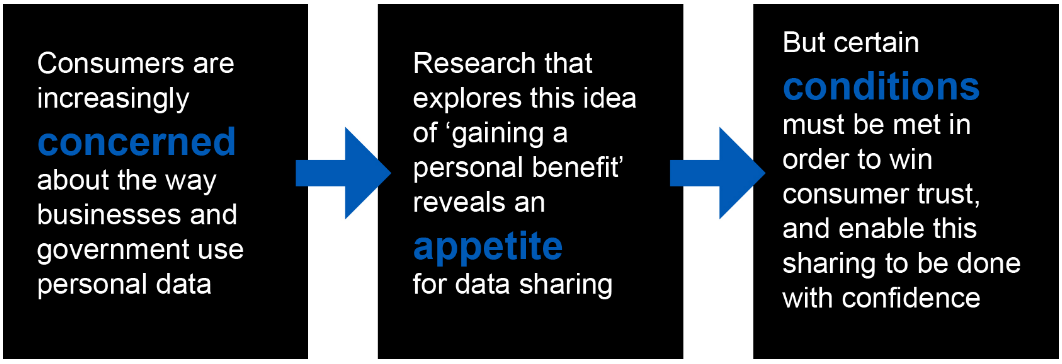
[22] Information Commissioner's Office (2013)
[23] Bricker D (2013) in Deloitte (2013)
[24] http://newsroom.fb.com/company-info/ (retrieved December 2014)
[25] http://www.itu.int/net/pressoffice/press_releases/2014/68.aspx#.VI7ZP2c-Kcw
[26] http://www.thedrum.com/news/2013/01/14/facebook-hits-27m-uk-users-and-unveils-retail-centre
[27] Consumer Focus (2012)
[28] Consumer Focus (2012)

More recent qualitative research by Consumer Futures into data privacy and smart meters found that, for most consumers, there was an underlying feeling of unease about data privacy, with a sense that they should be paying more attention to it but they don't know how; it is a complex area and they do not know who to trust.[29]

This in part suggests that the available mechanisms aren't meeting the consumer need for control, or that perhaps there is low awareness of them. In the last couple of years, we've seen a major change here, with 39 per cent of consumers reportedly using some sort of ad-blocking tool.[30] A number of ideas can be drawn from this: that awareness of the need for tools is higher (see the impact of Snowden in section 3.4), that awareness of the availability of tools is higher (thanks to software companies recognising privacy as a valuable asset to their brand), or even that the tools are better designed to be able to meet the needs of consumers.

### 2.3.2 A fresh look at what consumers are telling us

The following offers a fresh look at what consumers are saying and doing about personal data and information generally. This could help to inform a more constructive conversation on the potential for a fairer data settlement.



Consumers are increasingly **concerned** about the way businesses and government use personal data

Research that explores this idea of 'gaining a personal benefit' reveals an **appetite** for data sharing

But certain **conditions** must be met in order to win consumer trust, and enable this sharing to be done with confidence

- **Consumers are increasingly concerned about the way businesses and government use personal data**

The annual TRUSTe consumer confidence index for 2014 found 60 per cent of respondents were more concerned about online privacy today than they were a year ago.[31] 71 per cent of the UK population are not confident in the way that companies collect, use, handle and share data.[32] Levels of trust in internet companies (such as search engines or social media) are very low, with just six per cent saying they have high trust in them to use consumer data

[29] Griffiths C (2014)

[30] GfK (2013), 1,019 interviews conducted with a representative sample of online consumers between 7th-11th Feb 2014

[31] TRUSTe (2014)

[32] Economist Intelligence Unit (2013)

appropriately.[33] Online retailers fare slightly better in terms of trust with 13 per cent, which is on a par with government.[34]

The reasons for this mistrust and concern vary. The Royal Statistical Society's survey of trust in data use found 65 per cent of respondents reporting that their mistrust of internet companies' data use is based simply on these companies using personal data in hidden ways. This is echoed in other research showing that only 26 per cent of people believe that 'businesses are transparent enough in their use of consumers' personal data'.[35] Consumers believe that *"there is not a great enough incentive for businesses generally to protect my personal data"* (70 per cent),[36] and just 38 per cent believe companies will keep their data safe, while only 22 per cent are confident their details won't be sold on to other organisations.[37] The prospect of data being shared or sold on is high amongst concerns, with 82 per cent of consumers concerned that *"by sharing data I may be targeted for marketing campaigns in the future"*.[38]

For government, there are similar levels of mistrust regarding data being used for other purposes that people know nothing about, and a specific concern about personal information being used to discriminate against them (40 per cent). With regard to government and internet companies, the belief that they will be using consumers' personal data for their own benefit and not that of the consumer that it originated with is a reason for mistrust, with 53 and 55 per cent respectively reporting this.

- **Research that explores this idea of 'gaining a personal benefit' reveals an appetite for data sharing**

GfK research looked specifically at the consumer appetite for sharing for personal benefit, within limits. They found that most consumers are aware of the benefits of sharing data under certain conditions:

*"I would provide more information if…*
*…the service was better tailored to my needs (60 per cent)*
*…it helped me make better decisions (56 per cent)*
*…it helped me save money (71 per cent)."*[39]

However, 71 per cent of consumers would provide more information if they were sure that it would not be shared further.

- Almost 90 per cent of consumers want more control over their personal information.[40]

[33] Royal Statistical Society (2014)
[34] Ibid
[35] Economist Intelligence Unit (2013)
[36] Ibid
[37] Deloitte (2013)
[38] Economist Intelligence Unit (2013)
[39] GfK (2013), 1,019 interviews conducted with a representative sample of online consumers between 7th-11th Feb 2014

- 70 per cent say they would be more willing to share their data if they had the ability to withdraw it, and if they had the ability to see what data was being held about them.[41]

*Citizens Advice is playing a central role in UK smart meter development, addressing the real life implications of new data-rich technology on consumers in the home. Qualitative research around smart meter data sharing showed that consumers feel that they should be given the choice whether their personal details are shared, and with whom. There was a strong feeling that, in general, opting-out is made difficult and many consumers would like the options reversed – to opt in to sharing their data with third parties rather than having to opt out of the default setting. See Griffiths C (2014) for more details on this*

Consumer Futures research from 2013 into price comparison websites found that consumers trusted these sites as an information source (with 94 per cent feeling the information was either fairly or very reliable) but that they stopped short of allowing the sites to facilitate a switch on their behalf. This was because they did not want to provide the personal details necessary to do so, with concerns around being targeted by further marketing by third parties given as the most popular reason.[42]

When probed on the potential of data analyser services, even the more enthusiastic consumers had concerns about sharing of personal and usage data with other product providers, without their knowledge or permission.[43] These services meet data protection legislation requirements around consent, and yet it appears that this is still not enough to reassure trustworthiness in eyes of consumers. Again, this tallies with the earlier message from consumers, where 70 per cent felt that there are insufficient incentives for businesses generally to protect their personal data.[44] These insights suggest that there is potential demand from consumers to realise the benefits of data sharing, but that people have reservations about doing so within the current set up.

- **But certain conditions must be met in order to win consumer trust, and enable this sharing to be done with confidence**

As well having some idea of the outcomes consumers would like from their personal data use, there is also research evidence from consumers that tells us quite clearly the terms on which consumers would like their personal data used. Consumer research on the concept of *midata*, commissioned by the Department for Business Innovation and Skills (BIS) in 2012, asked consumers about how an organisation aggregating different personal data sets for enhanced decision-making could demonstrate trustworthiness. For consumers, the 'holy grail' of trust could be assured by:

[40] Direct Marketing Association (2012)
[41] Demos (2012)
[42] RS Consulting for Consumer Futures (2013)
[43] Ibid
[44] Economist Intelligence Unit (2013)

- ensuring data security and protection against data misuse
- enabling consumers to retain control of how their data will be shared and used
- guaranteeing data will not be used without clear permission
- knowing who is behind the initiative and who will keep it honest
- knowing how it will be funded or what the basis of its business model is.[45]

The next section will consider what it is about the current set up that does not engender trust in using personal data to innovate new services, looking at the current legal protections and the limits of the current implementation framework, the nature of data-driven services and the lack of consumer voice in discussions.

[45] Department for Business, Innovation and Skills (2012)

# 3 Defining the problem

This section considers why those consumers who want to share more of their data to gain personal benefit do not trust the current framework to enable this on their terms.

## 3.1 Limits of consent tools

It is widely accepted that data protection regulations in Europe need updating. They were adopted in 1995, when Microsoft released the first version of Internet Explorer and two years before Google.com was even registered as a domain name. However, there is much less agreement on what the updates should look like, or how they should be implemented. Indeed, it is at the implementation level where the biggest problems occur. The eight hard-fought-for principles upon which the European Union and UK data protection legislation are based remain essential foundations. In theory, they create a strong foundation for trust. The core provisions of the regulations stipulate that data should only be collected and used for a specified purpose, with the consumer's consent, and only held until that purpose is fulfilled. However, it is the way in which these provisions have been implemented that causes headaches for consumers, and contributes to the current asymmetric settlement that consumers have little choice but to accept.

The backbone of the system is 'notice (or disclosure) and consent'; consumers are informed of the purposes and use of their data via a privacy notice, to which they then indicate consent by ticking a box. This mechanism for establishing 'informed consent' is not fit for purpose because:

- **Consumers rarely read the terms and conditions or privacy notice before ticking the box.**

This is because the notices are too long, and too complex. Analysis undertaken in 2008 calculated that it would take 76 working days to read every privacy policy an internet user encounters in the course of a year. Research shows the median time users spend on license agreements was only six seconds; that 70 per cent of users spend less than 12 seconds on the license page; and that no more than 8 per cent of users read the License Agreement in full. Indeed, this has led some legal scholars to question whether they are actually valid, since consumers do not read them.[46]

*"Only in some fantasy world do users actually read these notices and understand their implications before clicking to indicate their consent."*[47]

- **Consumers are given a blanket either/or choice.**

[46] http://www.bbc.co.uk/news/technology-22772321

[47] President's Council of Advisors on Science and Technology (2014)

If the consumer wishes to access and realise the benefits of the service in question, they are left with little choice but to tick, click and hope for the best. There is no opportunity to negotiate, or to agree to some parts but not others. If they tick the box, they are deemed to have consented to everything stated in the privacy notice. As we learnt in section 2.3, privacy is above all a personal setting so trying to establish one blanket permission leads to policies that cover every eventuality and consequently minimise effective consumer control.

- **Privacy notices are written in a way that maximised an organisation's options for data use**

Since most consumers will tick the consent box, organisations have the opportunity to maximise the value of personal data by including more and more ways in which they can use it. So, the function of what is called a 'privacy' notice or policy becomes about demonstrating legal compliance with privacy legislation, as opposed to enabling real consumer choice over privacy requirements.

- **Terms and conditions represent a considerable burden to consumers**

Consumers are required to understand in depth the provisions of each organisation's data policies, and to do so anew every time they do business with a new organisation.

In addition, regulatory authorities have few resources and are unable to proactively monitor compliance with the law. Individuals objecting to a company's practices must take the company to court in an argument that they have little chance of winning. Individuals have to prove detriment on a case-by-case basis, and there is no systemic mechanism for reviewing the efficacy of the protection framework.

The net result is that the way data protection legislation is currently interpreted, implemented and enforced means that while the letter of the law is observed, its spirit can be routinely undermined and flouted. While the EU's proposals for data protection reform significantly tighten many of the provisions of the law, they do not address the flaws in its application surrounding the processes of informed consent. This means that regulatory reform alone may not yet provide an answer.

The application of the 'cookie law' is a good example of this, where the spirit of transparency and agreement has created a confusing array of notices for consumers[48] or even given way to workarounds such as alternative forms of tracking that bypass cookies.[49] This has done little to give consumers the controls they desire.

[48] http://www.cookielaw.org/media/105101/five-models-for-cookie-law-consent.pdf
[49] http://www.businessinsider.com/microsoft-plans-tracking-alternative-to-cookies-2013-10?IR=T

**Figure 3: Examples of EU cookie law compliance from across the web**

"Our site uses cookies and other technologies so that we, and our partners, can remember you and understand how you and other visitors use our site. To see a complete list of the companies that use these cookies and technologies and to tell us whether or not they can be used on your device, access our Cookie Consent Tool available on every page."

**"We value your privacy"**

"By continuing to use this site, you are agreeing to our use of cookies. If you do not want to see this message again, click continue."
More info

"We've updated our privacy policy, not that you care in the slightest. Like every site out there we collect some information online which we use to develop and enhance the services we offer to you. This involves the use of cookies. But don't worry, any data collected is all anonymous so even if we wanted we couldn't tell your wife, husband, civil partner, girlfriend, boyfriend or employer exactly what it is you're 'researching' on the Net these days."

"This site uses cookies to improve your online experience, click here to accept." More info

## EU data protection regulation reform summary

In March 2014, the European Parliament approved an amended draft of new, strengthened data protection reforms. They will take this to further negotiations with the European Council and European Commission to agree a final regulation.

There is widespread concern from consumer and privacy groups that the strengthened parliamentary text will be diluted during negotiations. In any case, the complexity and length of the regulation means few expect adoption before the end of 2016.

That the framework needed to create a good balance of innovation and control was never really in dispute, but what this elusive formula looks like, and how it could be reached, was subject to intense debate and the biggest lobbying campaign any piece of EU legislation had ever seen.

As at March 2014, the draft regulation tightens:[50]

- the definition of personal data to include anything that *"directly or indirectly"* is *"reasonably likely to be used"* to identify an individual including an *"identification number, location data, online identifier"*
- the definition of 'consent', which (as currently drafted) has to be a *"freely given specific, informed and explicit indication"* of the consumer's wishes via either a *"statement"* or *"clear affirmative action"*
- the requirements on businesses to explain their collection and use of personal data to customers, and to keep hold of data for a reduced time
- sanctions for companies that fail to comply, who could now face fines of up to 5 per cent of their annual turnover.[51]

Tensions remain over whether these reforms will create the right level of freedom to innovate with data, alongside adequate control and confidence for consumers. Some governments are unhappy with the amount of red tape that businesses will have to comply with. On the other hand, consumer and privacy campaigners claim that significant loopholes remain. For example, keeping an albeit narrower version of the 'legitimate interest' justification for retaining customer data effectively enables businesses to excuse themselves from many of the changes aimed at strengthening consent.

Whether the subsequent regulation will be a "breakthrough for data protection rules in Europe"[52], as claimed by former lead MEP, Jan Albrecht, or another easily circumvented rule book, remains to be seen. However, given companies' track records in sticking to the letter yet flouting the spirit of the law, these mammoth efforts to change the law may not create the principled approach to data protection that consumers deserve.

## 3.2 Lack of consumer voice

Finally, we must address the lack of consumer voice in the development of frameworks and practice for delivering changes to the way personal data is managed. This, of course, is not an issue limited to personal data – too often in business and regulation, the requirements and voice of the consumer is absent – but in this case it is arguably even more of a problem. For people whose behaviours, preferences and habits are more visible than ever, there is a distinct lack of agency to influence how all of these are used for anything other than company or state interests.

First of all, although personal data is a resource created by and originating from consumers, they have very few options for receiving value from it. That's not to dismiss the incredible benefits of instant and easy access to information, friends and products, but rather to think

[50] http://europa.eu/rapid/press-release_MEMO-14-186_en.htm
[51] http://europa.eu/rapid/press-release_MEMO-13-923_en.htm
[52] http://www.europarl.europa.eu/news/en/news-room/content/20131021IPR22706/html/Civil-Liberties-MEPs-pave-the-way-for-stronger-data-protection-in-the-EU

about the value that people get for giving up so much of their personal information, relative to the value that is derived by the data controller.

Secondly, participation in a system that collects and uses personal data is now practically mandatory; we are reaching a point where not participating in the digital world is becoming an extreme position, so it is not comparable to a choice over which supermarket to shop in, or which product to buy. And even if you are not a digitally savvy, next-generation user,[53] most interactions across different markets involve a personal data trail. So even if you choose not to take part in social media, or e-commerce, you are highly likely to be participating in banking or public services (planned to eventually be digital by default in the UK), which will involve leaving information trails used as the basis for other decisions being made about you or your family.

Thirdly, as the digital age takes hold, our online and offlline identities are experiencing profound shifts, with generations emerging who will not even demarcate a difference between the two. Actions taken or comments made are increasingly visible, and linkages between information and data trails much easier to make. Any debate, therefore, has to go beyond targeted advertising or privacy policies and have a more comprehensive understanding about how we control and manage information about ourselves and our identity in a digital age.

Moving towards a situation where consumer control and understanding of data use is at the centre of frameworks and decisions might get us out of the current discourse, which has not to date imbued consumers with confidence. This can be roughly described as businesses and government not only setting the terms on which data-sharing agreements are made (see section 3.1) but defining the terms on which organisations should be trusted. We are in a situation where, in terms of personal data use, the dominant preoccupation of businesses seems to be: ‘How can I persuade more people to trust us?’, when it should be ‘What level of trust do consumers want, and how can I demonstrate this?’. The two questions may look similar but only the second has consumers at its heart. Whilst putting consumers first is easy enough to talk about, actually enacting it in an authentic way would be quite a radical step as it requires a reversal of the current set up – whereby organisations own and manage data – to one where the individual is the central organising point of data.

In section 4, we will consider the development of emerging alternative ways to manage personal data that place the consumer at their centre, along with the evidence of consumers’ appetite for this and the associated risks and opportunities.

[53] As defined by Oxford Internet Institute (2013)

# 4 Emerging alternatives to the status quo

## 4.1 Personal data empowerment

Sections 2 and 3 of this report have set out how a data-flooded world and the inability of current regulations to give consumers confidence and control has made for an obvious gap in the market. We will now consider the emerging market for personal data empowerment tools and services that offer consumers an alternative to the current status quo. Understanding the needs that these services are meeting is helpful for both understanding the problems they solve and the opportunities they enable.

**Personal data empowerment** means consumers having meaningful control over the use of their personal data, and being easily able to understand and determine how it is used and the benefits they will derive, all within appropriate trust mechanisms.

The concept is simple enough; rooted in the idea of empowerment, it is about consumers having the tools and ability to secure the best outcomes for themselves and others. Personal data becomes a tool in the hands of the individual and consumers are empowered to achieve better outcomes by asserting more control over how their data is collected, managed, used and shared.

For the purposes of this report, the term ‘personal data empowerment’ covers:

- actual personal data empowerment tools that make controlled sharing and use possible
- the supporting and enabling infrastructure, policies and practices – sometimes called the ‘ecosystem’
- related services such as analytical or decision support services – that is, the application of data for more useful outcomes.

While this may sound convoluted, personal data empowerment is not about putting further onus and inconvenience on the consumer. It is about creating simpler tools for managing understanding, agreement and control.

### 4.1.1 Personal data empowerment tools and services

Over the last few years a growing number of new tools, apps and services have emerged with offers to help individuals assert more control over how their data is collected and used, and by whom. Importantly, these services are being offered independently of the consumer’s relationship with any particular supplier (such as a bank, retailer, energy company or telecommunications company). Indeed, one of the benefits offered by these new services is the help they provide to consumers in managing their dealings with their various suppliers.

Citizens Advice wanted to track the emergence of this market, which identified ten core service components on offer that go some way to addressing the barriers and problems experienced by consumers, as identified in sections 2 and 3 (see section 7 for methodology). These ten elements can work separately or together to create better mechanisms of control.

| | |
|---|---|
| 1. **Transparency** | 6. **Share data under my control** |
| 2. **Access** | 7. **Manage my identity online** |
| 3. **Generate my own data** | 8. **Build profiles of myself** |
| 4. **Store and manage my data** | 9. **Do personal analytics** |
| 5. **Set permissions for collection, storage and use of my data** | 10. **Control what information I receive** |

1. **Transparency: understanding who has data about me**
   Consumer research routinely shows that consumers feel they have lost control over their data, with data being collected surreptitiously (via cookies, for example), being held by organisations without their knowledge, or being sold on by companies that have collected it 'legitimately'. There are now a growing range of services promising to help consumers 'track the trackers', such as **Ghostery**, which provides a visual of the companies that are tracking you and now has 20 million global users.[54] **Privacyfix** is another example, which rates sites on their privacy basis and allows you to block some tracking.[55]

2. **Access: see and retrieve data about me from organisations**
   There is a growing international movement amongst regulators and policy makers to encourage or require organisations to release personal data they have collected back to the customer. The leader in this movement is the UK Government's **midata** programme,[56] which is focused on regulated industries, particularly banking, energy and telecoms. This is paralleled in the US by a series of **MyData** initiatives aiming to "empower Americans with secure access to their personal data".[57]

   These governmental initiatives are now being mirrored by new services that promise to help individuals retrieve their data from organisations, for example **FileThis**,[58] which authorises a digital assistant to obtain documents such as bank statements and bills, and store them securely.

[54] https://www.ghostery.com/en/
[55] http://www.privacyfix.com/start/faq
[56] https://www.gov.uk/government/policies/providing-better-information-and-protection-for-consumers/supporting-pages/personal-data
[57] http://www.whitehouse.gov/administration/eop/ostp/initiatives - Openness
[58] https://filethis.com

### 3. Generate my own data

Mass-market apps like **Jawbone UP**[59] and **Fitbit**[60] are already popularising the idea of individuals using gadgets to capture data about their own activities and behaviours. The 'quantified self'[61] and 'personal informatics'[62] movements have active groups around the world, where individuals are using devices to gather data about their day-to-day behaviours and using it to generate insights into their own lives that weren't previously available. This offers clear potential for managing the demands of long-term health conditions, and NHS England has incorporated the idea into its new strategy for Technology Enabled Care Services.[63]

In addition to hundreds of devices and services across a wide spectrum of behaviours (such as energy usage, time use, reading matter, physical activity and mood), new 'meta' services such as **Narrato**[64] are emerging. **Narrato** is a platform for combining your personal data generated by different data capture applications into one dashboard.

### 4. Store and manage my data

At the heart of personal data empowerment is the ability of individuals to store their own data safely, where a copy of the data in question remains under their own control. Personal data stores (or 'vaults' or 'clouds') are the subject of increasing entrepreneurial and corporate activity; examples include **Allfiled**[65], **Mydex**[66] (an identity assurer for the government) and also password stores such as **LastPass**. They offer a number of services and functions:

- **Record keeping**

Keep admin data such as insurance policy numbers, driving licence details, NHS and National Insurance numbers in a safe place that is instantly and easily accessible via a smartphone or computer.

- **Digital letterbox**

Act as a secure, easy-to-access repository for **midata** releases and other data provided by suppliers, such as bills, statements, receipts, contracts and policies.

- **Administrative efficiency**

Provide data management services such as automatic population of online forms.

- **Profile building**

Build up a bank of verified attributes – such as driving licence, passport and educational qualifications – that are stored safely and can be shared securely with other parties when needed.

[59] https://jawbone.com/up
[60] http://www.fitbit.com/uk
[61] http://quantifiedself.com
[62] http://www.personalinformatics.org
[63] http://www.england.nhs.uk/2014/09/23/tecs-programme/
[64] https://www.narrato.co
[65] https://www.allfiled.com/
[66] https://mydex.org/

- **Digital identity**
  Provide a digital identity at appropriate levels of assurance that can streamline access to online services while reducing risk. Taken together with the profile-building tools mentioned above, these functions contribute to data minimization by enabling consumers to reveal only the attributes required.
- **Data aggregation**
  Enable the aggregation of previously dispersed data sets, such as financial accounts or data relating to health, so that the data can be analysed to discover trends and patterns and inform decision-making.
- **Data combination**
  Enable the combination of different sets of data, such as energy use, financial circumstances, property attributes and lifestyle data, to create a rounded picture of a situation and inform decision-making.
- **Control**
  Empower individuals to decide what data to share with which organisations for what purposes in the context of an audited monitoring, compliance and enforcement system.
- **Data sharing**
  Create standing-order style data-sharing arrangements with chosen suppliers to drive administrative efficiencies for both sides, for example, ‘My current contact details are …, my current energy use is…’.
- **Contact management**
  Create a safe, easy-to-use contact management system that lets the user manage levels of intimacy and is independent of any device yet can be uploaded or linked to any device.
- **Monetisation**
  Create systems whereby individuals can ‘rent’ their data to organisations for a fee, on either an anonymised or identified basis.

5. **Set permissions for collection, storage and use of my data**
   Ultimately, privacy is a personal issue, not an organisational policy. Only the individual knows what information they feel comfortable sharing, and with whom, for what purpose and in what context. There is growing interest in new and alternative mechanisms that recognise this. Trying to establish a single, blanket permission in advance of data use is impractical and leads to cover-all permissions that allow everything and eliminate all effective consumer control.

   Instead, there is growing emphasis on context-driven permissioning, where a specific permission is given in the context of a specific action and consumers can change their settings via a dashboard. Most personal data stores build permission setting into their core service. So, for example, when using location data on a phone, a menu might pop up explaining that certain data will be used, what it will be used for and how it will be kept. **Mypermissions** is an example of a service that alerts smartphone/tablet users when their apps are accessing personal data.[67]

Closely related to this is the concept of time-stamped permissions. A permission may last for a day, a month or a year, after which it expires. This raises the question of monitoring and enforcement, and so-called 'sticky policies' are being developed as a solution to this, as discussed in section 4.1.2.

To enable effective permission setting of any type, consumers need to understand what they are agreeing to. This is prompting new initiatives in how to explain and present potentially complex contracts as easy-to-understand, simple visual icons, such as the examples from Mozilla in Figure 4. This work draws on the experience of Creative Commons-inspired licenses, which translate complex legal tools into simple terms that both humans and machines can understand. With Creative Commons, these tools help creators choose the right license for their work, including a simple set of visual icons that help users understand what they can do with the work.

Similar approaches can be applied to personal data. By attaching sticky policies to content, search engines and aggregators can automatically find and organise content according to the licenses applied. A number of innovators and entrepreneurs, such as the OpenNotice project,[68] are looking at how to translate these learnings into efficient, effective permissions-management services for individuals in the personal data context.

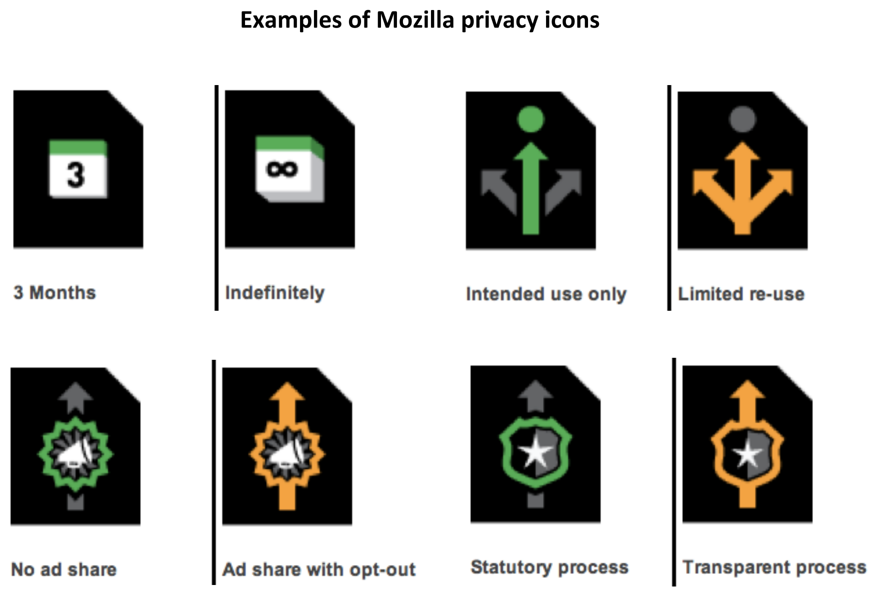


*Figure 4: Examples of privacy policy icons developed by Mozilla. For example, the '3' versus 'indefinitely' refers to how long the data is to be kept; the arrows refer to how the data will be used, the bursts to use of data for advertising purposes, and so on.*

[67] http://mypermissions.org/
[68] http://opennotice.org

6. **Share data under my control**

In addition to individuals' ability to set and change permissions for data collection and use, another key element of the new personal data ecosystem is their ability to choose what information they actively wish to share, and with whom. Most personal data stores include this as a core function, but a number of innovators and entrepreneurs are focusing on this challenge in particular.

Another aspect of controlled information sharing is the concept of 'intent casting', where individuals advertise their needs and wants to suppliers, as opposed to producers advertising their products and services to consumers. An 'intention' is a potentially rich (and sensitive) piece of data that lies at the heart of all marketing targeting, highlighting who an individual is, what they want and when. A number of new services have sprung up to put this idea into practice**,** such as **intently.co**.[69]

7. **Manage my identity online (including anonymisation)**

Identity assurance is simply the way in which people prove that they are who they say are, online, cutting out the need to present themselves in person or hand over physical documents. It causes one of the biggest headaches for consumers within the current personal data landscape, creating costs and risks for companies who are not sure that the person they are dealing with is who they say they are, and for individuals who find themselves having to jump through multiple hoops, remember numerous user names and passwords, and so on. Specialist personal data empowerment tools and services see big opportunities in creating 'user-centric' solutions where consumers or citizens can carry their own assured identity around with them from organisation to organisation.

***CABINET OFFICE IDENTITY ASSURANCE PROGRAMME***
*The Cabinet Office is currently testing a new system that allows a range of public service providers to easily verify a customer's identity, once that customer has proved their identity with one of the approved providers such as Mydex, The Post Office or Experian.*

While simplifying identity assurance presents major opportunities, the processes needed to establish assured identities open the door for much richer markets for *attribute exchange* – the exchange of verified attributes and credentials. A simple example is a university providing its graduates with a secure electronic token confirming that the student has a certain class of degree in a certain subject, so that the student can forward this token to future employers as part of their CV. This same idea can be extended to verification of any imaginable personal attribute, where organisations become both providers and receivers of verified attributes.

[69] http://intently.co/

This is a potentially huge new market that is predicated on the assumption that the individual is an active party within the ecosystem, holding and choosing to share a potentially wide range of verified attributes with the organisations they deal with.

Examples include:

- **Miicard** – a digital passport to verify identity[70]
- **DuckDuckGo** – a search engine that doesn't collect information[71]
- **Mailpile** – encrypted email services[72]

8. **Build profiles of myself**

Profiling is a very big business nowadays: collecting and aggregating different bits of data about an individual lies at the heart of online advertising and service personalisation. So it is not surprising that a number of personal data empowering tools and services are focusing on helping individuals build profiles of themselves, not only to monetise this data if they choose to and the opportunity exists, but also to replicate the benefits of analytics experienced by corporate data miners.

By definition, personal data stores help individuals build up profiles of themselves, as do specialist services such as **Handshake**[73] and **YesProfile**[74] (see point 6, 'Share data under my control', above). For example, **Datacoup**[75] is a service that aggregates data from all your online sources, then repackages and sells in anonymised form, thus enabling customers to benefit financially.

9. **Do personal analytics**

Once individuals have profiles of themselves, the obvious service is to 'mine' this data to understand trends and patterns, and to gain new insights into their own behaviours. What is your carbon footprint? How much money do you spend on coffee, or travel, or food, each month? Do you know which aspects of your energy usage cost you the most money? Do you know if the way you use your mobile phone fits with the tariff you are on? The possibilities for personal analytics are as big as they are for any corporate. Examples of this are **Billmonitor**[76] or **Ontrees**[77].

10. **Control what information I receive**

The other side of the coin to controlling what information they give out, many consumers also want to control and filter the information they receive – especially to filter out spam advertising. There are a large number of ad-blocking software services on the market, which is growing rapidly, with some estimates suggesting that up to a fifth of consumers use them. This is now a significant cause of concern

[70] http://www.miicard.com/
[71] https://duckduckgo.com/
[72] https://www.mailpile.is/
[73] http://www.handshake.uk.com/hs/index.html
[74] http://www.yesprofile.com/
[75] http://www.datacoup.com
[76] www.billmonitor.com
[77] www.ontrees.com

for online advertisers and content providers and may be a factor persuading them that different approaches may be preferable. Examples of this are **Adblockplus**[78] or **Adtrap**[79].

### 4.1.2 Wider personal data empowerment ecosystem

Personal data empowering tools and services can only gain critical mass within a supporting ecosystem – one where businesses are prepared to cooperate with them, where rules and regulations facilitate and support their operation, where technical infrastructure enables efficient, secure delivery of their services, and where consumers trust, and understand the usefulness of the services being offered.

'Privacy by Design' principles lend themselves well to this task, and their application within a full personal data ecosystem are examined in Dr Ann Cavoukian's paper, which demonstrates how regulators can work with new technological developments to help consumers make real the value of their data.[80]

**Privacy by design principles:**[81]

1. Proactive not reactive: take preventative action on privacy
2. Privacy as the default setting: high levels of privacy are default setting
3. Privacy embedded into design: not a bolt on extra
4. Full functionality: avoid trade-offs and try to create wins for all
5. End to end security: management of data through whole life cycle
6. Visibility and transparency: keep it open
7. Respect for user privacy: make all services user centric

There are, meanwhile, a range of initiatives outside traditional regulatory interventions designed to rebuild trust around personal data use. Central to these is a growing interest in trust frameworks, and the US National Institute for Standards and Technology (NIST) has just awarded funding for a project to "develop and demonstrate a Trustmark Framework that seeks to improve trust, interoperability and privacy within the Identity Ecosystem".[82]

A trust framework is essentially a club of organisations agreeing to abide by a certain set of rules that offer individual consumers greater protection and rights than they would experience when dealing with organisations outside of the club. One of the incentives for organisations to join the club is the fact that trust relating to the collection and use of personal data is becoming a differentiator among brands, with some brands, such as Microsoft and MoneySupermarket, including promises about personal data in their advertising campaigns.

[78] www.adblockplus.org
[79] www.getadtrap.com
[80] Cavoukian A (2012)
[81] http://www.privacybydesign.ca/index.php/about-pbd/7-foundational-principles/
[82] http://www.darkreading.com/risk/nist-awards-grants-to-improve-online-security-and-privacy/d/d-id/1140502?

By agreeing to abide by the club's rules, joining organisations are signing up to a common, standard default set of terms and conditions for data collection and use. As Synergetics, a Belgium-based Trust Framework provider explains, Trust Frameworks create a network of stakeholders that "lowers transaction costs and adds convenience, security, and trust to all parties, including the end-user … The a-priori assumption that it is basically safe to transact with any member of the network, promoting trust in the whole network which leads to its acceptance and widespread use".[83]

Personal data store operators such as Mydex offer their own trust framework (anyone seeking to connect to an individual's personal data store via Mydex must sign up to the Framework's rules)[84]. The Open Identity Exchange (OIX) is attempting to build a register of accredited Trust Frameworks that meet certain core standards, focused on identity assurance.[85]

A key challenge for would-be Trust Frameworks is the costs of audit, compliance and enforcement, which need to be automated as far as possible. Companies like Microsoft and SAP are working on technologies to enable this. One such technology is 'sticky policies', where metadata about the rules and agreements relating to any particular piece of information travel around with the information itself. This effectively 'locks' any use of the data until it is confirmed that the service provider's own policies conform. If a third party fails to act in accordance with the policy, then it is effectively a breach of contract and so the data subject (or more likely the personal data store or dashboard acting on their behalf) can take action against the offending party.[86]

### 4.1.3 Related decision support services, or next generation intermediaries

A system based on personal data empowerment offers the potential for new and more powerful services that help consumers and citizens make better decisions and manage transactions with greater ease. Consumer Futures' work on next generation intermediaries[87] looks, amongst other things, at how permissioned access to personal data can support automated switching based on preferences, working with current consumption data to establish the service that best suits consumers' actual needs on an ongoing basis.
There are strong potential synergies between these services and the personal data empowerment tools listed above. For example, Cheap Energy Club provides price comparison services for consumers but uses a personal data store (**Allfiled**), which enables the safe keeping and use of personal information.[88]

[83] www.synergetics.be
[84] https://mydex.org/the-mydex-charter/
[85] http://openidentityexchange.org/resources/trust-frameworks/
[86] Pearson S and Casassa Mont M (2011)
[87] Ctrl-Shift for Consumer Futures (2014)
[88] Ctrl-Shift for Consumer Futures (2014)

## 4.2 Opportunities and risks of personal data empowerment

So what can this emerging activity tell us about future opportunities for the consumer-centered use of personal data? Here, we consider the risks and opportunities of the current market and potential alternatives, based on original qualitative research with policy makers, regulators, practitioners and campaigners.[89]

### 4.2.1 Opportunities

Looking at the suite of functions offered by the ten categories of personal data empowerment tools and services, plus moves to strengthen the trust environment surrounding them, we can see a vision of a very different personal data ecosystem take shape. An optimistic take on this would see mass adoption of new personal data empowerment tools and services that fall into daily automatic use, rather like Google search or the use of plastic cards to make payments, with a number of expected results:

- **Problems solved:** the issues and abuses of the current system are significantly alleviated, if not eradicated, simply because it's no longer possible or commercially attractive for organisations to misuse the data they collect.
- **A new data deal**: this changes the personal data agenda in society to a new deal based on assumptions of transparency and individuals controlling and benefiting from the use of their data. This is expressed in new and different standards and best practice on the part of organisations. MIT Professor Sandy Pentland calls this "a New Data Deal".[90]
- **Consumer empowering services:** personal data empowerment tools and services act as a platform for the provision of new and more powerful consumer empowering services[91] to aid decision making and facilitate more efficient service provision.
- **Changed corporate priorities:** the changing climate prompts/forces corporations to shift their focus of service provision. If they had previously seen profit opportunities in taking advantage of poor decision-making by consumers, they now see more profit in the provision of personal data enhanced decision support services. For example, while energy companies may not like price comparisons about energy tariffs, they may find personalised energy saving advice an attractive market to enter. Likewise, this applies in other industries such as banks with money management services ('spend more wisely with us'), privacy-enhancing, location-based services by mobile operators and so on.

The net result could be that personal data empowerment tools and services help establish and sustain the 'rules and tools' of a much more productive, innovative and trust-based

[89] See methodology in section 7
[90] http://blog.digital.telefonica.com/2013/07/31/sandy-pentland-new-deal-on-data-mit/
[91] Ctrl-Shift for Consumer Futures (2014)

personal data ecosystem, where different forms of consumer empowerment are a routine feature or function of service provision.

If they gain critical mass, these new services, initiatives, and infrastructures could represent a major shift, outlined below in a before-and-after scenario:

| Before | After |
|---|---|
| Organisation collects, holds and uses data about customers. | Organisations release this data back to customers, helping customers collect, hold and use data about themselves. |
| Organisations use customer data to make and save money and manage their businesses better. | Via new forms of information service, individuals use their own data to make and save money and manage their lives better. |

Figure 5 depicts the World Economic Forum's vision of how this new personal data ecosystem might look. Under this vision, the data-empowered individual lies at the heart of the ecosystem, using their personal data store to acquire data from organisations that have collected it (supported by initiatives like *midata*), and then using this data to acquire new services from 'requesting parties'.

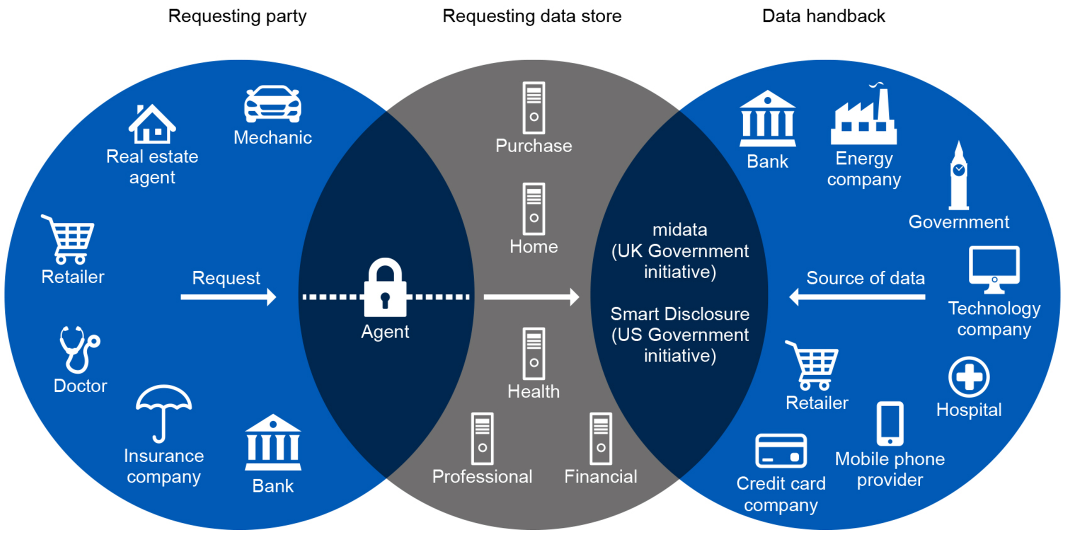


***Figure 5: The World Economic Forum's vision of the new personal data ecosystem, with the data-empowered individual at its heart***

If the 'before' scenario does indeed evolve towards the 'after', it could herald important changes in the ways consumers interact with companies.

### 4.2.2 Scope, scale and appetite

Of course, such important changes will only come about with sufficient consumer appetite and trust, along with the willingness of providers to bring such tools and services into the mainstream and, crucially, to be able to join together services to make some sort of coherent infrastructure.

To operate successfully in a digital world, consumers already have to manage digital personal data to some degree. They are building profiles of themselves on services like Facebook and LinkedIn, learning about the risks and rewards of sharing information on social media platforms, about the pains and necessities of identity assurance when applying for loans and mortgages or trying to remember user names and passwords, and about the ins and outs of administration when completing forms online. They are keeping records of phone conversations and email trails on their digital devices and storing and sharing documents through services like DropBox. Whether explicitly conscious of it or not, they are becoming 'data controllers' in their own right.

***THE SNOWDEN EFFECT***

*It would be impossible to produce a report about online personal data in 2014 without reference to the 'Snowden' effect, which has brought about a shift in awareness of the levels at which our data can be collected and shared, and with whom.*

*Edward Snowden was a contractor at the US National Security Agency (NSA) who, in June 2013, leaked details of classified information about the extent of US surveillance programmes.*

*Unpicking the impact of the revelations is the subject of much analysis, and has had a variable impact in different countries. From a citizen perspective, the relationship between spy agencies, governments and large-scale internet companies is now firmly in the spotlight. This has led to reduced public confidence in the control individuals have over their personal data, how companies use it and how governments might access social networking information.*

*A survey of US citizens from the respected Pew Internet project found the following results:*

***91 per cent** of adults surveyed 'agree' or 'strongly agree' that consumers have lost control over how personal information is collected and used by companies.*

***80 per cent** of those who use social networking sites say they are concerned about third parties like advertisers or businesses accessing the data they share on these sites.*

***70 per cent** of social networking site users say that they are at least somewhat concerned about the government accessing some of the information they share on social networking sites without their knowledge.*
*(Source: http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/)*

*But what can we learn about the impact on consumer perspectives on the control of personal data. Can a distinction be drawn? There is not enough space to unpick the implications here, but the TRUSTe Consumer Confidence Index published in January 2014, which surveyed UK citizens, found the following:*

*Overall, 60 per cent of respondents said they are more concerned about online privacy today than they were a year ago. Of those that said they were more concerned this year, 60 per cent attributed the feeling to companies sharing their personal information with other companies, while 54 per cent were concerned about companies tracking their online behaviour to target them with ads and content. Only 20 per cent cited media coverage of government surveillance programmes as a reason for their increased concern.*
*(Source: http://www.thedrum.com/news/2014/01/27/increase-consumers-online-privacy-concerns-signals-negative-impact-business)*

Large companies are increasingly recognising consumers' desire for more control and confidence over how their data is collected and used. Examples include:

- Microsoft's advertising campaigns around Your Privacy is Our Priority[92] and its provocative adverts directly criticising Google's data practices
- Apple's open letter on privacy covering security measures and also a reiteration that personal information will not be 'monetized'[93]
- Barclays Bank's launch of a personal data store, Barclays Cloud It[94]
- The decision by Acxiom, the huge US data broker, to let consumers see the data it holds about them[95]
- Intel's campaign, We The Data,[96] which is based on the consumer desire for increased trust and control
- Telefonica's Digital Confidence initiative[97]
- BT's interpretation of the e-privacy directive (or cookie law) as a way to increase choice and transparency.[98]

The question is whether independent personal data empowerment tools and services will gain critical mass and market influence in their own right. Many early pioneers have already gone under, but others survive and have the potential to gain some degree of critical mass:

- Through its link up with Cheap Energy Club, **Allfiled** already has over 1.2 million UK users, and this could expand dramatically as MoneySavingExpert rolls the same concept out across other markets.[99]
- AVG, the internet security service with over 100 million users, recently acquired Privacy Choice, the producer of **PrivacyFix**, which tells users what data sites are collecting and what they do with this data. It plans to roll out transparency and permissions settings services to all its users.[100]
- **Ghostery**, which helps internet users identify who is tracking them and block the trackers if they wish, has over 20 million users worldwide – small when compared to internet-scale services with billions of users but still evidence of demand.[101]
- As one of the UK Government's nominated identity service providers for 'digital by default' services, **Mydex** could potentially have a very large customer base over the next few years.[102]
- The Mozilla Foundation is taking a strong pro-privacy stance by introducing personal data empowerment tools and services into its core offerings (such as default Do Not

[92] http://www.microsoft.com/en-GB/security/online-privacy/overview.aspx
[93] http://www.apple.com/privacy/
[94] http://www.barclays.co.uk/CloudIt/P1242634022583
[95] https://aboutthedata.com
[96] http://wethedata.org
[97] http://dynamicinsights.telefonica.com/983/digital-confidence-discussion-at-campus-party
[98] http://home.bt.com/pages/navigation/privacypolicy.html
[99] http://www.moneysavingexpert.com/cheapenergyclub
[100] http://now.avg.com/avg-technologies-acquires-leading-online-privacy-firm-privacychoice/
[101] https://www.ghostery.com/en/about
[102] https://gds.blog.gov.uk/2013/09/03/identity-assurance-first-delivery-contracts-signed/

Track settings). Over 20 per cent of its browser users have already adopted Do Not Track. With hundreds of millions of users, Mozilla has a strong market influence and other browsers such as Microsoft Internet Explorer are following suit.[103]

These examples show that personal data empowerment tools and services have the *potential* to scale up and impact mainstream markets but they do not guarantee it. The question is whether they can offer the convenience, utility, sense of safety and business models to move from start-up mode to commercial viability and broader take-up.

Policy makers and regulators are particularly concerned with the level of impact that can be made. One obvious scenario is that of niche take-up, where a significant minority (say 10 or 15 per cent) of consumers adopt a range of different personal data empowerment tools and services, leaving the majority carrying on with business as usual. If this minority is large and vociferous enough, suppliers – and therefore regulators – will be forced to respond, which will prompt larger take-up.

Another scenario is a complex mix of services with different degrees of take-up. For example, ‘entry level’ data collection, storage and management services could well become mainstream. They might be incorporated into other services, for example a personal data store supporting automated switching, or a data dashboard enabling sharing preferences to be easily set.[104] Large corporates such as Barclays are offering services designed to a) compete in the market in their own right and/or b) diffuse consumer demand for alternative services. Under this scenario, a small number of personal data empowerment tools and services could gain significant market penetrations; only a tiny number need to survive and grow in order to make a significant impact on the market.

However, the biggest potential impact of personal data empowerment tools and services is that they introduce a *new business model* around personal data. Traditionally, organisations collect data about their customers and use this data to improve their operations. The web 2.0 model treats personal data more as a tradeable commodity, usually collecting and monetising personal data in exchange for a ‘free’ online service. Personal data empowerment tools and services create the infrastructure for personal data to be used to drive information services for those individuals – with potentially multiple different direct revenue streams. These include fees, commissions, advertising revenues, market research revenues and indirect benefits for companies, such as reduced go-to-market costs, the ability to attract new customers and to retain existing ones. In many ways this reflects wider trends in technology, such as the diffusion of computing and information processing power to the masses.

The challenge for policy makers and regulators is that these three underlying business models – personal data as ‘raw material’ for corporate service provision, personal data as a traded commodity, and personal data as ‘raw material’ for new information services to individuals – will evolve side by side for some time to come, interacting with each other and mutually influencing development.

[103] https://www.mozilla.org/en-US/firefox/dnt/
[104] See, for example, http://www.incontrolads.com/

### 4.2.3 Risks and caution

Any emerging system brings potential risks, particularly one that turns the model of data collection, use and control on its head:

- **Corporate flanking,** as existing companies offer watered-down versions of personal data empowerment tools and services to dampen and channel consumer demand into safer places. For example, instead of offering to release data back to customers, Tesco is investigating providing customers with new data services based on Clubcard data, where the data remains safely in the hands of Tesco.
- **Resistance from incumbents:** we may continue to see an increase in sites that don't allow access if viewers block the ads, as this is their core revenue stream.
- **New abuses** flourish on the back of new capabilities – for example, if it is easier for consumers to share rich data about themselves, there is a greater incentive for operators to persuade or con consumers into parting with this data on unfair terms. Control is an attractive theory but people can exercise poor controls or be influenced by carefully crafted incentives to use their data in a way that goes against their interests.
- **Market confusion** in the face of a proliferating number of different services, with consumers not knowing which ones they can trust.
- **Exacerbated digital divide** as those already empowered use personal data empowerment tools and services to become even more empowered, leaving the rest of the population relatively worse off. This could create new problems for both regulators and suppliers as they now have to deal with much greater extremes of customer behaviour. For example, if companies respond to margin pressure from highly empowered, digitally savvy consumers by driving up margins from less-empowered consumers, 'increased consumer empowerment' could be a mixed blessing.

Assessment of these risks suggests that all are likely to become realities, to some extent.

## 4.3 Implications of a new approach

An important part of this research was to test out the assumptions, risks and opportunities of personal data empowerment tools and services with a range of opinion formers and policy designers at the heart of the personal data and privacy space. We wanted to better understand what such new developments might mean for consumers, both at a technical implementation level and more broadly in terms of their potential for enabling a fairer data deal. Having set out a vision and approach for personal data empowerment, this section outlines some of the insights, implications and reservations of UK regulators, policy makers, privacy campaigners and technologists gleaned from in-depth, confidential one-to-one interviews. All remarks are reported anonymously.

### 4.3.1 The architecture of the new system: how to build security?

Some of our interviewees had reasons to be cautious of, or even oppose, new services such as personal data stores, because the underlying architecture of their systems is vulnerable and/or because the processes they use to collect, store and manage data are not secure.

“The concept of a personal data store is problematic [because] … centralised data storage in the cloud is not advisable.”

“Personal data stores represents a threat disproportionate to any value a consumer might extract.”

“There are a limited number of cloud providers and these will provide locations for personal data stores. However, this creates focal points of attack by hackers who could, if successful, get access to a large amount of very detailed data about millions of people. It is not just the details of one credit card that a hacker could gain access to, it is a large amount of granular data about millions of citizens. This offers potential for identity theft on a never-seen scale.” One solution could be to stipulate that services offering to collect, store or use personal data employ the same sort of Information Security Management Systems (ISMS) and penetration testing required of banks.

Some of the new services, such as the personal data store **Mydex**, claim they have risen to these challenges. It does not create a centralised database; each personal data store within its system is individually encrypted and Mydex itself is unable to ‘look inside’ any individual’s store because, as with Swiss banks, the individual holds one of the keys. Mydex also has company-wide ISO 27001 accreditation – the international ISMS standard adopted by banks. However, Mydex is the only ISO 27001 accredited personal data service we could find. If other services do not have the necessary robust data architectures or security processes, they might be creating new data security problems and, therefore, potentially new headaches for regulators.

### 4.3.2 ‘Rights’ vs ‘deals’

Another debate amongst privacy and consumer advocates is whether the focus of personal data empowerment should be on consumers’ rights to privacy or the value of their data to themselves and to others. Some warned that the current debate about the commercial value of personal data is ‘commoditising’ a basic human right: “There is no such thing as a property sale where you retain control after you have sold it…that’s why we don’t treat personal information as property.”

Others, however, focused more on the division of the cake, arguing that consumers are not getting a fair share of the commercial benefits generated by their data. In this view, personal data empowerment is aligned to a ‘redistribution of wealth’ from large corporations to consumers:

“Increasingly, we are concerned about equitable benefit. There is an increasing disequilibrium between the individual consumer and the services they interact with.

There ought to be some sort of equitable benefit being derived by the consumer as much as the business."

This is a potentially crucial business model issue. Do personal data empowerment tools and services earn by monetising consumers' data? If so, what incentives does this create? If not, how are they to achieve financial sustainability? This debate is reflected by the varying priorities of different personal data empowerment tools and services. Some, such as the new start-up, **Handshake**, are explicitly focusing on the promise of helping consumers monetise their data by 'renting' it to brands. Others, such as Mydex, do not try to monetise individuals' data. Rather, it charges companies a flat-rate fee for the *process* of sharing data with consumers via Mydex. For the consumer, the value comes from being able to complete data-reliant administrative tasks much more easily, (use value), not from the ability to monetise it (exchange value).

### 4.3.3 Who to trust in a data-driven world?

Knowing who to trust was a constant theme in the interviews. But there are many levels and interpretations of the word 'trust'. Consumers trust energy suppliers to supply energy safely, and they trust banks to keep their financial data safe and secure. But they don't necessarily trust the same organisations to treat them fairly in general, and when it comes to the sharing of personal data, there is widespread mistrust.[105]

While most respondents viewed trust as pivotal to consumers' uptake and use of personal data empowerment tools and services, which in turn will support the emergence of viable commercial models and foster innovation, there was no consensus view as to how higher levels of trust are to be achieved.

Levels of understanding of what might be entailed in building sufficient levels of trust to support the development, operation and sustainability of personal data empowerment tools and services ecosystems varied between regulators and government departments. One benchmark could be the work the Financial Conduct Authority (FCA) has done on building trust in the emerging mobile payments market, with its focus on key issues such as business models and incentives, deep understanding of customer journeys, supporting infrastructure, provisions for information and communication, and accountability and recompense.[106] All these issues apply to the development of the personal data ecosystem: most of the general issues relating to trust building have already been addressed somewhere by someone. The challenge is how to apply these general learnings to a new market and a new situation.

### 4.3.4 Education: how much do consumers need to know?

All respondents accepted that consumer knowledge about such a system and tools will have an important influence on the uptake and use of personal data empowerment tools

[105] Royal Statistical Society (2014)
[106] Financial Conduct Authority (2013)

and services. However, there are currently no clear answers as to what exactly consumers need to be educated about, how this is to be achieved or who should take the lead. Without clarity on these issues, common recognition of the need to educate consumers will not result in effective action.

Personal data empowerment tools and services, and any related services, will rely on complex technologies and sophisticated design processes to work effectively. Education, in the sense of the consumer right to education, will thus be about understanding what could go wrong and how to seek redress, and ensuring consumers know how to identify which product best suits their needs and how to use it safely.

Interviewees were keen to avoid the assumption of knowledge, time and awareness from consumers under current mechanisms of ‘informed consent’, where they are expected to be able to understand and agree to complex provisions relating to how their data is going to be collected, what it’s going to be used for, who it’s going to be shared with, for what purposes and so on.

### 4.3.5 Adoption curves: the generation gap and the digital divide

There were varying opinions with respect to the anticipated rates of adoption of personal data empowerment tools and services. Two particular issues stood out:

- the generation gap – whether it exists, whether it will last, and what it means
- the 'digital divide' between those who have access to digital devices and are comfortable using them, and those who do not have access.

These two issues clearly overlap, but they are different. There are open questions, for example, as to how different generations will respond to personal data empowerment tools and services. There is a widespread assumption that the 'Facebook generation' has a different attitude towards privacy – being more relaxed about the inevitability of sharing personal data in exchange for free services.

Others are more sceptical and feel this relaxed attitude may be the result of naivety. Part of the generation gap may relate to simple life experience. As research for the *midata* programme found, real data management challenges such as those relating to bills, contracts or proving one's identity to access services, affect older people with jobs, kids and homes more than the younger generation.[107] So the younger generation's attitudes and behaviours may change as they grow older, and their expectations of technology may change as their relationship with it matures.

The digital divide[108] poses different issues. The degree to which the divide is fixed (relating to factors such as income, class and education) and to which it is temporary and will close as digital access becomes more and more mainstream (as with other technological advances such as cars, bank accounts, credit cards, central heating or mobile phones) remains an open question. For example, the latest Oxford Internet Institute research identified that 21 per cent of the UK population did not use the internet, and that many of them have no intention to. The survey also found that consumer attitudes towards general internet use is remaining stable, with significant proportions of the population remaining enthusiastically 'pro', pragmatic or 'anti'.[109]

[107] Department for Business, Innovation and Skills (2012)

[108] IPSOS MediaCT (2014), 9.5 million people across the UK aged 15 and over do not have basic online skills, such as the ability to send an email or perform a simple search

[109] Oxford Internet Institute (2013)

# 5 Articulating a new approach

*"We have a responsibility to fight for the sanctioned use of personal data for consumer good."*

Amanda Long, Director General, Consumers International[110]

## 5.1 The need for a new vision

This report has set out how the rising complexity and scale of personal data issues over the last 10 to 15 years has left consumers at a disadvantage. Current protection frameworks have been unable to either promote confidence or prevent exploitation, or enable a more productive application of personal data to meet consumers' own goals and increase innovation. To recap, the key factors driving this are:

- disillusionment with the status quo and lack of faith in the 'notice and consent' model to reassure trust
- ties to the established business model of data gathering and sale as the primary way to provide digital services
- low mainstream awareness of more imaginative ways to control and manage personal data.

Whilst the legislative and regulatory route will continue to provide the backbone for personal data protections, and privacy safeguards and control, this report has also examined the potential of additional approaches from outside the traditional consumer solution space. The report recognises that, just as technology has created new risks and challenges around data, it also presents new opportunities – not least the opportunity to create an additional complement to legislation and regulation.

These new approaches are offering consumer-centric solutions to some difficult problems, which could help consumers achieve better outcomes and businesses and organisations build trust by creating a more equitable way to get value from data. This is not to welcome these as some kind of silver bullet, but more to look beyond avoiding risk by minimising options for use, and towards enabling safe opportunities for consumers to use personal data on their terms to meet their own ends. This will require a more vibrant and ambitious vision of what can be achieved through the application of personal data. The vision and guiding principles below are an attempt to articulate this.

[110] Speech to international conference on Consumer Protection in the digital age, April 2014

## 5.2 A new vision and guiding principles

We feel that now is the right time to articulate a fresh vision of personal data empowerment: one that sees the value of data shared more evenly amongst both the consumers who generate it and the organisations that use it; that balances safeguards with the ability to innovate; and that is based on a deeper, more consumer-centric understanding of our behaviour, needs and desires. To this end, we have created a vision for what personal data empowerment might look like for consumers:

*Consumers are able to exert meaningful control over their personal data. They can determine how data about them and created by them is used and the benefits they wish to derive, within a trusted and safe system.*

A fresh approach is needed in order to enable this vision to become reality. Below, drawn from insights in this report, are a set of starting points or principles for this new approach. These can be used as a guide for strategies, policies or products, or as discussion points to kickstart a new way of doing things within an organisation. They reflect the beginnings of a new approach; one that will hopefully enable more innovative development of consumer-centric solutions to personal data issues across business and policy:

- Personal data can empower consumers towards better individual and collective outcomes – this should be given as much attention as the potential risks and detriments.
- Consumers have an appetite for greater personal data sharing and aggregation but they want a fair value exchange – they should be able to get a clear benefit from sharing their personal data.
- The ability and means to gain a benefit from sharing personal data should be accessible to all consumers, and contribute towards challenging wider detriment
- Consumers want to control how their data is used and by whom – these choices should be organised around an individual's personal preferences, not the organisation's needs.
- Organisations should be transparent in their use of data - information should be accessible and clear so consumers can easily understand what is happening with their data
- Organisations should recognise the importance of transparency in showing they can be trusted to handle personal data – their business model, security standards and lines of accountability should be obvious so that consumers can easily establish whether they meet their trust requirements.
- Consumers' information and data protection rights must be properly enforced and upheld
- Mechanisms to manage privacy and consent should be designed to reflect actual behaviours, not those of the legislators' and regulators' idealised consumer, or data gatherers' convenience.

## 5.3 **Realising the vision**

Many actors will play a part in bringing this vision to reality – their roles are outlined below, along with a reminder of some of the benefits they could gain:

1. Businesses can shape strategy and activity around a new understanding of consumer-centred management of personal data; new ways to deliver value for all. This could benefit organisations by increasing consumer participation and delivering better designed products and services. Engendering trust can make business sense – customers are willing to share more if there is a clear value exchange and they are confident their wishes are respected.

2. Policy makers and regulators can implement further enabling structures so that it is easier for businesses and new entrants to deliver consumer-centred management of personal data across different sectors. Cross-regulator action will be critical in successfully enabling such developments. This could solve or avoid some problems for regulators because consumers empowered with their data (and using services driven by this data) may be more engaged in the market, act more effectively and create more competitive markets.

3. Those working in the consumer interest can articulate this new expectation of businesses and policy makers by fighting for the confident and consumer-controlled use of personal data to achieve better individual and collective outcomes. There is an immediate opportunity to raise awareness and to influence decisions and developments happening now – such as *midata*, European Union Data Protection Regulation reform, Information Economy Council and regulators' third-party intermediary codes of practice – from a joined-up perspective. There is also a longer-term opportunity to influence the debate positively for consumers with an ambitious vision of what they should expect from businesses and organisations in the future, with regard to personal data.

# 6 Conclusion

The scale and speed at which personal data is now created, gathered, applied and repurposed makes unpicking the consumer experience a particularly complex challenge. Consumers have also grown accustomed to the existing, one-sided data deal on offer, despite their reservations, and all parties find it difficult to consider an alternative approach. This report proposed that a new approach is not only possible but necessary to enable consumers to get better outcomes from their personal data, whilst ensuring their protection, security and control.

Research showed that public concern about the use and management of personal data could be overcome if they were able to gain a clear benefit, exert more control over how their data is used and by who, and trust those offering beneficial services. The concept of personal data empowerment, and its practical application through emerging tools and services, has demonstrated how such permissioned sharing might work in practice, and how personal data can provide utility value to help decision-making, identity verification, or control choices.

Interviews with commentators, technologists and regulators raised further questions around whether: aggregating personal data in this way increases risk; focusing only on value diminishes our rights to privacy; it is possible to make the macro-level changes needed in order to create a secure and trusted system within which such new tools and services can operate; the benefits of greater personal data sharing can benefit everyone in society. This led to the proposal of a new approach that recognises how personal data can drive consumer empowerment, while still considering risk and detriments. This vision is intended to complement existing legislative and regulatory measures, and emphasised the value to consumers of being able to control, utilise and share their data, and the need to maintain high levels of security and protection whilst doing so.

Guiding principles developed this further; going forward, each guiding principle will hopefully spark further questions around implementation within a supportive infrastructure. This will require much collaboration and joining up, more discussion, testing out and questioning. The new vision and approach will help to move the conversation around personal data from the limited ‘business value versus consumer risk’ approach to one that encompasses the potential for the consumers who create data and the organisations that use it to both take a share in its value.

Citizens Advice looks forward to working with practitioners, businesses, regulators and policy makers wanting to embark on this process to create an alternative to the status quo, and lay the groundwork for consumers to get a fairer data deal.

# 7 Methodology of research

The Consumer Futures Unit at Citizens Advice commissioned research from Ctrl-Shift to:

- understand different types of personal data empowerment applications in practice, their significance and understand consumer attitudes towards them
- understand the likely implications of developments in personal data empowerment for consumers
- understand current levels of awareness and policy engagement amongst principal stakeholders of the significance of emerging developments in personal data empowerment

The core findings of the report are informed by qualitative data from semi-structured interviews. Interview transcripts were analysed and coded to identify key themes for inclusion in the report.

For the interviews, Ctrl-Shift:

- conducted interviews with key regulators (Ofgem, Ofcom, FCA, ICO, OFT, DECC, EU) involved with personal data and/or the regulated industries
- conducted interviews with a selection of entrepreneurs working within the arena of personal data empowerment, consumer advocacy groups and influential commentators, including Privacy International, Which?, Technology Strategy Board, CDEC, Mydex and MiiCard
- analysed research and interviews on personal data empowerment tools and services to generate an overview of key trends and developments in the market, regulator awareness and responses to these trends, and issues that may need to be addressed over the coming years.

For the research on personal data empowerment tools and services, Ctrl-Shift:

- reviewed its pre-existing directory of consumer empowering services and highlighted those that were relevant to this particular project
- conducted fresh desk research into the highlighted services
- used its ongoing tracking research for *Market Watch* to add new services that were launched during the operation of the project
- analysed the review of existing services to create the typology of personal data empowerment tools and services that is explained below.

## 7.1 Disclosure

Alan Mitchell, one of the researchers on this project, is a non-executive director of Mydex, one of the personal data empowerment tools and services covered in this report. As part of his work for Ctrl-Shift, Alan Mitchell has also acted as an advisor to the UK Department of Business, Innovation and Skills' midata programme.

# 8 Bibliography

Bates R (2014). *Next Generation Intermediaries: Examining A New Approach To Market Engagement*. Available at: http://www.consumerfutures.org.uk/files/2014/01/Next-Generation-Intermediaries.pdf [accessed 4 January 2015].

Bricker D (2013). *Five Global Trends.* June 2013. Ipsos Global Public Affairs [quoted in Deloitte (2013)].

Cavoukian A (2012). *Privacy By Design And The Emerging Personal Data Ecosystem.* October 2012. Available at: https://www.ctrl-shift.co.uk/research/product/70 [accessed 4 January 2015].

CIFAS (2014). *Fraudscape 2014*. March 2014. Available at: https://www.cifas.org.uk/secure/contentPORT/uploads/documents/CIFAS%20Reports/External-CIFAS-Fraudscape-2014-online.pdf [accessed 4 January 2015].

Coll L and Bates R (2014). *Realising Consumer Rights: From JFK To The Digital Age.* Consumer Futures. Available at: http://www.consumerfutures.org.uk/files/2014/03/Realising-consumer-rights.pdf [accessed 4 January 2015].

Consumer Focus (2012). *Digital Behaviour Survey.* March 2012. Available at: http://www.consumerfocus.org.uk/files/2013/02/Digital_Behaviour_Survey_report.pdf [accessed 4 January 2015].

Ctrl-Shift for Consumer Futures (2014). *The Rise Of The Consumer Empowering Intermediary.* January 2014. Available at: http://www.consumerfutures.org.uk/files/2014/01/The-Rise-of-the-Consumer-Empowering-Intermediary-Ctrl-Shift.pdf [accessed 4 January 2015].

Deloitte (2013). *Data Nation 2013: Balancing Growth And Responsibility.* August 2013. Available at: http://www2.deloitte.com/content/dam/Deloitte/uk/Documents/deloitte-analytics/data-nation-2013-balancing-growth-and-responsibility.pdf [accessed 4 January 2015].

Demos (2012). *The Data Dialogue.* September 2012. Available at: http://www.demos.co.uk/publications/thedatadialogue [accessed 4 January 2015].

Department for Business, Innovation and Skills (2012). *Potential Consumer Demand For Midata: Findings Of Qualitative and Quantitative Research.* July 2012. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/34742/12-976-potential-consumer-demand-for-midata.pdf [accessed 4 January 2015].

Direct Marketing Association (2012). *Data Privacy: What The Consumer Really Thinks.* June 2012. Available at: http://www.dma.org.uk/research/data-privacy-what-the-consumer-really-thinks [accessed 4 January 2015].

Economist Intelligence Unit (2013). *Privacy Uncovered: Can Private Life Exist In The Digital Age?* Available at:

http://www.economistinsights.com/sites/default/files/legacy/mgthink/downloads/Privacy uncovered_0.pdf [accessed 4 January 2015].

Financial Conduct Authority (2013). *Mobile Banking And Payments – Supporting An Innovative And Secure Market.* August 2013. Available at: http://www.fca.org.uk/static/documents/thematic-reviews/tr13-06.pdf [accessed 18 January 2015].

GfK (2014). *The Emergence Of The Personal Data Economy.* March 2014. Referenced in Marketing Week (12 March 2014). Available at: http://www.marketingweek.com/2014/03/12/taking-back-control-the-personal-data-economy/

Griffiths C (2014). *Smart and Clear: Consumer Attitudes To Communicating Rights And Choices On Energy Data Privacy And Access.* Consumer Futures. Available at; http://www.consumerfutures.org.uk/files/2014/01/Smart-and-clear.pdf [accessed 4 January 2015].

Information Commissioner's Office (2013). *Annual Track 2013: Individuals.* June 2013. Available at: https://ico.org.uk/media/about-the-ico/documents/1042195/annual-track-2012-individuals.pdf [accessed 4 January 2015].

International Telecommunications Union (2014). *The World In 2014: ITU Facts And Figures.* April 2014. Available at: http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2014-e.pdf [accessed 4 January 2015].

IPSOS MediaCT (2014). *Media Literacy: Understanding Digital Capabilities Follow-up.* September 2013 and March 2014. Available at: http://www.bbc.co.uk/learning/overview/assets/digital_capabilities_2014.pdf [accessed 4 January 2015].

Ofcom (2013). *The Communications Market.* August 2013. Available at: http://stakeholders.ofcom.org.uk/market-data-research/market-data/communications-market-reports/cmr13/ [accessed 20 January 2015].

Ohm, P (2009). *Broken Promises Of Privacy: Responding To The Surprising Failure Of Anonymization.* August 2009. UCLA Law Review, Vol. 57, p. 1701, 2010; University of Colorado Law Legal Studies Research Paper No. 9-12. Available at: http://ssrn.com/abstract=1450006 [accessed 4 January 2015].

Oxford Internet Institute (2013). *Cultures Of The Internet: The Internet In Britain.* Oxford Internet Survey 2013 Report. Available at: http://oxis.oii.ox.ac.uk/reports/ [accessed 4 January 2015].

Pearson S and Casassa Mont M (2011). 'Sticky Policies: An Approach for Managing Privacy across Multiple Parties' *Computer*, vol. 44, no. 9, pp. 60-68, Sept., 2011. Available at: http://www.computer.org/csdl/mags/co/2011/09/mco2011090060-abs.html [accessed 4 January 2015].

President's Council of Advisors on Science and Technology (2014). *Big Data And Privacy: A Technological Perspective.* May 2014. Available at:

http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf [accessed 4 January 2015].

Romanosky S, Telang R. and Acquisti A (2011). 'Do Data Breach Disclosure Laws Reduce Identity Theft?' *J. Pol. Anal. Manage.,* 30: 256–286. doi: 10.1002/pam.20567. Available at: http://onlinelibrary.wiley.com/doi/10.1002/pam.20567/full [accessed 4 January 2015].

Royal Statistical Society (2014). *Public Attitudes Towards The Use And Sharing Of Their Data.* July 2014. Available at: https://www.ipsos-mori.com/researchpublications/researcharchive/3422/New-research-finds-data-trust-deficit-with-lessons-for-policymakers.aspx [accessed 4 January 2015].

RS Consulting for Consumer Futures (2013). *Price Comparison Websites: Consumer Perceptions And Experiences.* July 2013. Available at: http://www.consumerfutures.org.uk/files/2013/07/Price-Comparison-Websites-Consumer-perceptions-and-experiences.pdf [accessed 4 January 2015].

TRUSTe (2014). Consumer Privacy Confidence Index (Research Report). Available at: http://www.truste.com/uk-consumer-confidence-index-2014/ [accessed 16 January 2015].

UK Regulators Network (2014). *The Use Of Data Publication To Enable Reputational Regulation*. July 2014. Available at: http://www.ukrn.org.uk/wp-content/uploads/2014/07/Data-publication-to-enable-reputational-regulation.pdf [accessed 4 January 2015].

Wellcome Trust (2013). *Summary Report Of Qualitative Research Into Public Attitudes To Personal Data And Linking Personal Data.* July 2013. Available at: http://www.wellcome.ac.uk/stellent/groups/corporatesite/@msh_grants/documents/web_document/wtp053205.pdf [accessed 4 January 2015].

3rd Floor North
200 Aldersgate
London EC1A 4HD
Tel: 03000 231 231

www.citizensadvice.org.uk

Citizens Advice is an operating name of
The National Association of Citizens Advice Bureaux.

Registered charity number 279057
Published April 2015