Which?

POLICY RESEARCH REPORT MARCH 2018

The Digital Revolution

Consumers and their data

Research review

Contents

Executive Summary

Consumer data is helping to shape our lives. Sharing and collating information has become ingrained within our culture and, as technology grows, it has become an increasingly common part of our daily interactions with businesses and organisations. This report is the result of a rapid scoping review into consumers' motivations, concerns and knowledge towards data collection and sharing. Following this report, Which? has commissioned its own primary research to further investigate consumers' attitudes and behaviour towards data collection and sharing in more detail.

Research shows that many consumers have adapted to this new data-driven world and enjoy its benefits. Sharing data has become normalised and consumers (albeit to differing extents) are willing to share their data if they can see a direct benefit to them, a societal benefit or if it's required for the product or service to function.

However, this seemingly acquiescent behavioural response should be understood in the context of consumers' knowledge. Most consumers are aware that their browsing history is collected along with data they actively provide, for example their social media posts. However, there is less awareness of some of the other means by which data is collected, for example through the information that others share about them, or through the apps on their phone. Moreover awareness does not equate to understanding – even when consumers are aware of data collection methods they do not necessarily know what this entails or the affects this could have on them. In addition they can often only guess about how their data is used.

Consumers' behavioural response to data collection can also fail to give a true impression of their concerns. The research we have reviewed shows three notable areas of concern:

1. Security: the very tangible outcomes of identity theft and risk of the exposure of financial details are salient to consumers and they raise these spontaneously.
2. Privacy: whilst privacy is not a top of mind concern for consumers (in contrast to the tangible risks associated with security) it is seen as a fundamental right which organisations should respect. Some research indicates that privacy concerns are in decline; however they are still expressed by the vast majority.
3. Third party sharing: this is a fundamental concern to people. We hypothesise that this concern links to consumers' want for control over their data, and

their perception that data should only be collected if they gain something from it (i.e. that there is a transaction which benefits them).

Consumers' desire for control and transparency (arguably the former's proxy) over data collection is a repeated theme in research, but if often left without further exploration. We believe that to enable an intelligent understanding of why this is important we need to place consumers' concerns and needs in a wider socio-cultural context. In this report we have used social contract theory to do this, citing Malhorta, Kim and Agarwal's (2004)[1] theory that organisations and individuals enter into a "social contract" when data is collected. As such the collection of data is only perceived to be "fair" when the consumer is granted control over the information (e.g. through being able to opt-out) and informed about the intended use. It is in this context that consumers' anger at third-party sharing can also be fully understood - they did not decide to enter into a contract with the third-party, and perceive it as having no benefit to them; as such it is considered unfair.

Trust and familiarity are also important concepts which underlie consumer behaviour and attitudes: trust affects whether consumers are happy or not to share their personal data and familiarity with brands is associated with perceptions of good security and less heightened privacy concerns. A useful framework is Gefen, Karahanna and Straub's (2003)[2] definition of trust, which describes it as a willingness to depend on a party to the extent to which they have benevolence, ability and integrity and where consumers can predict the organisations behaviour. This framework can be used to gain a more nuanced understanding of how these differing elements may affect consumers' attitudes and behaviour to data collection and use.

Consumers are engaging in a constantly evolving and growing technology market. It is important to understand how they are engaging and look beyond their behaviour to understand their motivations, their concerns and their knowledge, as well as how concepts such as trust, control and transparency influence these.

KEY POINTS

1. Personal data is defined differently between consumers, and is dependent on context.

What is considered "personal" is linked to how we define privacy and, as such, is a culturally constructed concept that is individual and context dependent. Notions of privacy are linked to wanting to be in control – individuals want to have the power to determine for themselves what personal information is kept private, and the manner in which that information is shared.

There is a mismatch between the legal definition of personal data and what people define it as, and within these definitions there is considerable variability.[3]

[1] Malhorta N, Kim S, Agarwal J (2004) 'Internet users' information privacy concerns (IUIPC): the construct.

[2] Gefen D, Karahanna E, Straub W (2003) 'Trust and TAM in online shopping: an integrated model', MIS Quarterly vol 27(1) p51–90

[3] Digital Catapult (2015) 'Trust in personal data: a UK review'

2. **Consumers' "personal data" is being collected digitally in multiple ways. However, they are not necessarily aware of the extent of data collection, or how it is used.**

   People are increasingly active online, with 6 in 10 (62%) going online through a computer and a similar proportion (66%) through a smartphone. Half of consumers (53%) use online banking and 76% have a social media account. Of those with a social media account, 78% have posted comments or shared videos/photos, a third (32%) have checked in at a location.[4]

   People provide data consciously (eg by giving away information in forms and on social media) and give access to data when they allow cookies and permissions on apps across mobile devices. However, research has found that they are granting permission to apps without much consideration of the request.[5]

   People are sometimes trying to control the data that is collected. For example, by limiting the data they provide (when there is an option to), by 'dirtying' the data (eg providing incorrect or incomplete information) or by limiting their use of products/services which require data disclosure or collection.[6]

3. **In general, consumers are resigned to data disclosure being increasingly part of modern life. However they do not have full knowledge of the ways this data is being collected and used.**

   People are resigned to their data being collected in exchange for use of products or services. Two thirds (65%) say that publicly disclosing information is an increasing part of modern life.[7]

   Knowledge of information being collected through internet use (eg browsing history, transactions) is high, as is knowledge that information that posted on social media is collected. The majority of internet users (87%) say they are aware that their data is being is collected through their internet use,[8] and 70% of online and social media users think that services collect their search history, sites visited, 'likes', location and purchases.[9]

   However, less confident (and often older) internet users are found to be less aware of the different ways companies can collect personal data online, and many are unaware that they are routinely sharing their browser history and location.[10] In addition, there is an apparent gap in knowledge about the information mobile devices are collecting about consumers. Only half (53%) of people who use the internet on their mobiles say they are aware that apps can collect personal information.[11]

[4] Ofcom (2017) 'Adults' media use and attitudes'

[5] Kantar (2014) 'The app environment'

[6] Ofcom (2017) 'Adults' media use and attitudes'

[7] Which? and GMI surveyed 2,067 UK adults online between 12 and 31 December 2014. Data weighted to be demographically representative of the UK population

[8] Ipsos MORI (2016) 'Digital footprints: consumer concerns about privacy and security'

[9] Consumer Focus (2012) 'Consumer Focus digital behaviour survey', cited in the CMA's 'The commercial use of consumer data'

[10] Ipsos MORI (2016) 'Digital Footprints: consumer concerns about privacy and security'

[11] Communications Consumer Panel (2011) 'Online personal data: the consumer perspective'

Consumers are often unclear about what is done with their data once it has been collected. They do not understand how brands make money from collecting, storing and selling their data.[12] They suspect that their information is being used for financial gain, rather than for service improvement.[13] However, they are not always clear how this works in practice; 23% of non-confident online users are unable to name any use that companies may have for their data.[14] In general, research shows that consumers are particularly unclear about what the value would be of their browsing history or shopping behaviour, as opposed to their names and addresses which they are more likely to be aware could be used for direct marketing.[15]

4. People are willing to share their data if there is a benefit in doing so, or if it is necessary for the product/ service to function.

A third (35%) of consumers say they are happy to provide personal information as long as they "get what they want".[16] Skatova, Ng and Goulding (2014) found that for those who were less willing to give their data to aid a wider public good, they wanted assurances of direct personal benefits.[17]

Arguably, concerns about selling of data to third parties[18] may fit with consumers feeling that they are not in an equitable relationship; the personal benefit they receive is not equal to the profit the organisation is gaining from their data.

People may allow their data to be collected if the organisation is going to use it for a "greater good". Skatova, Ng and Goulding (2014) found the majority of respondents were willing to donate personal data to research intended to lead to public good.[19] Civic responsibility has also been identified as a potential reason for the relatively high trust in sharing personal data with government and public services.[20]

Consumer decision-making with regards to data sharing and the collection of consumer data by companies, is subjected to cognitive biases and behavioural limitations. Privacy researcher Prof Alexander Acquisti has identified how choices are affected by incomplete and asymmetric information, bounded rationality, hyperbolic discounting and rational ignorance.[21]

[12] Illuminas for Citizens Advice (2016) 'Consumer expectations for personal data management in the digital world'

[13] Ipsos MORI (2016) 'Digital Footprints: consumer concerns about privacy and security'

[14] Ipsos MORI (2016) 'Digital Footprints: consumer concerns about privacy and security'

[15] Illuminas for Citizens Advice (2016) 'Consumer expectations for personal data management in the digital world'

[16] Ofcom (2017) 'Adults' media use and attitudes'

[17] Skatova A, Ng E, Goulding J (2014) 'Data Donation: sharing personal data for public good'

[18] Ipsos MORI (2016) 'Digital footprints: consumer concerns about privacy and security'

[19] Skatova A, Ng E, Goulding J (2014) 'Data Donation: sharing personal data for public good'

[20] C Strong (2015) 'Private lives? Putting the consumer at the heart of the privacy debate', MRS Delphi Group, p35

[21] Acquisti A and Grossklags J (2006) 'What can behavioural economics teach us about privacy?', presented as a keynote paper at ETRICS 2006

5. People are concerned about security of their personal data and their privacy, although the latter is less 'top of mind'.

Privacy concerns are not top of mind, but when consumers are prompted to think about it, it is clear privacy is important to them. Research by Ofcom[22] and the Communications Consumer Panel[23] found that 9% and 14% of consumers respectively, cite privacy as a concern spontaneously when asked. However, when prompted about privacy issues, 67% of internet users said that they were concerned about their privacy online.[24]

Specifically, people talk about concerns around having their location tracked and their browser history shared[25/26] and of the possibility for an organisation knowing "too much" about them, by linking data such as their name and address with time and location-based information.[27] In experimental research it was found that people are (hypothetically) prepared to pay to keep some of their data private.[28]

While consumers are uniformly concerned about privacy, albeit only when prompted, concern about security is more varied. When prompted, 7 in 10 (72%) say they are concerned that companies will fail to keep their data safe.[29] However, Ipsos MORI found that non-confident users of the internet are less likely than confident users to say they are worried about the safety of their personal details. Users with lower confidence tend to be older[30] and therefore less likely to be doing online transactions such as online banking,[31] therefore they may not feel the risk is relevant to them.

People are particularly concerned about the passing on of data to third parties. For example, 68% said they are concerned about their data being sold on to third parties for marketing purposes[32] and separate research found that 63% of people said that companies selling anonymous data is a concern.[33]

Those who are confident using the internet are more aware of concerns around personal information and how it is used for commercial purposes, but they do not always act on that awareness.[34]

[22] Ofcom (2017) 'Adults' media use and attitudes'

[23] Communications Consumer Panel (2011) 'Online personal data: the consumer perspective'

[24] Ipsos MORI (2016) 'Digital Footprints: consumer concerns about privacy and security'

[25] Kantar (2014) 'The apps environment'

[26] Ipsos MORI (2016) 'Digital Footprints: consumer concerns about privacy and security'

[27] Illuminas for Citizens Advice (2016) 'Consumer expectations for personal data management in the digital world'

[28] Skatova et al 'Perceived risk of personal data sharing'

[29] Ipsos MORI (2014) 'Public attitudes to the use and sharing of people's data', cited in Ipsos Mori (2016) 'Digital footprints: consumer concerns about privacy and security'

[30] Ipsos MORI (2016) 'Digital Footprints: consumer concerns about privacy and security'

[31] Ofcom (2017) 'Adults' media use and attitudes'

[32] ICO (2016) Annual Track

[33] Ipsos MORI (2014) 'Public attitudes to the use and sharing of people's data', cited in Ipsos Mori (2016) 'Digital footprints: consumer concerns about privacy and security'

[34] Ipsos MORI (2016) 'Digital Footprints: consumer concerns about privacy and security'

6. Transparency and control of data is important to consumers.

7 in 10 consumers don't believe they currently have control over how their data is collected and used by companies.[35]

Consumers want to be clearly informed about how their data will be used, to be able to choose whether to opt-in and out of various items,[36] and to have a say over who their data is shared with and how long it is retained for.[37]

The importance of control can be understood in the context of social contract theory.[38] When people's data are collected they enter into a "social contract" with that organisation. As with any social contract, both parties need to gain something from being in the contract, consumers want to have control to some degree (eg change terms, exit), and to be aware of the terms of the contract (eg privacy policies). If these are violated the person becomes concerned.

Sharing data with third parties is particularly concerning to consumers, as it violates social contracts on all levels: they do not agree to enter a social contract with the third party – there is therefore no equitable relationship; they do not have control over the relationship, and they do not have any awareness of the organisations' privacy practices (found to be an influence on people's level of concerns).

7. Trust in services is a key factor in data sharing decisions; it is used by consumers to assess whether an organisation will keep their data private and secure. Familiarity is used as a heuristic to determine whether an organisation is trustworthy.

People place trust as the top reason when asked to rank factors that made them happy to share their information with companies.[39] Research has indicated that pre-existing trust in an organisation is used as a factor in deciding whether or not to share personal information with a party online.[40]

Trust in relation to e-commerce has been defined by Gefen et al[41] as
a willingness to depend on a party based on the extent to which they:
1) behave in way that doesn't just serve their own interests (benevolence)
2) have the skills and competencies to be good at their role (ability),
3) adhere to a set of principles that are found to be honest and fair (integrity)
4) and where consumers have knowledge that allows them to predict the organisation's behaviour (predictability).[42]

[35] Ipsos MORI (2016) 'Digital footprints: consumer concerns about privacy and security'

[36] Communications Consumer Panel (2011) 'Online personal data: the consumer perspective'

[37] Illuminas for Citizens Advice (2016) 'Consumer expectations for personal data management in the digital world'

[38] Malhorta N, Kim S, Agarwal J (2004) 'Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model'. Information Systems research, December 2004, vol 15 (4) p336–355

[39] DMA (2018) 'Data privacy: What the consumer really thinks'

[40] Ipsos MORI (2016) 'Digital footprints: consumer concerns about privacy and security'

[41] Gefen D, Karahanna E, Straub W (2003) 'Trust and TAM in online shopping: an integrated model', MIS Quarterly vol 27(1) p51-90

[42] Definitions of 'benevolence', 'ability' and 'integrity' are based on Mayer et al (1995), 'An integrative model of organisational trust', The Academy of Management review, July 1995

Trust is linked to familiarity. Research has found that familiarity with brands is associated with perceptions of good security[43] and less heightened privacy concerns.[44] Familiarity attenuates perceptions of risk, as people habituate to the risk and start to accept it.[45] Well-known brands are considered to have more to lose reputationally if there was a data breach.[46] Similarly consumers feel that global brands would need to be responsible in their data practices as there would be "too much at stake" for them to risk bad practice.[47]

Consumer research has found that 57% of people do not feel that businesses are open and transparent about how they collect and use consumers' data.[48] Separate research has found that consumers want organisations to be transparent about what they are doing.[49] And there is research which suggests that, at least for some purposes (eg marketing), by simply being transparent about the motive, consumers may find it more acceptable.[50]

8. The detriment that consumers have experienced as a result of data sharing is unclear.

There is little detailed information on the direct (eg identify theft) and indirect (eg adjusted pricing) detriment that consumers perceive and experience. Despite some high profile cases of data loss by institutions, Ofcom estimates consumer detriment to be low.[51] This has been identified as an area for more research.

There is a lack of research which offers a comprehensive view on the incidence of consumer detriment, and the nature of the harm it can have. Research tends to focus on safety/security risks and detriment caused by security transgressions. Although there have been some high-profile breaches of data security, there is less published research on detriment as a consequence of privacy violations. We have not identified detailed consumer research on the nature, likelihood and impact of harm that is possible by sharing data in the future.

9. Areas for further research.

While there is an abundance of research on consumer behaviour and concerns regarding data collection, there are some notable gaps in our understanding of this area, which we will look to address through further primary research. In particular, we consider the most important of these to be:

- A more in-depth and nuanced understanding of consumers' concerns by considering specific data types, data collection method and use (and risks attached to any single or combination of these).

[43] Ipsos MORI (2016) 'Digital footprints: consumer concerns about privacy and security'

[44] Sheehan K, Hoy G (2000) 'Dimensions of privacy concern among online consumers', Public Policy Marketing vol 19(1) p62-73

[45] Store P, Fischhoff B, Lichenstein S (1982) 'Why study risk perception?' Risk analysis, vol 2, no 2, cited in Schmidt M (2004) 'Investigating risk perception: a short introduction'

[46] Ipsos MORI (2016) 'Digital footprints: consumer concerns about privacy and security'

[47] Illuminas for Citizens Advice (2016) 'Consumer expectations for personal data management in the digital world'

[48] ICO (2016) Annual Track

[49] Ipsos MORI (2016) 'Digital footprints: consumer concerns about privacy and security'

[50] Ipsos MORI (2016) 'Digital footprints: consumer concerns about privacy and security'

[51] Ofcom (2017) 'Adults' media use and attitudes'

- Understanding the detriment to consumers of collecting their data and how the risks or likelihood of harm may change in the future. Are consumers experiencing detriment as a result of their data being collected and, if so, what is the detriment and how is it impacting them? How will impact or risk of detriment change as the digital revolution marches on?
- Exploring how concepts of trust, privacy, transparency and control affect consumers' behaviour and attitudes towards data collection now, and in the future. There has been little explanation of what these concepts actually mean to consumers in the context of data collection, and how they interrelate. These concepts provide the foundations of how consumers engage with data collection; it is important that we have an understanding of these in order to inform policy discussions.
- Understanding consumers' views about rapid changes in data collection methods, data manipulation techniques, future uses of data and what the impacts might be for individual consumers and the markets they take part in.

1 What is personal data?

Personal data is defined differently between consumers, and is dependent on context

There is a mismatch between the legal definition of personal data and what people define it as, and within these definitions there is considerable variability.[52]

What is considered "personal" is linked to how we define "privacy" and, as such, is a culturally constructed concept that is individual and context dependent.

Notions of privacy are linked to wanting to be in control – individuals want to have the power to determine for themselves what personal information is kept private, and the manner that any information is shared.

Personal data is legally defined as information that a person can be identified from.[53] Sometimes this data is obvious (eg contact details) but it also covers information that could easily be analysed or combined to create information about an identifiable individual, for example transaction information. Personal data is therefore, a name, address, email, telephone number, image, date of birth or geolocation data, but also information such as a person's hobbies, browsing history, medical history, or financial status.

In consumer research, however, it has been found that there is variability between consumers as to how they define personal data, and that it does not necessarily match the legal definition. Digital Catapult's 2015 online survey of 4,005 people, found that 96% of consumers claimed that they could define personal data, but only 64% defined it as "all information about me in existence", and there was a large variance between people's definitions.[54]

What is considered personal data can also be linked to what we would prefer to keep private about ourselves. Psychologists Luft and Ingham describe privacy as being about the boundaries between your "inner and outer worlds".[55] They developed the "Johari Window", which provides a useful framework illustrating how these outer and inner worlds are divided by whether the information is known to the individual and/or the world (organisations).[56]

[52] Digital Catapult (2015) 'Trust in personal data: a UK review'

[53] ICO (2012) 'What is personal data? A quick reference guide'

[54] Digital Catapult (2015) 'Trust in personal data: a UK review'

[55] Luft J, Ingham H, 'The Johari window, a graphic model of interpersonal awareness; proceedings of the western training laboratory in group development', UCLA, 1955. Cited in C Strong (2015) 'Private lives? Putting the consumer at the heart of the privacy debate', MRS Delphi Group

[56] Luft J, Ingham H, 'The Johari window, a graphic model of interpersonal awareness; proceedings of the western training laboratory in group development', UCLA, 1955. Cited in C Strong (2015) 'Private lives? Putting the consumer at the heart of the privacy debate', MRS Delphi Group

Figure 1: Johari Window by Luft and Ingham[57]

	UNKNOWN SELF	KNOWN SELF
KNOWN OTHER	**BLIND SELF** Where an organisation may know something about you that you don't know yourself	**OPEN SELF** Knowledge about yourself that is shared by you and the organisation
UNKNOWN OTHER	**UNKNOWN SELF** Information about yourself that is not consciously known by yourself or by the organisation	**HIDDEN SELF** Information that you know about yourself, but the organisation doesn't. Much of which you'd consider private.

The "hidden self" would be personal information that consumers want to keep private and the "blind self" – where an organisation may know something about a consumer that they themselves do not know.

Abrams[58] has produced a taxonomy to categorise the differing kinds of personal data and the level of awareness that consumers have about it being collected. However, more research is required on the difference in knowledge around the data that consumers are aware of and want to hide, and the data that is kept about consumers without their knowledge.

There also seems to be a gap in the research about what privacy means in practical terms. How important is it to be private? What things should be private, is it all things deemed personal? How does one decide if a company knows too much about a consumer or their habits? What actual harm does it is cause when a company knows something about you which is deemed private? How closely related are 'private' and personal identifiable data?

[57] Luft J, Ingham H, 'The Johari window, a graphic model of interpersonal awareness; proceedings of the western training laboratory in group development', UCLA, 1955. Cited in C Strong (2015) 'Private lives? Putting the consumer at the heart of the privacy debate', MRS Delphi Group

[58] Abrams, The Information Accountability Foundation, 'The origins of personal data and its Implications for governance'

Figure 2: Taxonomy of data by Abrams[59]

Category	Sub-category	Example	Level of individual awareness
Provided:	Initiated	Applications, credit card purchases	High
	Transactional	Bills, public health records, surveys	High
	Posted	Social media	High
Observed:	Engaged	Cookies, enabled location sensor on devices, purchases on loyalty card.	Medium
	Not anticipated	Data from sensor technology on devices (eg car)	Low
	Passive	Facial image on CCTV, wi-fi readers that establish location	Low
Derived:	Computational	Average purchase per visit	Medium to Low
	Notional	Classification based on common attributes	Medium to Low
Inferred:	Statistical	Credit scores	Low
	Advanced analytical	Risk of developing a disease based on multiple risk factors	Low

[59] Abrams, The Information Accountability Foundation, ‘The origins of personal data and its implications for governance’

2 Consumers' behaviour in relation to data collection

Consumers' data is being collected digitally in multiple ways

Consumers are increasingly active online, with 6 in 10 (62%) going online through a computer and a similar proportion (66%) through a smartphone. Half of consumers (53%) use online banking and 76% have a social media account. Of those with a social media account, 78% have posted comments or shared videos/photos, a third (32%) have checked-in at a location.[60]

People provide data consciously (eg by giving away information in online forms, on social media) and give access to their data when they allow cookies and permissions on apps. However, research has found that consumers are granting permission to apps to access information on their devices without much consideration of the request.[61]

People are sometimes trying to control the data that is collected. For example, by limiting the data they provide when there is an option, by 'dirtying' the data (eg providing incorrect or incomplete information) or by limiting their use of products/services which require data disclosure or collection.[62]

How are people going online?

There is now a proliferation of ways to access the internet. Ofcom found that two thirds (66%) of people have gone online through a smartphone; 6 in 10 (62%) through a computer and half (49%) had used a tablet.[63] 14% of people have used a Smart TV to go online and 3% wearable technology.[64] 7 in 10 (67%) of smartphone users say they have used public wi-fi.[65] This increases to three quarters (76%) of younger adults (16-24 years).

What are people doing online?

People are using the internet for a multitude of tasks. Ofcom found that in the last week half or more of people used the internet for online banking (53%),

[60] Ofcom (2017) 'Adults' media use and attitudes'

[61] Kantar (2014) 'The app environment'

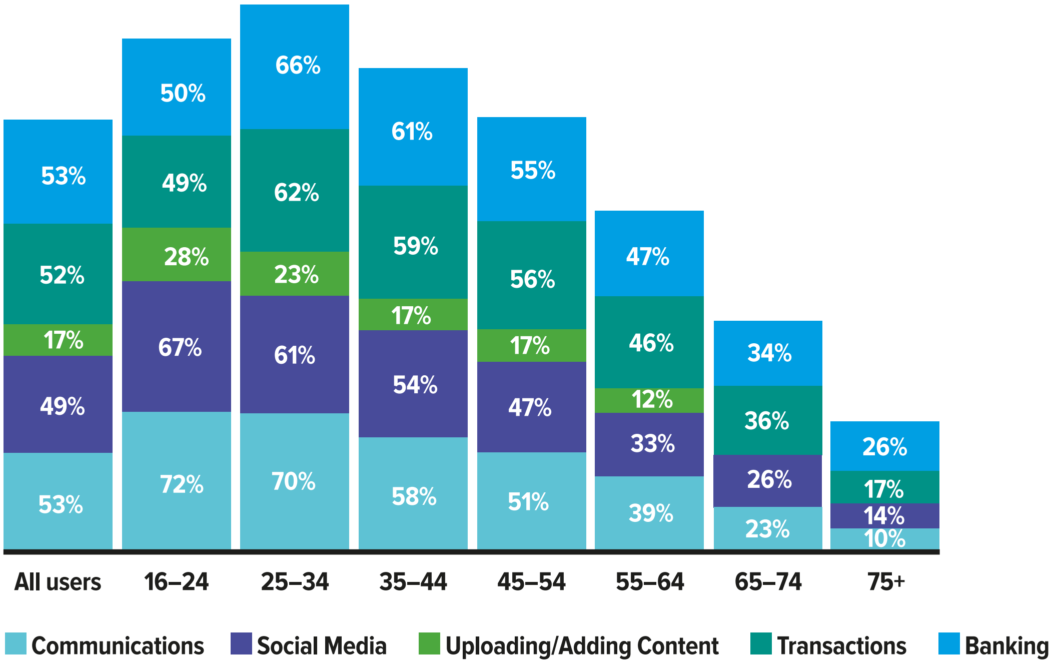
[62] Ofcom (2017) 'Adults' media use and attitudes'

[63] Ofcom (2017) 'Adults' media use and attitudes'

[64] Ofcom (2017) 'Adults' media use and attitudes'

[65] Ofcom (2017) 'Adults' media use and attitudes'

Figure 3: Activities on the internet in the last week, by age



Source: Ofcom 'Adults' media use and attitudes' [66]

financial transactions (52%), communications (53%) and social media (49%).[67] There is a trend for social media use and communications to increase as age decreases and banking and online transactions show the same trend from the age of 25 years.

Many internet users are also using online communication methods. Half (46%) of internet users say they have communicated via instant messaging (eg Facebook chat, Skype, Snapchat) in the last week, a quarter (24%) have made video calls (eg via Facetime, Skype) and 16% have made voice calls (eg via Facetime).[68] Young people are more likely than older people to be doing all of these.

Overall three quarters (76%) of internet users say they have a social media account.[69] Of these users 8 in 10 (78%) say they have posted comments or shared videos/photos, a third (32%) say they have checked-in at a location before and a quarter (25%) said they have said they have liked/ shared/ commented to win prizes.[70]

Smartphones are used in a number of ways – 8 in 10 (81%) smartphone users say they have used maps/ satellite navigation on their phone and 3 in 10 (28%)

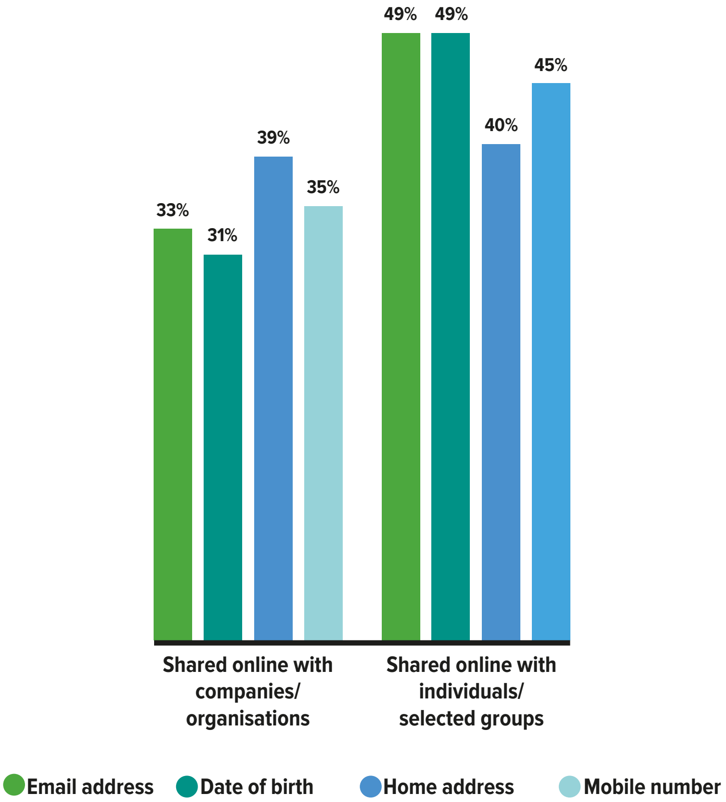
[66] Ofcom (2017) 'Adults' media use and attitudes'
[67] Ofcom (2017) 'Adults' media use and attitudes'
[68] Ofcom (2017) 'Adults' media use and attitudes'
[69] Ofcom (2017) 'Adults' media use and attitudes'
[70] Ofcom (2017) 'Adults' media use and attitudes'

people have used their phone for a contactless payment in the past.[71] Social media users are also using their phone with communication apps such as WhatsApp (45%) and Snapchat (23%).[72]

What data do consumers share?

In the course of accessing services, consumers may provide personal information, such as socio-demographic, contact details and financial information. However, as more time is spent online, 'behavioural data' is created. Examples of behavioural data are records of websites visited and adverts clicked on, data on consumers' use of games apps, and telematics data captured by motor insurance companies.[73] Consumers are less likely to think of this data as 'personal'.[74] However because behavioural data is observed, rather than actively offered by the consumer, they are less likely to be aware of this data being recorded.

Figure 4: Personal data shared online



Source – *Question:* Please indicate whether the following pieces of personal information you have voluntarily provided online through social networks, public registers, academic institutions etc. Which? and GMI surveyed 2,067 UK adults online between 12 and 31 December 2014. Data weighted to be demographically representative of the UK population.

[71] Ofcom (2017) 'Adults' media use and attitudes'

[72] Ofcom (2017) 'Adults' media use and attitudes'

[73] CMA (2015) 'The commercial use of consumer data'

[74] Illuminas for Citizens Advice (2016) 'Consumer expectations for personal data management in the digital world'

The chart on page 15 shows that consumers are consciously providing data both to "select groups" online as well as making it publicly available; half (49%) of consumers say have shared their date of birth to a "select group" online, 45% have shared their mobile number and 4 in 10 (40%) have shared their home address.[75]

People may not be fully aware of the extent or types of data they have agreed to share. This is often the case with agreeing to permissions on apps. Research with app users found that they paid little attention to the "permissions" requested by apps and used the apps without looking at them.[76] Acceptance of permissions was found to depend on the following factors: the extent to which the person wanted to use the app; lack of experience/knowledge with apps; implicit trust in app stores; and word of mouth and peer influence.[77]

How are consumers maintaining their privacy?

Qualitative research by Ofcom has found that awareness of privacy issues has increased over the last few years.[78] They found that a number of people were using tactics to manage these concerns, for example by managing their privacy settings and using multiple email addresses. Another tactic is to "dirty" the data – a quarter (27%) of internet users say they give out inaccurate or false details on some websites to protect their personal identity online, with this rising to a third (35%) for those aged 16–24years.[79]

People also try to limit the data they give away about themselves when they have the option to, for example only filling out the mandatory parts of online forms. Two in five (42%) say they always opt out of sharing information with the main company and a similar percentage (41%) with partner companies; 32% say they often do this with the main company and 26% with partner companies.[80] A third (33%) of people say they often or always use the private mode on their internet setting and nearly 4 in 10 (38%) often or always change their browser setting to block cookies.[81] Amending settings is another tactic: over half (54%) of people who own a smartphone say they have adjusted the device or app settings to limit the amount of information they share with others; 4 in 10 (40%) of all consumers say they have turned off the location tracking feature on their smartphone.[82]

There are people who take more extreme action to limit the amount of data they share, by deciding not to use a product or service. For example over half

[75] Which? and GMI surveyed 2,067 UK adults online between 12 and 31 December 2014. Data weighted to be demographically representative of the UK population

[76] Kantar (2014) 'The app environment'

[77] Kantar (2014) 'The app environment'

[78] Ofcom (2017) 'Adults' media use and attitudes'

[79] Ofcom (2017) 'Adults' media use and attitudes'

[80] Ipsos MORI (2016) 'Digital footprints: consumer concerns about privacy and security'

[81] Which? and GMI surveyed 2,067 UK adults online between 12 and 31 December 2014. Data weighted to be demographically representative of the UK population

[82] Which? and GMI surveyed 2,067 UK adults online between 12 and 31 December 2014. Data weighted to be demographically representative of the UK population

(54%) of people say they have decided not to install, or uninstalled, an app on their smartphone, because of the amount of personal information they would have to provide.[83]

However, an unintended consequence of not engaging with services and/or products is that consumers may experience social or economic detriment, by excluding themselves from such digital activity. Therefore some consumers are trying to manage data sharing/collection by using more subtle strategies. For example they are more likely to say that they will sign up for emails than sign up for text messages.[84] This may be because email is seen to be less intrusive than text messages, and is therefore less likely to be seen as an invasion of privacy. Another strategy is putting filters in place to manage spam.

Other research has found that teenagers are taking steps to manage their various social media accounts by using different networks to communicate with different connections and for different purposes. Thereby protecting their privacy, whilst still taking part in the commercial digital world.[85]

How do consumers maintain the security of their data?

Ipsos MORI found that three quarters (74%) of internet users always or often have anti-virus installed and over half (55%) say they always or often make sure there is a padlock/secure web address when they are purchasing a product or service online.[86] However qualitative research indicates that security concerns can be with organisations not using consumers' data responsibly, or with organisations storing personal data being hacked, rather than security of data at the consumer end.[87]

[83] Which? and GMI surveyed 2,067 UK adults online between 12 and 31 December 2014. Data weighted to be demographically representative of the UK population

[84] DMA (2012) 'Data privacy: what the consumer really thinks'

[85] C Strong (2015) 'Private lives? Putting the consumer at the heart of the privacy debate', MRS Delphi Group

[86] Ipsos MORI (2016) 'Digital footprints: consumer concerns about privacy and security'

[87] Ipsos MORI (2016) 'Digital footprints: consumer concerns about privacy and security'

3 Consumers' knowledge

Consumer's knowledge of digital data collection and use is limited

People are resigned to their data being collected in exchange for use of products or services.[88]

Knowledge of information being collected through internet use (eg browsing history, transactions) is high, as is knowledge that information posted on social media may be collected and used.

However, less confident (and often older) internet users are found to be less aware of the different ways companies can collect personal data online, and many are unaware that they are routinely sharing their browser history and location.[89]

There is an apparent gap in knowledge about the information mobile devices are collecting about consumers. Only half (53%) of people who use the internet on their mobiles say they are aware that apps can collect personal information.[90]

People are often unclear on what is done with their data once it has been collected. They do not understand how brands make money from collecting, storing and selling their data.[91] **They suspect that their information is being used for financial gain, rather than for service improvement.**[92] **However, they are not always clear how this works in practice.**[93]

In general, research shows that consumers are particularly unclear about what the value would be of their browsing history or shopping behaviour, as opposed to their names and addresses which they are more likely to be aware of being used for direct marketing.[94]

[88] Which? and GMI surveyed 2,067 UK adults online between 12 and 31 December 2014. Data weighted to be demographically representative of the UK population

[89] Ipsos MORI (2016) 'Digital footprints: consumer concerns about privacy and security'

[90] Communications Consumer Panel (2011) 'Online personal data: the consumer perspective'

[91] Illuminas for Citizens Advice (2016) 'Consumer expectations for personal data management in the digital world'

[92] Ipsos MORI (2016) 'Digital footprints: consumer concerns about privacy and security'

[93] Ipsos MORI (2016) 'Digital footprints: consumer concerns about privacy and security'

[94] Illuminas for Citizens Advice (2016) 'Consumer expectations for personal data management in the digital world'

Consumers' knowledge of data collection

The majority of internet users (87%) say they are aware that their data is being is collected through their internet use.[95] However when this was discussed with consumers, less confident (and often older) internet users are found to be less aware of the different ways companies can collect personal data online. Many are unaware that they are routinely sharing their browser history and location.[96]

Awareness that online activity, such as browsing history, is collected is high but there is a lack of awareness of the detail of data collection. For example almost two thirds (64%) of internet users say they are aware that cookies are used to collect data about the websites they visit. However in discussion it was found that while confident users are aware of cookies and what they do, some less- confident users only have a vague awareness.[97]

In addition, awareness of data collection differs according to type of data collected and whether people have actively shared it or it has been observed. For example, 68% of people believe that data about their searches is collected and 70% that data about the products and services they have purchased is collected. However, only 38% believe that data about their internet connection (IP) is collected.[98] With regards to social media – 68% of people who have a social networking profile say they are aware that companies can gather information from their profiles[99] and separate research found that 70% of online and social media users thought that these services would collect their search history, sites visited, 'likes', location and purchases.[100] However, only 17% believe that information that others share about them online is collected.[101]

Mobile apps are a key area where knowledge is lacking, only half (53%) of people who use the internet on their mobiles say they are aware that apps can collect personal information.[102] Research with app users found that some do not realise that the apps run in the background when their phone is locked or when an app is exited. Many do not know what permissions they have accepted on frequently-used apps, and do not consider the permissions when downloading the app. Not all know they have given permission for browser history data to be shared, their location and call logs. All of these are seen as invasive.[103]

Consumers' knowledge of use of data

Research has found that people are resigned to the fact that data sharing is required to access our increasingly digital world.[104]

[95] Ipsos MORI (2016) 'Digital footprints: consumer concerns about privacy and security'

[96] Ipsos MORI (2016) 'Digital footprints: consumer concerns about privacy and security'

[97] Ipsos MORI (2016) 'Digital footprints: consumer concerns about privacy and security'

[98] Doteveryone (2018) People, Power and Technology: The 2018 Digital Attitudes Report

[99] Communications Consumer Panel (2011) 'Online personal data: the consumer perspective'

[100] Consumer Focus (2012) 'Consumer Focus digital behaviour survey', cited in CMA (2015) 'The commercial use of consumer data'

[101] Doteveryone (2018) People, Power and Technology: The 2018 Digital Attitudes Report

[102] Communications Consumer Panel (2011) 'Online personal data: the consumer perspective'

[103] Kantar (2014) 'The apps environment'

[104] Turiw J, Hennessy M, Draper N (2015) 'The trade-off fallacy'

Two thirds (65%) say that publicly disclosing information is an increasing part of modern life.[105]

In general, over half (58%) of consumers believe that if someone wants to be able to use the full range of products and services there is no alternative to disclosing data;[106] this does not feel like a fair choice to consumers.[107] There is concern that in the future, digital brands will be able to dictate any terms they want and people will have to submit to these terms in order to fully participate in the digital world.[108]

People also sometimes feel they do not have a choice about providing their information, as the alternative is to not use the product/service.[109]

> *'To be part of the modern world, we have to be on all of the key sites: Facebook, Linkedin, WhatsApp you have no choice. But the problem is that they have a monopoly because of their size. If you weren't on these sites, you couldn't have a social life. If I wasn't on LinkedIn, people would ask what I'm trying to hide.'*
>
> Confident/informed, male, age 31, social grade C1, London[110]

An example of this unfair balance is where consumers feel obligated to grant apps permission to access information about the consumer via their digital device in order to download and use the app. This can be a source of frustration.[111] In the end, acceptance of upfront permissions was found to depend on the following factors: the extent to which the person wanted to use the app; lack of experience/knowledge with apps; implicit trust in app stores; and word of mouth and peer influence.[112]

People do not appear to be clear about what is done with their data. Ipsos MORI report that consumers are unsure how organisations are using their data.[113] Currently terms and conditions are the primary way in which most companies inform consumers about how they use their data. However, the majority (57%) of internet users say they rarely or never read T&Cs statements on websites[114] (and it is likely that this percentage could be an overestimation due to the tendency towards responses that are socially desirable).

[105] Which? and GMI surveyed 2,067 UK adults online between 12 and 31 December 2014. Data weighted to be demographically representative of the UK population

[106] Which? and GMI surveyed 2,067 UK adults online between 12 and 31 December 2014. Data weighted to be demographically representative of the UK population

[107] Illuminas for Citizens Advice (2016) 'Consumer expectations for personal data management in the digital world'

[108] Illuminas for Citizens Advice (2016) 'Consumer expectations for personal data management in the digital world'

[109] Illuminas for Citizens Advice (2016) 'Consumer expectations for personal data management in the digital world'

[110] Illuminas for Citizens Advice (2016) Consumer expectations for personal data management in the digital world p41.

[111] Kantar (2014) 'The apps environment'

[112] Kantar (2014) 'The apps environment'

[113] Ipsos MORI (2016) 'Digital footprints: consumer concerns about privacy and security'

[114] Ipsos MORI (2016) 'Digital footprints: consumer concerns about privacy and security'

People feel the information about how data is used is probably out there, but that it has been deliberately made difficult to find and it would take time and effort to uncover.[115] Illuminas ran a series of discussion groups to research consumer understanding of the digital world. They found that consumers do not understand how brands make money from collecting, storing and selling their data.[116]

> *'Why would anyone be interested to know about what I'm browsing for? I just don't get it'*
>
> Confident/informed, female, age 25, social grade C1, London, 2016 [117]

Research found that the majority (79%) of consumers think their personal data is being used by organisations solely for economic gain.[118] Separate research found that consumers suspect that their information is being used for financial gain, rather than for service improvement.[119] However they are not always clear how this works in practice; 23% of non-confident users in Ipsos MORI's research are unable to name any use that companies may have for their data.[120] In general, consumers are particularly unclear about what the value would be of their browsing history or shopping behaviour, as opposed to their names and addresses, which they are more likely to be aware could be used for direct marketing.[121]

[115] Ipsos MORI (2016) 'Digital footprints: consumer concerns about privacy and security'

[116] Illuminas for Citizens Advice (2016) 'Consumer expectations for personal data management in the digital world'

[117] Illuminas for Citizens Advice (2016) 'Consumer expectations for personal data management in the digital world', p19

[118] Digital Catapult (2015) Trust in personal data; a UK review.

[119] Ipsos MORI (2016) 'Digital footprints: consumer concerns about privacy and security'

[120] Ipsos MORI (2016) 'Digital footprints: consumer concerns about privacy and security'

[121] Illuminas for Citizens Advice (2016) 'Consumer expectations for personal data management in the digital world'

4 Consumers' motivations for sharing

People are willing to share their data if there is a benefit in doing so, or if it is necessary for the product/ service to function. There are also cognitive biases and behavioural factors which pre-dispose people to sharing data

A third (35%) of consumers say they are happy to provide personal information as long as they "get what they want".[122] **Ng and Goulding (2014) found that for those who were less willing to give their data to aid a wider public good, they wanted assurances of direct personal benefits.**[123]

People may allow their data to be collected if the organisation is going to use it for a "greater good". Skatova, Ng and Goulding (2014) found the majority of respondents are willing to donate personal data to research intended to lead to public good.[124] **Civic responsibility has also been identified as a potential reason for the relatively high trust in sharing personal data with government and public services.**[125]

The decision as to whether to allow access to one's data is subject to cognitive biases and behavioural limitations. Privacy researcher Prof Alexander Acquisti has identified how choices are affected by: incomplete and asymmetric information: bounded rationality: hyperbolic discounting; rational ignorance.[126]

When reading consumer research, three factors emerge as variables related to motivations for data sharing: 1) if there is personal benefit to the consumer 2) if it is for a "greater good" and 3) the extent that it is needed to access a service/product. Some products/services may fit all three motivations, while others may only fit one.

[122] Ofcom (2017) 'Adults' media use and attitudes'

[123] Skatova A, Ng E, Goulding J (2014) 'Data Donation: sharing personal data for public good'

[124] Skatova A, Ng E, Goulding J (2014) 'Data Donation: sharing personal data for public good'

[125] C. Strong (2015) 'Private lives? Putting the consumer at the heart of the privacy debate', MRS Delphi Group, p35

[126] Acquisti. A and Grossklags. J. (2006) What can behavioural economics teach us about privacy? Presented as a Keynote Paper at ETRICS 2006.

Personal benefit

A sizeable minority of consumers (35%) say they are happy to provide personal information as long as they "get what they want".[127] For example, Ipsos MORI found that nearly 1 in 5 (16%) confident internet users said that they are willing to give access to their personal information in exchange for benefits such as free access to a website.[128] Separate research found that 38% of 18–24 year olds said they would be happy to share data about their spending habits, to help them save money via products such as new saving accounts and shopping discounts.[129] In qualitative research despite people initially not supporting the collecting of their data, when they deliberated over it they concluded that they would prefer to provide their data in return for free use of websites, than have to pay.[130]

Skatova, Ng and Goulding (2014)[131] found that for those who were less willing to give their data to aid a wider public good, they wanted assurances of direct personal benefits. Higher trust in giving government and public services personal data could also be explained with the theory that the benefits that individuals can gain from it are clearer.[132] Contrastingly, concerns about selling of data to third parties [133] may fit with consumers feeling that they are not in an equitable relationship; the personal benefit they receive is not equal to the profit the organisation is gaining from their data.

Societal benefit

Research suggests that people may allow their data to be collected if the organisation is going to use it for a "greater good", although people's willingness to do this will be affected by individual differences. This pro-social behaviour was found by Skatova, Ng and Goulding's study (2014)[134] where the majority of respondents were willing to donate personal data to research intended to lead to 'public good'. For this willing group their motivation to donate personal data was associated with concern for others. This is also supported by research which found more support than opposition for sharing health data with commercial organisations for the specific purposes of health research (54% and 26% respectively).[135] Civic responsibility has also been identified by some authors as a potential reason for the relatively high trust in sharing personal data with government and public services.[136]

Functionality for product or service

When people were asked in a deliberative setting their views on certain permissions often required by apps, the only permissions that people said they would ideally want to accept are those which were necessary for the main

[127] Ofcom (2017) 'Adults' media use and attitudes'

[128] Ipsos MORI (2016) 'Digital footprints: consumer concerns about privacy and security'

[129] ODI (2018) British consumer attitudes to sharing personal data

[130] Ipsos MORI (2016) 'Digital footprints: consumer concerns about privacy and security'

[131] Skatova A, Ng E, Goulding J (2014) 'Data Donation: sharing personal data for public good'

[132] C.Bates, P. Gooch, H.Lewis. (2014) Data Nation 2014. Putting customers first. Deloitte.

[133] Ipsos MORI (2016) 'Digital footprints: consumer concerns about privacy and security'

[134] Skatova A, Ng E, Goulding J (2014) 'Data Donation: sharing personal data for public good'

[135] Ipsos MORI, 2015, "public attitudes to commercial access to health data" (for the Wellcome Trust).

[136] C Strong (2015) 'Private lives? Putting the consumer at the heart of the privacy debate', MRS Delphi Group, p35

function of the app, eg access to a calendar if it is a diary app or the camera if it is a photography app.[137] Researchers have also suggested that for public services the higher trust may stem from consumers understanding the need for organisation to hold this information.[138]

Behavioural factors

Behavioural research has shown us that consumers are not always rational beings; they do not always weigh up costs and benefits and then come to the "ideal" conclusion. This is because of a number of behavioural biases and cognitive limitations.

The decision as to whether to allow access to one's data is subject to these same biases and limitations. Privacy researcher Prof Alexander Acquisti [139] has identified how choices are affected by:

- **Incomplete and asymmetric information**: consumers often know less than the organisations about the extent of data collection, how it may be used and by whom, and the associated consequences. It is unrealistic to assume knowledge of probabilities of all possible outcomes and for consumers to be able to evaluate these against each other.
- **Bounded rationality**: consumers are unable to contemplate the multitude of consequences that could result from sharing their data due to cognitive limitations. This leads to decision-making based on heuristics and simplified models.
- **Behavioural biases**:
  - *Hyperbolic discounting*: refers to the idea that people do not discount distant and close events in a consistent way. There is therefore a tendency to trade-off privacy costs and benefits in ways that may be inconsistent with individuals' initial plans, and which ends up "costing" future selves in favour of immediate gratification.
  - *Rational ignorance*. Ignorance can be considered rational when the cost of learning about a situation enough to inform a rational decision would be higher than the potential benefit one may derive from that decision. Individuals may avoid assessing their privacy risks for similar reasons: for instance, they may disregard reading terms and conditions as they believe that the time cost associated with inspecting the notice would not be compensated by the expected benefit.

Acquisti also notes that other heuristics may also be found in decision making. For example, the simulation heuristic where individuals may tend to discount as improbable those events that are difficult to picture mentally, such as identity theft, or the representative heuristic may lead people to associate trustworthy behaviour with the neat appearance and design of a website.[140]

[137] Kantar (2014) The apps environment.

[138] C.Bates, P. Gooch, H.Lewis. (2014) Data Nation 2014. Putting customers first. Deloitte.

[139] Acquisti. A and Grossklags. J. (2006) What can behavioural economics teach us about privacy? Presented as a Keynote Paper at ETRICS 2006.

[140] Acquisti. A and Grossklags. J. (2006) What can behavioural economics teach us about privacy? Presented as a Keynote Paper at ETRICS 2006.

5 Consumers' concerns about data collection

Concerns about data collection are mainly linked to security/safety and privacy

Privacy concerns are not top of mind, but when consumers are asked to think about it, it is clear it is important to them.

Specifically, consumers talk about concerns around having their location tracked and their browser history shared [141/142] and of the possibility for an organisation knowing "too much" about them, by linking data such as their name and address with time and location-based information.[143] In experimental research it was found that people are (hypothetically) prepared to pay to keep some of their data private.[144]

While people are uniformly concerned about privacy, albeit only when prompted, concern about security is more varied. When prompted, 7 in 10 (72%) say they are concerned that companies will fail to keep their data safe.[145]

People are particularly concerned about the passing on of data to third parties. For example, 68% said they are concerned about their data being sold on to third parties for marketing purposes[146] and separate research found that 63% said that companies selling anonymous data is a concern.[147]

Selling of data to third parties, may be particularly concerning to consumers for the following reasons; they do not agree to enter a "contract" with that third party and therefore relationship is not equitable; they cannot control the relationship (by opting out for example) and they have no awareness of that party's privacy practices.

[141] Kantar (2014) The apps environment.

[142] Ipsos MORI (2016) 'Digital footprints: consumer concerns about privacy and security'

[143] Illuminas for Citizens Advice (2016) 'Consumer expectations for personal data management in the digital world'

[144] Skatova et al. Perceived risk of personal data sharing.

[145] Ipsos MORI (2014) Public attitudes to the use and sharing of people's data cited in Ipsos MORI (2016) 'Digital footprints: consumer concerns about privacy and security'

[146] ICO (2016) Annual Tracker.

[147] Ipsos MORI (2014) Public attitudes to the use and sharing of people's data cited in Ipsos MORI (2016) 'Digital footprints: consumer concerns about privacy and security'

Consumers' confidence in managing their personal data varies between individuals and is context dependent. Age and levels of confidence in online abilities are factors which have been found to affect behaviour and opinions.

- **Age:** younger adults are more likely to be doing various tasks online.[148] They are also more likely to say that they are very confident they know how to manage who has access to their personal data online, and are less likely to say they are concerned about their privacy online.[149] However it should be noted that the research does not check whether younger people are better are managing their data than older adults.
- **Confidence in online abilities:** high confidence users are more aware of concerns around personal information and how it is used for commercial purposes (although they may not act on that knowledge). In contrast low confidence users tend to have particular concerns around "scamming" or being "taken advantage of". Low confidence users tend to be less frequent users, with the main barrier to use being lack of confidence rather than concerns.[150]

In addition to these broad characteristics, individuals have varying subjective perceptions of threats and potential damage, psychological needs and actual economic returns. These all play a role in affecting opinions on data collection and subsequent decisions to allow access to personal data by commercial bodies.[151]

Demos found that there were five segments when looking about knowledge and concern about data protection:[152]

- **Non-sharers** (30% of the population): knowledgeable about data protection, view much of their data as personal and take measures to protect it.
- **Sceptics** (22% of the population): do not have a single view as to whether data is personal or impersonal, but sceptical of whether or not government and companies can be trusted. They do not use online services much and only share data if the personal benefits of doing so are clear to them.
- **Pragmatists** (20% of the population) – do not know all of the details about how their data is used, but take small measures to protect their privacy. Prefer efficient services to complete privacy.
- **Value-hunters** (19% of the population): 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% of the population): categorise a lot of their information as impersonal and therefore are comfortable sharing it. Amenable to sharing more in future, but concerned about the ways in which those data could be misused.

[148] Ofcom (2017) 'Adults' media use and attitudes'

[149] Ipsos MORI (2016) 'Digital footprints: consumer concerns about privacy and security'

[150] Ipsos MORI (2016) 'Digital footprints: consumer concerns about privacy and security'

[151] Acquisti. A and Grossklags. J. (2006) What can behavioural economics teach us about privacy? Presented as a Keynote Paper at ETRICS 2006.

[152] Demos (2012) The Data Dialogue.

Consumer concerns by data type

The research reviewed here tends to look generically at data collection concerns; there is little research which explicitly asks consumers about concerns related to different types of data. Illuminas however did find that concerns around personal information which a consumer inputs to a website or app (eg name and address) are more salient than concerns around inferred data which can be created (eg behavioural inferences from time spent browsing, location, comments posted).[153] They also found that concern was higher when various disparate pieces of information can be pieced together, as this is not what consumers generally agree to.[154]

The categories below examine data types and existing research relating to concerns about each. Further research is required to more fully understand each of these different data types and related concerns.

- **Location data**: Almost half (45%) of consumers consider location to be "personal data" [155] and one fifth (20%) of internet users say they are concerned about providing their location data online:[156] Qualitative research found that location data is seen as invasive by app users; [157] and confident internet users of the internet do not like how cookies are used to track location.[158] Skatova et al found that people are prepared (hypothetically) to pay varying amounts to keep their data private from companies, and that physical location history is in the second highest band for the amount people are prepared to pay to ensure this.[159] The only reference of security concerns relating to location data is by a minority of people who are concerned that SMART technology could be hacked. Qualitative research linked some of this concern to hackers accessing their home, in the knowledge that the individual might be out judging from inactivity or changes in activity of these SMART apppliances.[160]
- **Browsing history**: one fifth (20%) are concerned about providing their browsing history to companies [161] and qualitative research found that this is seen as invasive by app users.[162] Ipsos MORI's research into consumers attitudes to cookies found that when it was explained what cookies do, the general consensus was that whist they are "sneaky", they are not concerning enough to be a barrier to internet use. [163]

[153] Illuminas for Citizens Advice (2016) 'Consumer expectations for personal data management in the digital world'

[154] Illuminas for Citizens Advice (2016) 'Consumer expectations for personal data management in the digital world'

[155] Demos (2012) The Data Dialogue.

[156] Ipsos MORI (2016) 'Digital footprints: consumer concerns about privacy and security'

[157] Kantar Media (2014) Apps environment research report.

[158] Ipsos MORI (2016) 'Digital footprints: consumer concerns about privacy and security'

[159] Skatova et al. Perceived risk of personal data sharing.

[160] Ipsos MORI (2016) 'Digital footprints: consumer concerns about privacy and security'

[161] Ipsos MORI (2016) 'Digital footprints: consumer concerns about privacy and security'

[162] Kantar Media (2014) Apps environment research report.

[163] Ipsos MORI (2016) 'Digital footprints: consumer concerns about privacy and security'

- **Information from social networking sites**: A third (33%) of those with a social media account are concerned about their personal information when on these platforms.[164] Around a third (36%) of social media users say they always consider privacy/data security implications when they are "checking in", nearly half (46%) say they do this when posting photos.[165] However, the research does not report what they are considering and how, if at all, it affects their behaviour. It may also be that people responded in a socially desirable way to this question. Skatova et al [166] found that people are prepared to pay the second highest amount to keep data from social networking profiles private.
- **Digital communication history**: Skatova et al also found that people are prepared to pay the most to keep digital communication history data from companies.[167]
- **Health records**: Skatova et al found that people are prepared to pay the second highest amount to keep their health records from companies.[168] Sheehan and Hoy (2000) cite that consumers are more concerned about the collection and use of data from their medical records, than some other data types.[169]
- **Financial data**: Skatova et al found that people are prepared to pay the most to keep their bank account statement from companies.[170] Sheehan and Hoy (2000) report that consumers are more concerned about the collection and use of their financial data, than some other data types.[171]

Figure 5: Types of data grouped by relative amounts people would be prepared to pay to keep the data from an organisation. Skatova et al [172]

The most money			The least money
• Bank account statement • Digital communication history	• Social networking profile and activities • Physical location history • Health records	• Household bills • Online purchasing history • Internet browsing • Search history • Demographic information	• Loyalty card data • Online advertising clicks

Privacy concerns

Due to its cultural construction, perceptions of privacy are changing and evolving. However, central to the idea of privacy is the characteristic of

[164] Ipsos MORI (2016) 'Digital footprints: consumer concerns about privacy and security'

[165] Ofcom (2017) 'Adults' media use and attitudes'

[166] Skatova et al. 'Perceived risk of personal data sharing'

[167] Skatova et al. 'Perceived risk of personal data sharing'

[168] Skatova et al. 'Perceived risk of personal data sharing'

[169] Sheehan K, Hoy G (2000) 'Dimensions of privacy concern among online consumers', Public Policy Marketing 19 (1) p62-73

[170] Skatova et al. 'Perceived risk of personal data sharing'

[171] Sheehan K, Hoy G (2000) 'Dimensions of privacy concern among online consumers', Public Policy Marketing 19 (1) p62-73

[172] Skatova et al. 'Perceived risk of personal data sharing'

individual control: that individuals want to “determine for themselves when, how, and to what extent information about them is communicated to others”. [173]

Research suggests that privacy is not top of mind for consumers but when they are prompted to think about it, it is important to them. Consumers still feel that they have a fundamental right to privacy and that they should be able to trust organisations to respect this.[174] Research by Ofcom[175] and the Communications Consumer Panel[176] found respectively that 9% and 14% of consumers spontaneously cite privacy as a concern when asked. When prompted about privacy issues, 67% of internet users said that they are concerned about their privacy online.[177]

Specifically, consumers talk about concerns around having their location tracked and their browser history shared[178/179] and of the possibility for an organisation knowing “too much” about them, by linking data such as their name and address with time and location based information.[180]
In experimental research it was found that people were (hypothetically) prepared to pay to keep their data private.[181]

The proliferation of social media, online products and services and apps has, however, normalised data sharing and some consumers are re-defining what they view to be private. For example, two thirds of people agree that their definition of privacy is changing due to social media and the internet, and over two-thirds of consumers agree that being on social networks has changed their view on what is and is not private from companies.[182] A segmentation by the DMA conducted in 2012, 2015 and 2017 has found an increase in the percentage of people who are “unconcerned about the collection and use of personal information about them” (from 16% in 2012 to 25% in 2017); and a decrease in the percentage who are “unwilling to provide personal information even in return for an enhanced service” (from 31% to 25%).[183]

The most recent segmentation by DMA shows the following sizes of groups in the population:[184]

- **Privacy pragmatists** (50% of the population): those who make trade-offs on a case-by- case basis as to whether the service (or enhancement of service) offered is worth the information requested. They are most likely to see their personal information as an asset to be negotiated in return for better prices and offers.

[173] Westin, A (1967) Privacy and Freedom New York, Atheneum. Cited in Dwyer, C (2009) Behavioural Targeting: A Case Study of Consumer Tracking on Levis.com

[174] Illuminas for Citizens Advice (2016) ‘Consumer expectations for personal data management in the digital world’

[175] Ofcom (2017) ‘Adults’ media use and attitudes’

[176] Communications Consumer Panel (2011) ‘Online personal data: the consumer perspective’

[177] Ipsos MORI (2016) ‘Digital footprints: consumer concerns about privacy and security’

[178] Kantar (2014) The apps environment.

[179] Ipsos MORI (2016) ‘Digital footprints: consumer concerns about privacy and security’

[180] Illuminas for Citizens Advice (2016) ‘Consumer expectations for personal data management in the digital world’

[181] Skatova et al. ‘Perceived risk of personal data sharing’

[182] DMA (2012) Data privacy: What the consumer really thinks.

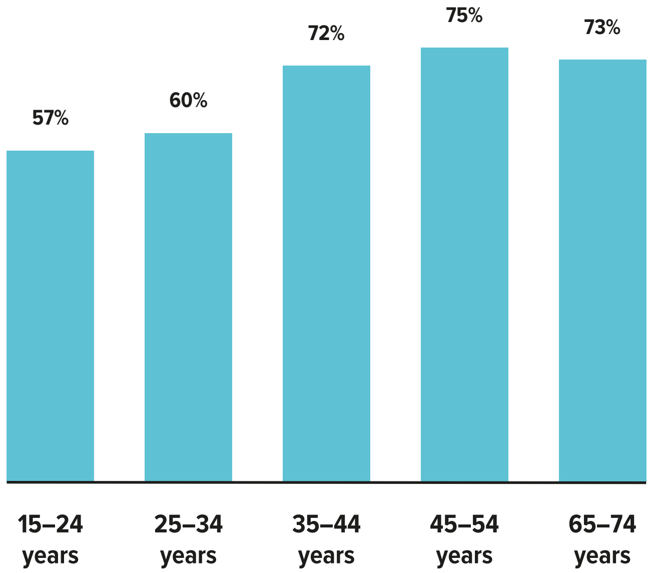
[183] DMA (2018) Data privacy: what the consumer really thinks.

[184] DMA (2018) Data privacy: What the consumer really thinks.

- **Privacy fundamentalists** (25% of the population): those who are unwilling to provide personal information even in return for service enhancement. Tends to be an older age group and also tend to be those who use the internet and social media less frequently.
- **Privacy unconcerned** (25% of the population): those who are unconcerned about the collection and use of personal information about them. The segment which is characterised by a relatively positive attitude towards the sharing of personal data.

Ofcom found that 72% of internet users say they are confident knowing how to manage who has access to their personal data online, and younger users are more likely to say they are very confident (60% among 16–24 and 47% among 25–34 year olds).[185] Younger users were also found to be less concerned than older users about their privacy online. However privacy is still a concern for the majority of people across all age groups.[186]

Figure 6: Percentage of people who expressed concern about privacy when going online, by age group



Source: Ipsos MORI (2016) 'Digital footprints: consumer concerns about privacy and security'

Ipsos MORI's research found that concern about privacy did not vary greatly according to whether respondents are confident (67%) or non-confident (72%) internet users.[187] This suggests that privacy concerns may be reflective of an ideological perspective, rather than linked to security concerns. However, research would be needed to see if this is supported.

[185] Ofcom (2017) 'Adults' media use and attitudes'

[186] Ipsos MORI (2016) 'Digital footprints: consumer concerns about privacy and security'

[187] Ipsos MORI (2016) 'Digital footprints: consumer concerns about privacy and security', p33

Safety and security concerns

Research has found that safety and security of data is mentioned in various forms when consumers are asked about what top of mind concerns they have when using the internet. Four in ten (38%) mentioned safety of personal details (eg identity theft and hacking), 3 in 10 (26%) fraud, a quarter each said lack of safety around financial transactions (26%) and viruses (24%). In addition, the activities which most people say they are concerned about, in relation to how their information is being used, are financial transactions – half (52%) mentioning banking/paying bills online and 3 in 10 (28%) buying/selling online. Furthermore, two thirds (66%) said they are concerned about putting their credit/debit card details in online.[188]

When prompted 7 in 10 (72%) people say they are concerned that companies will fail to keep their data safe.[189] Separate research has found that only one quarter (23%) are confident that companies always remove their personal details when passing on their information to third parties.[190] Qualitative research found that consumers are more concerned that organisations themselves will be hacked, rather than the consumer being concerned about security breaches when the data is held by themselves.[191] Regarding the sharing of health data, one fifth (20%) of those who do not want commercial organisations to receive health data say that commercial organisations cannot be trusted to store the data safely.[192]

While people are uniformly concerned about privacy, albeit only when prompted, concern about security is more varied. Ipsos MORI found that non-confident users of the internet are less likely than confident users to say they are worried about the safety of their personal details (28% v 39% respectively). However, there could be a number of reasons for this. For example, having less knowledge of the risks and the fact that low confidence users tend to be older[193] and less likely to be doing online transactions,[194] might create a sense the risk is not relevant to them.

Low-frequency internet users are more likely to have particular concerns about scamming or 'being taken advantage of' and are less likely to say they were concerned about personal safety/ID theft, compared to more frequent users (30% v 39%).[195] One interpretation of this finding is that it could be that less frequent users feel vulnerable to safety violations due to their lack of knowledge, whereas higher frequency users are concerned about more sophisticated methods of capturing their data. It would be useful to do further research to explore these concerns, and the reasoning behind them.

[188] Ipsos MORI (2016) 'Digital footprints: consumer concerns about privacy and security'

[189] Ipsos MORI (2016) 'Digital footprints: consumer concerns about privacy and security'

[190] C.Bates, P. Gooch, H.Lewis. (2014) Data Nation 2014. Putting customers first. Deloitte.

[191] Ipsos MORI (2016) 'Digital footprints: consumer concerns about privacy and security'

[192] Ipsos MORI, (2015) "Public attitudes to commercial access to health data".

[193] Ipsos MORI (2016) 'Digital footprints: consumer concerns about privacy and security'

[194] Ofcom (2017) 'Adults' media use and attitudes'

[195] Frequent user defined as someone who uses the internet several times a day; less-frequent user as someone who uses it less than once a day. Ipsos MORI (2016) 'Digital footprints: consumer concerns about privacy and security'

Perceptions of security and safety of their data vary by how consumers connect to the internet. Research with app users has found that there is a belief that apps are more safe and secure than internet browsers. This is due to the idea of an app having a "contained environment" (despite it being connected to the internet) and being a discrete piece of software which has little interconnectivity with other apps and the internet. In contrast a browser is believed to open up a wider expanse of connections and the unknown Correspondingly there is little association of malicious threats with apps, whereas anti-virus' are associated with using an internet browser.[196]

The same research found that when it came to purchasing through apps and browsers, people feel that both methods offered the same level of security. However, if people were to purchase through their mobile they preferred to do it when connected to the home wi-fi rather than their mobile network, as this is perceived to be more secure.[197] This is not the case when it comes to privacy concerns – people are just as concerned about privacy when using a mobile signal (63%) or public wi-fi (64%) or "in general" (67%).[198]

Concern over third-party use

People are particularly concerned about the passing on of data to third parties – for example, a majority (68%) say they were concerned about their data being sold on to third parties for marketing purposes[199] and separate research has found that 63% of people say that companies selling anonymous data is a concern.[200]

Qualitative research found there is a concern about the number of companies that hold personal data, how many other companies it is shared with and whether the passing on of their data would ever end.[201] This feeling of concern links to consumers wanting to feel in control: qualitative research has found that once people had "given" their data they felt that they were no longer able to control what was done with it or where it went.[202]

[196] Kantar media (2014) Apps environment research report.

[197] Kantar media (2014) Apps environment research report.

[198] Ipsos MORI (2016) 'Digital footprints: consumer concerns about privacy and security'

[199] ICO (2016) Annual Tracker.

[200] Ipsos MORI (2014) Public attitudes to the use and sharing of people's data cited in Ipsos MORI (2016) 'Digital footprints: consumer concerns about privacy and security'

[201] Illuminas for Citizens Advice (2016) 'Consumer expectations for personal data management in the digital world'

[202] Ipsos MORI (2016) 'Digital footprints: consumer concerns about privacy and security'

6 Control and transparency are important to consumers

The majority of consumers do not believe they currently have control over how their data is collected and used by companies and want this to change.[203]

People want to be clearly informed about how their data will be used; to be able to opt-in and out of different permissions;[204] **to have say over who their data is shared with, and for how long it is retained.**[205]

The importance of control can be understood in the context of social contract theory.[206] **When people's data are collected they enter into a "social contract" with that organisation. And, as with any social contract, both parties need to gain something from being in the contract; consumers should have control to some degree (eg be able to change terms, exit) and to be aware of the terms of the contract (eg privacy policies).**

Sharing data with third parties is particularly concerning to consumers as it violates social contracts on all levels – 1) they do not agree to enter a social contract with the third party – there is no equitable relationship – 2) they do not have control over the relationship and 3) they do not have any awareness of the various organisations' privacy practices.

The main factor which affects people's level of concern over collection of their data is their own perceived control over their data.[207]

The majority (69%) say they have little or no control over how their personal information is used.[208] People want to be clearly informed about how their data will be used, and want to be able to opt-in and out of various permissions.[209] They also want to have more control over who this data is

[203] Ipsos MORI (2016) 'Digital footprints: consumer concerns about privacy and security'

[204] Communications Consumer Panel (2011) 'Online personal data: the consumer perspective'

[205] Illuminas for Citizens Advice (2016) 'Consumer expectations for personal data management in the digital world'

[206] Malhorta N, Kim S, Agarwal J (2004) 'Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model', Information Systems Research, December 2004, vol 15 (4) p336-355

[207] Sheehan K, Hoy G (2000) 'Dimensions of privacy concern among online consumers', Public Policy Marketing 19 (1) p62-73

[208] Ipsos MORI (2016) 'Digital footprints: consumer concerns about privacy and security'

[209] Communications Consumer Panel (2011) 'Online personal data: the consumer perspective'

shared with and for how long it is retained.[210] They potentially want to be able to set up their own personal privacy settings to meet personal preferences, and have an option to pay to keep data private.[211]

Research has found that although people think there are probably already opportunities to opt out of sharing data with third parties, they feel it is not always clear what they have to do in order to achieve this.[212] Moreover some consumers have more choice than others, for example, depending on their phone's operating system app users are able to control what permissions they can grant (through push notifications which prompts them with individual permissions requests as-and-when the apps require them) or they have to accept, an up-front "contractual" agreement likened to T&Cs, which are seen as frustrating.[213]

Malhorta et al (2004)[214] has drawn on social contract theory to explain the concern of people and how it links to control. When an organisation collects data from an individual both parties enter into a "social contract"; social contracts are only considered equitable when both parties have a "shared understanding about contractual terms and self-control over the course of the relationship".[215] Therefore, as with other social contracts, the consumer must have the freedom to voice an opinion over its use or exit the contract (ie they must have control over the collected information). Organisations' collection of data is perceived to be fair, therefore, only when the consumer is granted control over the information (in this context through approval, modification or being able to opt-out) and informed about the intended use of the information. This need for control becomes more important when a large potential exists for opportunistic exploitative behaviour and a breach of the social contract.

Malhorta et al (2004)[216] also report that consumers' concern about information privacy is linked to the degree to which they are concerned about their own awareness of organisational information privacy practices. This refers to issues of transparency and ownership of the data collected; if these are seen as violated, perception of fairness decreases. Contrastingly, perception of fairness increases with the specificity of information used to provide justification. Lack of knowledge about what data is collected, how it is used and what its value is to organisations undermines consumers' ability to control their data and set the terms for what should happen.[217]

[210] Illuminas for Citizens Advice (2016) 'Consumer expectations for personal data management in the digital world'

[211] Illuminas for Citizens Advice (2016) 'Consumer expectations for personal data management in the digital world'

[212] Ipsos MORI (2016) 'Digital footprints: consumer concerns about privacy and security'

[213] Kantar media (2014) Apps environment research report.

[214] Malhorta N, Kim S, Agarwal J (2004) 'Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model', Information Systems Research, December 2004, vol 15 (4) p336–355

[215] Malhorta N, Kim S, Agarwal J (2004) 'Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model', Information Systems Research, December 2004, vol 15 (4) p336–355

[216] Malhorta N, Kim S, Agarwal J (2004) 'Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model', Information Systems Research, December 2004, vol 15 (4) p336–355

[217] Illuminas for Citizens Advice (2016) 'Consumer expectations for personal data management in the digital world'

People's concern over selling of their data to third parties data can be understood in the light of Malhorta et al's (2004) model,[218] as it violates the three dimensions: 1) they do not agree to enter a social contract with the third party – therefore presenting an unequal relationship; 2) they do not have control over the relationship; and 3) they do not have awareness of the organisations' privacy practices (found to be an influence on people's level of concerns).

Consumer research has found that over half (57%) of people do not feel that businesses are open and transparent about how they collect and use consumers' personal data.[219] Separate research[220] has found that consumers want organisations to be transparent about what they are doing. And there is research which suggests that, at least for some purposes (eg marketing), by simply being transparent about the motive consumers may find it more acceptable.[221]

However, it should be noted that even though consumers say that they want greater transparency,[222] this does not necessarily benefit them. Adjerid et al (2013) found that "new and better" privacy notices – intended to have increased readability and usability – are not sufficient to solve issues with consumers' privacy decision-making and could lead people to provide more personal information, rather than less.[223]

[218] Malhorta N, Kim S, Agarwal J (2004) 'Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model', Information Systems Research, December 2004, vol 15 (4) p336-355

[219] ICO (2016) Annual Track.

[220] Ipsos MORI (2016) 'Digital footprints: consumer concerns about privacy and security'

[221] Ipsos MORI (2016) 'Digital footprints: consumer concerns about privacy and security'

[222] Ipsos MORI (2016) 'Digital footprints: consumer concerns about privacy and security'

[223] Adjerid I et al 'Sleights of privacy: framing, disclosures and the limits of transparency', draft preliminary paper, www.heinz.cmu.edu/~acquisti/papers/acquisti-sleights-privacy.pdf

7 Trust and familiarity

Consumers use trust and familiarity as indicators of whether they should share their data

People place trust as the top reason when asked to rank factors which make them happy to share their personal information with companies.[224] Research has indicates that pre-existing trust in an organisation is used as a factor in deciding whether or not to share personal information with a party online.[225]

Trust in relation to e-commerce has been defined by Gefen et al[226] as a willingness to depend on a party based on the extent to which they:
1) behave in way that doesn't just serve their own interests (benevolence)
2) have the skills and competencies to be good at their role (ability),
3) adhere to a set of principles that are found to be honest and fair (integrity)
4) and where consumers have knowledge that allows them to predict the organisation's behaviour (predictability).[227]

Trust is linked to familiarity. Research has found that familiarity with brands is associated with perceptions of good security [228] and less heightened privacy concerns.[229] Familiarity attenuates perceptions of risk, as people habituate to the risk and start to accept it .[230] Familiar brands are considered to have more to lose reputationally if there was a data breach.[231] Similarly consumers feel that global brands would need to be more responsible in their data practices as there would be "too much at stake" for them to risk bad practice.[232]

Consumer research has found that 57% of people do not feel that businesses are open and transparent about how they collect and use people's personal data.[233] Separate research has found that people want organisations to be transparent about what they are doing.[234]

[224] DMA (2018) Data privacy: What the consumer really thinks.

[225] Ipsos MORI (2016) 'Digital footprints: consumer concerns about privacy and security'

[226] Gefen D, Karahanna E, Straub W (2003) 'Trust and TAM in online shopping: an integrated model', MIS Quarterly vol 27(1) p51–90

[227] Definitions of 'benevolence', 'ability' and 'integrity' are based on Mayer et al (1995), 'An integrative model of organisational trust', The Academy of Management review, July 1995

[228] Ipsos MORI (2016) 'Digital footprints: consumer concerns about privacy and security'

[229] Sheehan K, Hoy G (2000) 'Dimensions of privacy concern among online consumers', Public Policy Marketing 19 (1) p62–73

[230] Store P, Fischhoff B, Lichenstein S (1982) C Strong (2015) 'Why study risk perception?' Risk Analysis, vol 2, no 2, Cited in Schmidt M (2004) 'Investigating risk perception: a short introduction'

[231] Ipsos MORI (2016) 'Digital footprints: consumer concerns about privacy and security'

[232] Illuminas for Citizens Advice (2016) 'Consumer expectations for personal data management in the digital world'

[233] ICO (2016) Annual Track

[234] Ipsos MORI (2016) 'Digital footprints: consumer concerns about privacy and security'

Trust in organisations is particularly important in an online setting, and consequently with regards to data collection, because there is a risk that organisations may behave in a negatively opportunistic manner. For example, violating privacy, unauthorised use of credit card details, selling data on without permission and so on. People place trust as the top reason when asked to rank factors which make them happy to share their personal information with companies.[235] And research has indicated that pre-existing trust in an organisation is used as a factor in deciding whether or not to share personal information with a party online.[236]

Currently people tend to think that organisations are acting in their own interest when collecting data, rather than in the consumers' interest.[237] Therefore organisations need to develop trust by demonstrating they have consumers' interests at heart. Providing more control and being more transparent are key ways that organisations can encourage people to trust them when sharing their personal data.

A report by Illuminas[238] for Citizens Advice links control and transparency to building trust. It states that consumers want to be able to trust online interactions with companies and this can – in part – be achieved through honesty and transparency about the collection, storage, flow and uses of consumer data. They also suggest companies should give more consumer control over data and show they are behaving in a 'trustworthy way' – however this is not defined.

General consumer research does not explore what "trust" means to people. However academic research has explored trust a great deal, although has not arrived at one single definition.[239] Gefen et al (2003)[240] have studied trust and define it in relation to e-commerce as a willingness to depend on a party based on the extent to which they: 1) behave in way that doesn't just serve their own interests (benevolence); 2) have the skills and competencies to be good at their role (ability), 3) adhere to a set of principles is found to be honest and fair (integrity) and 4) where a consumer has knowledge which allows them to predict the organisation's behaviour (predictability).[241]

[235] DMA (2018) 'Data privacy: what the consumer really thinks'

[236] Ipsos MORI (2016) 'Digital footprints: consumer concerns about privacy and security'

[237] Ipsos MORI (2016) 'Digital footprints: consumer concerns about privacy and security'

[238] Illuminas for Citizens Advice (2016) 'Consumer expectations for personal data management in the digital world'

[239] Summary of trust conceptualisations: 1) a set of specific beliefs in integrity, benevolence and the ability of another parts; 2) a general belief that another party can be trusted and that the other party is willing to be vulnerable to their actions; 3) feelings of confidence and security in response to the 'caring response' of the other party; 4) a combination of these elements. Gefen D, Karahanna E, Straub W (2003) 'Trust and TAM in online shopping: an integrated model', MIS Quarterly vol 27(1), p51–90

[240] Gefen D, Karahanna E, Straub W (2003) 'Trust and TAM in online shopping: an integrated model', MIS Quarterly vol 27(1), p51–90

[241] Definitions of 'benevolence', 'ability' and 'integrity' are based on Mayer et al (1995), 'An integrative model of organisational trust', The Academy of Management Review, July 1995

In addition research by Ipsos MORI identified three core factors in relation to trust and data sharing 1) organisations should be fully open about what data they collect/use and what they will do with it; 2) organisations should provide the consumer the opportunity to opt-out of any use of their data; 3) organisations should keep consumers' information secure.[242]

Trust has also been linked to familiarity. Familiarity has been found to attenuate perceptions of risk as people get used to the risk and start to accept it.[243] Research has found that familiarity with brands is associated with perceptions of good security[244] and less heightened privacy concerns.[245] Familiar brands are considered to have more to lose reputationally if there is a data breach.[246] Similarly, people feel global brands need to be more responsible with consumer data as there would be "too much at stake" for them to risk bad practice.[247]

Familiarity is a main factor, as well as trust, which people say they consider when deciding whether or not to give access to personal data.[248] Less confident (often older) internet users tend to restrict their usage to only visiting "safe places", for example, or recognised brands or websites they trust. Even if this means 'overlooking' the fact that these websites use their personal data.[249] Instead, they trust that these brands will use their data responsibly.[250]

> "*I'm not all that worried because I only use sites I trust like Sainsbury's or my bank. I feel safe with them but wouldn't visit a website I don't know or ever heard of.*"
>
> Male, East of England, 75+, low confidence internet user [251]

When brands are not familiar, people may trial them on a small scale to see if any issues arise, and/or rely on others' reviews.[252] They may also rely on the website's appearance or design to decide whether their data would be secure, for example looking for institution-based assurances such as statements of guarantees, contact telephone numbers, quality marks etc – and the website having a "typical" interface (ie procedures and information required are typical of other websites).[253]

[242] Ipsos MORI (2016) Digital Footprints: consumer concerns about privacy and security.

[243] Store.P, Fischhoff.B, Lichenstein.S (1982) Why Study Risk Perception? Risk Analysis, Vol 2, No 2. Cited in Schmidt. M (2004) Investigating risk perception: a short introduction.

[244] Ipsos MORI (2016) Digital Footprints: consumer concerns about privacy and security.

[245] Sheehan, K. Hoy, G. (2000) Dimensions of privacy concern among online consumers. J. Public Policy Marketing 19(1) 62–73.

[246] Ipsos MORI (2016) Digital Footprints: consumer concerns about privacy and security.

[247] Illuminas for Citizens Advice (2016) Consumer expectations for personal data management in the digital world.

[248] Skatova, A, Ng, E, Gouling J (2014) Data Donation: Sharing personal data for public good? Conference paper.

[249] Ipsos MORI (2016) Digital Footprints: consumer concerns about privacy and security.

[250] Ipsos MORI (2016) Digital Footprints: consumer concerns about privacy and security.

[251] Ipsos MORI (2016) Digital Footprints: consumer concerns about privacy and security. Pg 40.

[252] Illuminas for Citizens Advice (2016) Consumer expectations for personal data management in the digital world.

[253] Gefen, D. Karahanna, E. Straub, W. (2003) Trust and TAM in Online Shopping: An Integrated Model. MIS Quarterly Vol 27(1). P51–90.

High consumer trust can compensate for organisations having low privacy standards, conversely low trust requires higher privacy standards.[254] There is therefore potential for organisations to take advantage of a consumer's trust by not having high privacy/security standards. However, people will punish a more trusted organisation if they undermine that trust, than they would a less trusted organisation for the same infraction.[255]

Levels of trust in organisations is sector dependent

Ipsos MORI[256] found that banks are trusted by the most users (56%) when it comes to personal information, followed by government and public services (33%). Online retailers are only trusted by around a fifth (18%) and communication providers[257] are trusted by between 13% and 16% of users. Around 1 in 10 (9%) users trust social media networks and the same percentage (9%) trust online marketplaces, eg Ebay. With regards to who they do not trust, social media networks are top; half (49%) of internet users say they do not trust them, compared to 4 in 10 (38%) of users who not trust online marketplaces.

Trust in banks seemed to stem from the banks' familiarity and experience with sensitive financial information - with users assuming that they are more likely to have better security practices in place. As well as some people citing that they had a vested interest in keeping data secure as they assume banks need to preserve their branding and reputation.[258]

Research has indicated that people are divided as to whether government and public services are more responsible with their use of personal information than private companies. A quarter (24%) feel that they are not, but a similar proportion (27%) feel that they are. However, nearly half (46%) of people are neutral giving a "neither" response, which might indicate not having enough information to say either way.[259]

[254] Johnson A, Reips U, Buchanan, Schofield C (2010) Privacy, trust, and self-disclosure online. Human-Computer Interaction. Vol 25, Issue 1.

[255] C.Strong (2015) Private lives? Putting the consumer at the heart of the privacy debate. MRS Delphi Group.

[256] Ipsos MORI (2016) Digital footprints: consumer concerns about privacy and security.

[257] Email providers 16%, mobile phone providers 13%, Internet service providers 13%.

[258] Ipsos MORI (201 6) Digital Footprints: consumer concerns about privacy and security.

[259] Ipsos MORI (2016) Digital Footprints: consumer concerns about privacy and security.

8 Consumer detriment

The detriment that consumers have experienced as a result of data sharing is unclear

There is little detailed information on the direct (eg identify theft) and indirect (eg adjusted pricing) detriment that consumers perceive and experience as a result of giving access to their data online. Despite some high profile cases of data loss by institutions, Ofcom estimates consumer detriment to be low.[260]

There is a lack of research which offers a comprehensive view on the incidence of consumer detriment, and the nature of the impact it can have. Research tends to focus on safety/security risks and detriment caused by security transgressions. Although there have been some high profile breaches of data security, there is less published market research on detriment as a consequence of privacy violations. We have not identified detailed consumer research on the nature, likelihood and impact of harm that is possible by sharing data in the future.

The extent that 'Personal Data' is shared without its originators' knowledge, and the resultant detriment is not fully known. Within government, the National Audit Office found that 8,995 data breaches were recorded by the 17 largest departments in 2014–15, but only 14 of those breaches were reported to the Information Commissioners Office.[261]

Direct detriment

Data breaches can result in 'identity theft', where a person's data is used fraudulently – for example, to purchase products or services, open bank accounts or take out credit cards in that person's name. There have been a few high profiles UK cases, such as the £2.5m taken from 9,000 Tesco Bank customers after a data breach in 2016 (which the bank later repaid), and the estimated £20m that was taken from British accounts by Dridex, malware which infects PCs and harvests online banking details from users, in 2015.[262] However, relatively little is known about what direct detriment consumers have experienced overall from misuse of their personal information.

Ofcom's adult media use and behaviour survey asked about direct detriment and found there to be little. Their research found that 15% of internet users had had a computer virus (on any online device) and 8% had had their email hacked. Less than 1 in 20 said they had lost money online/ had been scammed

[260] Ofcom (2017) Adults' Media Use and Attitudes.

[261] National Audit Office (2016) Protecting information across government.

[262] https://www.theguardian.com/business/2016/nov/12/tesco-cyber-theft-serious-questions-bank-security

(4%); reported having their social media account hacked (4%); said they had had their financial personal information stolen and used online (4%).[263] Other detriment has been reported, for example the 2010 Eurostat ICT survey found that 54% of UK internet users reported having received spam emails in the last 12 months.[264]

Indirect detriment

Incidence of consumer detriment may be underestimated as it may not be obvious what detriment consumers are experiencing, for example personalised pricing. Therefore, it is worth noting that some detriment is not easily perceived and can be hidden. Accenture found that 10% of consumers do not feel confident at all that the security of their personal data is protected on the Internet and, therefore, never share information.[265] This may reduce their access to the market. Furthermore, 14% of consumers in 2010 stated that they refrained from buying goods or services online because of security concerns[266] and over half (54%) of people say they have decided not to install, or uninstalled, an app on their smartphone, because of the amount of personal information they would have to provide.[267]

> *'I was searching for Pandora jewellery for my wife for Christmas – and all of a sudden, ads for Pandora jewellery came up on her facebook page – it completely ruined the surprise. I definitely didn't tick a box to say they could do that so I don't know how that's happened'.*
>
> Confident/informed, male, age 49, social grade C1, Leeds[268]

Qualitative research has found contrasting opinions on targeted advertising. Some found that although some people saw personalised adverts as "underhand" they did not consider it to be of detriment to consumers.[268] Other research has found that consumers are sometimes positive about targeted advertising, as it could save them time, effort and money.[270] There are ways in which consumers can take action to stop receiving targeted adverts: 4 in 10 (39%) consumers have some sort of ad blocking software in place.[271] However, some websites are responding to this by refusing visitors access to content unless they suspend this software.

[263] Ofcom (2017) Adults' Media Use and Attitudes.

[264] Cited in The Government Office for Science (2013) Foresight Future Identities, Final Project Report.

[265] Accenture, (2015) Digital Trust.

[266] Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M. J. G., Levi, U., Moore, T. and Savage, S. (2012) Measuring the Cost of Cybercrime. Workshop on the Economics of Information Security 2012 [online]. http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf

[267] Which? Editorial survey. GMI surveyed 2067 UK adults online, between 12th and 31st December2014. Data were weighted to be demographically representative of the UK population.

[268] Illuminas for Citizens Advice (2016) Consumer expectations for personal data management in the digital world p17.

[269] Ipsos MORI (2016) Digital Footprints: consumer concerns about privacy and security.

[270] Illuminas for Citizens Advice (2016) Consumer expectations for personal data management in the digital world.

[271] GfK (2013), 1,019 interviews conducted with a representative sample of online consumers between 7th–11th Feb 2014. Cited in Citizens Advice Bureau (2015) Personal data empowerment.

9 Areas for further research

While there is an abundance of research on consumer behaviour and attitudes towards data collection these tend to be broad. As such, there are notable gaps in our understanding of this area, the most important of these are:

1 . A more in-depth and nuanced understanding of what consumers' concerns are by considering: specific data types, data collection method and use (and risks attached to any single or combination of these).

2. Understanding what the detriment is to consumers of companies collecting their data and how the risks or likelihood of harm may change in the future. Research tells us that people are concerned about data collection – both from a security/ safety perspective and one of privacy. However there is little research which indicates whether not this concern is justified: are consumers experiencing detriment as a result of their data being collected and, if so, what is the detriment and how is it impacting them? How will impact or risk of detriment change as the digital revolution marches on?

3. Exploring how concepts of trust, privacy, transparency and control affect consumers' behaviour and attitudes towards data collection now, and in the future. These concepts run throughout the research into consumers' attitudes and behaviour regarding data collection. However, there has been little explanation of what they actually mean to consumers in the context of data collection, and how they interrelate. It is important that we have an understanding of these as they provide the foundations of how consumers engage with data collection and use.

4. Understanding consumers' views about rapid changes in data collection methods, data manipulation techniques, future uses of data and what the impacts might be for individual consumers and the markets they take part in.

Which? will be reporting on new research in the next few months, which build on previous research and gives further insight into consumers attitudes and behaviour towards data collection and its use.

Which?, 2 Marylebone Road,
London NW1 4DF
Phone +44 (0)20 7770 7000
Fax +44 (0)20 7770 7600

For more information please contact:
Harriet Pickles – harriet.pickles@which.co.uk