Competition & Markets Authority

The commercial use of consumer data

Report on the CMA's call for information

CMA38
June 2015

Contents

Page

Summary

1. The Competition and Markets Authority (CMA) has carried out a fact-finding project to understand how consumer data is being collected and used commercially. This has become an increasingly important economic activity, and is expected to continue to grow in size and scope in the coming years. We wanted to learn more about how firms across the economy are using data and how consumers are engaging with them. We wanted to understand what benefits are created – for consumers, firms and the economy – from this activity. We also wanted to explore the concerns that have been raised about whether this activity is working well for consumers and for businesses and how competition and regulation are impacting on its development.

2. As part of our call for information (CFI) we:

    - commissioned research into data collection and use in three illustrative case study sectors – motor insurance, clothing retailing and games apps;
    - reviewed published literature, quantitative and qualitative evidence, including more than 40 responses to our CFI; and
    - held meetings and workshops with key parties, including businesses, consumer bodies, trade associations, academics, government departments and regulators.

3. Our report is largely a factual review of what we have learned during this project, which involved engaging with a wide range of interested parties to understand the many ways in which data is being collected and used. Where possible, we have drawn high-level conclusions on this activity and suggested ways in which positive developments might be encouraged. We set out our main conclusions in this summary. These are explained more fully in the main report.

Data markets

4. Consumer data is being used across a wide range of sectors. Firms have always sought information on actual and potential customers but the advent of digital, connected technologies have allowed this to happen on a much greater scale, with greater range and more quickly than ever before.

5. Firms want consumer data because it helps them understand better what their customers want and how they respond to their goods and services. Firms can create more value for their customers by responding directly to customer feedback (explicitly through comments and implicitly through what they buy) to

improve the services and products they offer as well as to make their operations more efficient. At its simplest, this transaction offers a potential 'win-win' scenario where consumers, firms and the economy benefit. However, the collection and use of data has become highly complex and widespread, and the nature of the transaction can be difficult for consumers to understand and engage with.

6. A very wide range of types of data is collected from consumers, including internet browsing histories, location via mobile devices, and contacts and interests via social media. The data is then processed and reused by a wide variety of firms. Some of these have a direct relationship with the consumer, such as retailers. Others, like those in the infomediary sector that specialise in data collection and analysis, are not clearly visible to many consumers. One prominent use of data has been the growth of targeted online advertising where data about consumers' interests and preferences are used to place advertising, and which, at least in part, funds a significant number of online services. Our factual overview of the collection and use of data is in **Chapter 2** and is supplemented by accompanying research by DotEcon with Analysys Mason.[1]

7. Data is used in different ways by different firms. In the broad review we have carried out, we have not assessed every type of use. We have however observed that new data-driven market structures have developed and that these might operate differently in relation to how firms deal with consumers, how they invest and how they behave in the market. We describe in **Chapter 3** what different incentives might drive firms that:

   - collect data directly from consumers, including firms that use data collected to provide their services to the consumer and fund the service from advertising revenues;
   - collect data indirectly, including the infomediary sector; and
   - act as intermediaries on the consumer's behalf to manage and control data release (Personal Information Management Services, PIMS).

8. Through constant innovation firms are taking advantage of new technologies and new sources of data to find a competitive edge. This is creating a dynamic market environment where businesses and markets are evolving rapidly. One key trend likely to drive changes in the market is the increase in the passive collection of data (for instance via the Internet of Things, IoT) and

[1] DotEcon and Analysys Mason, *The Commercial Use of Consumer Data – A research report for the CMA*, June 2015.

increasing automation of data handling (such as machine-to-machine sharing and the automation of decision-making).

9. The use of consumer data can lead to important benefits for the consumer, for firms and for the economy which we describe in **Chapter 2**. These include the following:

- **Growing sales through targeted advertising and special offers** – this is the most recognised use of data and it allows firms to find customers more quickly and cheaply. Consumers can benefit from promotional offers and more relevant advertising.

- **Better customer analysis** – this helps firms understand their customers better to support marketing. It is also particularly important to the financial services sector to manage and reduce risk, for example potentially reducing the cost of insurance.

- **Personalising products and services** – this includes using consumer preferences to offer a service more closely matched to their needs – for example in retailing, to make tailored recommendations.

- **Product improvement and development** – understanding consumer demand better helps firms develop new products and services, as well as to adjust these in the light of customer feedback, whether directly or via comments on social media.

- **Business process improvements** – holding individual consumer data helps firms deal more effectively with them, and holding aggregate data helps them understand demand patterns, potentially reducing operating costs.

- **Free services** – as described above, the business model for some internet service is to make them free at point of use for the consumer and to fund them from advertising revenue.

- **PIMS** – new businesses are emerging to empower consumers by, for instance, enabling them to manage the use of their data and, in some cases, to receive a financial return from selling or licensing it.

10. These benefits will only be realised if consumers continue to provide data and this relies on them being able to trust the firms that collect and use it. We have reviewed at a high level how competition and regulation are working in these markets and how consumers are experiencing it. We have identified some elements of how firms' collection and use of consumer data could support well-functioning markets:

- Consumers should know when and how their data is being collected and used and be able to decide whether and how to participate. They should have access to information from firms about how they are collecting, storing and using data, so that they can select the firm that best meets their preferences.

- Firms should compete on the issues that matter to consumers, including the provision of clear and useable controls that enable consumers to manage data-sharing.

- Consumers and firms should share the benefits of using consumer data. Consumers may get a new or better service or lower prices because firms are becoming more efficient, or even trade their data for a direct financial reward. Firms may gain more sales or market share or become more profitable.

- The regulation of the collection and use of data should ensure the protection of essential rights such as privacy. The market can help achieve this goal where regulations encourage competition and choice, allowing a 'race to the top' by firms to offer consumers better services.

- Non-compliance with regulation should be tackled proportionately and effectively, so that firms and consumers can feel confident that the rules are being applied fairly.

11. The diverse and rapidly evolving nature of these markets mean that our high-level and general conclusions about the impact of data collection and use on markets and consumers may not apply in every circumstance. It would be essential to understand the specific circumstances of each market in order to assess whether it is working well for consumers. The views in this report on the competition, consumer and regulatory issues that arise in data markets are a starting point for any assessment we may undertake in future.

Competition and data

12. We have identified a number of important characteristics of consumer data and data markets which may differ from other markets:

    - The same consumer data can be used simultaneously by more than one person at the same time. However, restrictions can be placed on access to consumer data, for example through contractual conditions. This gives rise to a risk of exclusionary behaviour by firms preventing access to, and use of, data at reasonable prices.

- The cost structure of the collection, storage and processing of consumer data can generate economies of scope and scale. This can generate barriers to entry and expansion, leading to data markets having fewer and larger firms than would otherwise be the case.

- A number of data markets are two-sided, which can lead to these markets having fewer and larger firms and can also generate barriers to entry. This could arise where links between the two sides of the market are strong, and particularly in cases where consumers do not use multiple providers.

- Given the relatively fast evolution of data markets, competition assessments should examine both the level of competition prevailing at the time of assessment and the likely ways in which the market may evolve.

13. We received mixed evidence about barriers to entry across a range of data markets. However, where concerns were raised, the most common were whether firms could gain access to consumer data, and the difficulties experienced by small and potential new entrants in some markets that arise from the economies of scale and scope.

14. Respondents raised concerns about the potential for consumer data to be used to generate or exacerbate market power in a single market, or being used as a source of power that could be leveraged into a related market. We have not received evidence in the CFI that indicates an abuse of dominance in breach of Chapter II of the Competition Act 1998 (CA98) and/or Article 102 of the Treaty on the Functioning of the European Union (TFEU) has been, or is being committed.

15. We also considered whether consumer data might be used by firms to discriminate between consumers in a way that would be detrimental to at least a proportion of them. While we reviewed information on instances of targeted price discounts, for example in loyalty schemes in grocery retailing, we did not receive evidence of consumers suffering detriment from such discounts.

16. Given the number of different types of markets using consumer data and the variation in the use of data within these markets, we would need to understand the specifics of the market or markets in order to reach a view on whether the collection and use of consumer data is beneficial for competition or more likely to be damaging.

17. However, we have identified a number of market indicators that suggest a greater likelihood of competition concerns:

- **Markets in which data is a significant input into products and services produced**. The ability and incentives to exclude competitors by denying access to data, and/or the barriers to entry arising from consumer data, will be stronger where the data is a significant input into the quality or other attributes of a product or service. Concerns related to possible leverage of market power may arise where consumer data obtained in one market is a significant input to products and services produced in a related but separate market.

- **Markets where there are few substitutes for the data collected by firms**. Firms are more likely to be able to exclude competitors by either preventing or restricting access to and use of consumer data where there are few or no substitutes for this data.

- **Firms with existing market power that control the collection of consumer data in a marke**t. Where a firm or firms in a market already have a position of market power, their ability and incentives to exploit further power over the collection of consumer data may be stronger.[2]

- **Markets in which firms do not compete openly over data privacy and transparency of their uses of consumer data**. An absence of competition over privacy may indicate data markets failing to deliver what consumers want. This may occur where the implicit price of data used by firms is unclear, and where consumers are unable or unwilling to drive competition and incentivise firms to improve the degree to which consumers' privacy is protected.

18. For each of these characteristics, a competition assessment would need to differentiate between the use of consumer data to generate efficiencies for firms and consumers, and the collection and use which might lead to competition concerns.

19. Based on our analysis of consumer data and data markets, as well as the information received in our CFI, we consider that there are some characteristics that set data and data markets apart from other products, services and markets. However these characteristics are not unique to consumer data and the markets in which it is collected and used. Consequently, we see no reason, at present, why our existing competition and markets tools would not be effective at tackling conduct that gave rise to competition concerns in these markets.

---

[2] We note that a firm must be in a dominant position in order to be found to have abused that position under Chapter II of the CA98 and Article 102 of the TFEU.

Consumers and data

20. In order for the potential benefits we described above to be realised, consumers need to trust firms and to be willing to provide data. We describe in **Chapter 4** a number of potential barriers to this and the evidence we have found on them:

    - **Consumers lack awareness and understanding**. While their awareness of data collection for advertising purposes is quite high, consumers' wider understanding of how and why their data is collected is more limited. Most feel they lack information on how they benefit, and perceive that firms benefit more than they do. Furthermore, many consumers appear unhappy with how well firms explain why they collect data. This situation potentially limits consumers' ability to make informed decisions, including whether and how to share data. In addition, it risks a growing mismatch between consumer knowledge and businesses' use of data, which may undermine trust as new ways develop to collect, analyse and reuse data.

    - **Consumers are concerned about sharing their data**. Surveys indicate that many consumers have significant concerns about sharing data and the problems that may arise if they do so. While attitudes vary depending on a range of factors, common concerns include potential data loss, unexpected data sharing and use, as well as fears about exposure to nuisance contacts. These may be inhibiting consumers' willingness to share their data.

21. We also found widespread concerns about the effectiveness of the means by which consumers engage with the process of collecting data, including the use of privacy policies, terms and conditions and cookie notices. The evidence suggests that many consumers do not actively engage with these mechanisms and, where they do, they are not always sure what they are agreeing to.

22. There are some positive developments in terms of firms' responses to these concerns, including efforts to raise awareness of privacy controls, as well as better tools to help consumers control use of their data. Tools available include the ability to change browser settings; dashboards that some service providers have created to give consumers more choice on their privacy settings; and online tracking services that allow consumers to see what firms are tracking them and choose whether to allow that to continue. However, while most consumers take some form of action to protect their security and privacy, many do not appear to have taken up some of the more sophisticated solutions. This may be changing as consumers become accustomed to the

relatively more sophisticated tools that have become available on social media.

23. To improve consumer awareness of the way data is collected and used, companies need to be transparent with consumers about how they use data and what benefits consumers will get from allowing their data to be used. There are many different ways that firms engage with consumers, and where a firm is providing information, they need to give consumers simple and clear information to allow consumers to make informed choices. It is important that efforts to improve business transparency, consumer awareness, consent and control are spread across all sectors that use data.

24. More flexible mechanisms for consumers to exercise choice and control could help address their concerns and enable them to make decisions according to their individual preferences. For example, these could include mechanisms that allow consumers to choose between accepting essential and non-essential cookies; and where possible, to have defaults that enable consumers to opt-in to sharing their data only if they want to. Given the wide range of companies now collecting data, we would hope to see much wider adoption of such mechanisms by firms and, where they do exist, more active promotion of their existence to drive take-up.

25. These measures may help with improving trust between consumers and the firms with which they have a direct and visible relationship. However, there are many third party companies that collect consumer data (eg via cookies and apps) and share it with other firms, but do not have any direct engagement with the consumer. Firms should ensure that their contractual arrangements with third parties protect consumers' interests. This pressure through the data supply chain is a helpful way to raise standards overall.

26. Despite the concerns expressed, many consumers continue to provide their data. However we are concerned that this may mask underlying weaknesses in consumer sentiment, leading to a false sense of security that this will continue unchanged. Consumer trust could be fragile and at risk if negative perceptions about new technologies or the way firms manage data take hold. We are concerned that future changes in the way that data is collected and used (such as more passive collection via the IoT) could test how far consumers would be willing to continue to provide data.

Regulation and data

27. Regulation can play an important role in ensuring that markets work well – in in particular, in helping overcome market failures. For data, regulation can also ensure essential privacy rights are respected. We describe in **Chapter 2**

the existing regulatory framework for data, including the relevant data protection and consumer legislation, as well as several prominent self-regulation initiatives.

28. Data protection regulation is set at European level. There are ongoing negotiations underway (now as part of the European Commission's Digital Single Market plan) to create a new data protection regulation that may introduce new standards that would impact on the way data markets operate and address some of the potential concerns described above. In relation to data protection, the Information Commissioner's Office (ICO) is the relevant enforcement body in the UK.

29. Consumer protection regulations also apply to data collection and we have described in **Chapter 5** how they may apply to data-related activities. This is an area we will keep under review.

30. Self-regulation can play a part in raising standards for consumers. In relation to data markets, there are several different self-regulation initiatives, in particular, covering advertising and marketing sectors that share broadly similar aims to inform consumers and to offer enhanced controls over the data they share. ICO is developing a privacy seals scheme to provide consumers with a quality Kite mark to enhance consumer confidence. In order to be most effective, self-regulation initiatives need to be visible to consumers and have standards that demonstrate a commitment to higher quality in relation to how data is managed.

31. We believe that regulation can help create positive market conditions – where firms are incentivised to compete to meet the needs of consumers, on non-price issues like privacy, not just on price. The CMA takes as a given that fundamental rights of privacy will continue to underpin regulation in this area.

32. We will play an active role in the enforcement of regulation on consumer data. In particular we will work with other authorities to track new developments in the collection and use of consumer data and to ensure an integrated approach to enforcement and regulation, assessing which tools are most appropriate to tackle specific problems. It is important to work together because the growth in the collection and use of data, and the complexity of data markets make the role of regulators increasingly challenging. In addition to ICO and the CMA, other authorities such as Ofcom and the Financial Conduct Authority (FCA) are becoming even more involved in data issues in relation to the markets they oversee. Our aim is to create a robust, consistent and proportionate approach to tackling breaches of regulation in order to create confidence in the market.

33. During the course of our project we have heard many concerns that current regulations are inadequate. The European Commission's Digital Single Market programme will bring regulatory change. We also noted that private actions are being brought relating to data protection and privacy issues that may have an impact on the collection and use of consumer data. The regime therefore seems likely to undergo further change and we stand ready to advise on any proposed changes, building on the evidence we have gathered in this exercise about how markets are currently working and how they are evolving.

34. We live in a global economy, and many businesses operate across international boundaries. It is important that the framework for standards and regulation develops in a coordinated way internationally, such as using the Organisation for Economic Co-operation and Development (OECD) as a forum to develop new approaches. We will contribute to the development of international policy in this area, using the knowledge we have gathered in this project.

Conclusion

35. The work we have carried out in this project has allowed us to get a better understanding of the way consumer data is being collected and used. Our report sets out the evidence we have received and shows the scope and scale of this activity. Many other organisations are involved in discussion of the issues around the collection and use of consumer data both in the UK and more widely. We hope they find this report a helpful contribution to the continuing debate.

1. Introduction

The growing importance of consumer data in the economy

1.1 The collection and commercial use of consumer data has become widespread in the UK, being carried out by a large number of firms across a wide range of sectors. Forecasts suggest that this trend is set to continue and that firms will seek to broaden the types of data collected, the routes for data collection and the ways that data gets processed and used.

1.2 There are significant benefits for consumers, firms and the economy from the widespread collection and use of consumer data, and potential for even greater benefits in future. At the same time, there are persistent consumer concerns about data collection and use. The most significant of these revolve around consumers' privacy, with differing levels of awareness and understanding of data use, and concerns over the control consumers are able to exercise over sharing data. Another important concern is that consumer data has become an important asset for some firms and may lead to anti-competitive behaviour that could generate detriment for consumers and some firms. As a result of these concerns, various ideas have been suggested – and some specific proposals made – to regulate this activity further. These ideas cover both the consumer-focused concerns and the competition concerns.

1.3 The CMA decided to take a closer look at this activity because of the growing importance of the collection and use of consumer data to the economy. It is hard to imagine that many consumers in the UK could avoid providing information on themselves, given the wide reach and scale of the activity. Firms across many different sectors are increasingly becoming involved in data collection as the commercial opportunities arising from its use expand. We needed to get a better understanding of the activity and how it is impacting consumers and firms, because we anticipate that issues around the activity relating to our consumer and competition responsibilities will become more frequent in future.

Previous work

1.4 While this is the first opportunity for the CMA to look in depth at consumer data issues, we have previously considered consumer data to some extent in our work on private motor insurance[3] and on payday lending.[4] We also note

[3] CMA, *Private motor insurance market investigation*, March 2015.
[4] CMA, *Payday lending market investigation*, February 2015.

that other organisations have carried out significant work in this area to date. One of the CMA's predecessor organisations, the Office of Fair Trading (OFT), also carried out a number of investigations which are relevant to this work and on which our report builds. These included:

- **A market study into the online targeting of advertising and pricing during 2009 and 2010**. This study looked at various practices that are used in the advertising of prices. To establish how consumers respond to these practices the OFT drew on research from the field of psychology and behavioural economics. The evidence showed that certain pricing techniques, when used in a misleading way, could result in consumers making purchasing decisions they would not have made were prices more clearly advertised, or spending more than they needed to.[5]

- **Call for information into personalised pricing during 2012 and 2013**. The OFT launched a CFI to improve its understanding of how the use of consumers' data affected online markets and, its effect, if any, on pricing. It sought to investigate whether firms used data to modify prices offered to consumers, whether this was harmful, where the boundaries of acceptable conduct would be, and whether consumer protection legislation was potentially being breached.[6]

- **Work on price comparisons sites in 2012**. The OFT published a report to highlight how consumers could make the best use of price comparison websites (PCWs). This followed an OFT review which found that while PCWs can help people get better deals, use of these sites can be held back by a lack of understanding, trust and confidence among some groups of consumers.[7]

1.5 We have also taken account of a number of investigations and reports from other organisations, the most significant of which include:

- Ofcom: Research undertaken by Analysys Mason into the online data economy value chain.[8]

- Ofcom: Promoting investment and innovation in the Internet of Things – a summary of responses from its call for information and next steps.[9]

---

[5] OFT1231, *Online targeting of advertising and prices*, May 2010.
[6] OFT1489, *Personalised pricing - increasing transparency to improve trust*, May 2013.
[7] OFT1467, *Price comparison websites*, November 2012.
[8] Analysys Mason, *Report for Ofcom – Online data economy value chain*, February 2014.
[9] Ofcom, *Promoting investment and innovation in the Internet of Things - summary of responses and next steps*, January 2015.

- Information Commissioner's Office (ICO): Big data and data protection.[10]
- ICO: Data protection rights: What the public want and what the public want from Data Protection Authorities.[11]
- Citizens Advice: Personal data empowerment – Time for a fairer data deal?[12]

Our call for information

1.6 We decided to carry out a broad CFI in January 2015, and sought information on data collection and use from all parts of the UK.[13] This covered a wide range of types of data collected from consumers – including identity, what they consume, where they live and work and other demographic information, as well as information on who they connect with, their interests and attitudes. We also included data about an individual consumer (personal data) as well as metadata (the analysis of data patterns from consumers' web searches that enable groups of consumers to be targeted according to some common characteristics even if their individual identities are not known).

Our sources of information

1.7 We have gathered information from a wide range of sources. We published a set of questions designed to seek views from respondents to the CFI on:

- what data is collected, how, and who collects it;
- how data is used and how value is created from it;
- the controls available to consumers to manage data transfers;
- the benefits and risks associated with data use; and
- the regulatory environment, policy implications and future developments.

1.8 We received over 40 responses, including from firms, consumers, interest groups and regulators.

1.9 To supplement the information in our high-level, broad CFI, we commissioned DotEcon and Analysys Mason jointly to carry out factual reviews of three

---

[10] ICO, *Big data and data protection*, July 2014.
[11] ICO, *Data Protection Rights: What the public want and what the public want from Data Protection Authorities*, May 2015.
[12] Citizens Advice, *Personal data empowerment - Time for a fairer deal?*, April 2015.
[13] CMA, *Call for information - The commercial use of consumer data*, January 2015.

specific sectors where data was being used in order to reach a deeper understanding of data uses. Their report informs our report and is being published alongside it. We considered a range of possible sectors for these case studies, taking into account factors such as their characteristics and the extent and nature of data collection and use. The final selection was not based on any particular concerns about the sectors; instead, the aim was to identify case studies that would provide a wide range of factual evidence as well as deeper insights into specific examples of data collection. On this basis, those selected were:

- **motor insurance** – in part because of its long history of collecting and using consumer data to assess risk and set premiums, as well as recent developments such as the collection of telematics data;
- **clothing retailing** – to provide indicative evidence that may be relevant to the wider retail sector more generally and, in part, because of the growing role of social media in clothing product reviews and development; and
- **games applications** (or 'apps') – due to the relatively young and fast-moving nature of the sector and to help us understand the growth in online mobile data collection and use. This work focused on games apps accessed either directly as installed apps on mobile devices or indirectly via social media networks.[14]

1.10 We supplemented the information gathered through the research above and our CFI with a series of meetings with interested parties. We also held three workshops with relevant parties, including one hosted by the Internet Advertising Bureau (IAB) and another by techUK. We received input from a wide range of parties and we are extremely grateful for all those who took the time to help us.

1.11 Many other bodies have responsibilities for, and interests in, consumer data. We worked with relevant regulators in the UK – primarily ICO and Ofcom – to share information and discuss how the regulatory regime is impacting on the collection and use of data. We also spoke to international authorities that have taken an active interest in this area, in particular those in the European Union (EU).

1.12 Given the high level of interest in the topic, a significant amount of material was publicly available – including factual reports and consultations by

[14] The research on games applications addressed the collection of consumer data through games applications used by adults (excluding gambling).

regulators, consumer surveys, business reports, and interest group reviews. We have drawn on this material where appropriate in our report.

Our report and findings

1.13 In carrying out this work, our objective has been to understand the operation of markets where data has become an important element of the engagement between consumers and firms. We have taken into account how firms and consumers are behaving, and how competition and regulation are impacting on what happens in these markets.

1.14 Our report is largely a factual review of the large amount of information on data collection and use that we have gathered. We have used this information, together with a more principles-based approach in some areas to develop a high-level view on how data is collected and used, the operation of data markets, and regulation. We have done this for two reasons. First, in some areas we received little information because our project was short and broad in its scope. Second, this is a fast-moving area and many respondents stressed the rapid pace of change in the technologies that underpin data collection and use. We therefore focused on the characteristics that are likely to remain relevant for the foreseeable future.

1.15 We identify and consider not only a number of different benefits that can arise from the collection and use of consumer data, but also a number of areas in which consumers may suffer detriment. Given the scope of this CFI, and the complex nature of some of the detriment we discuss, we do not, as part of this report, seek to measure, quantify or attach monetary value to the detriment, or compare it with detriment from other markets.

1.16 We hope both the factual evidence we have set out in this report and our findings will:

- shed light on the way that consumer data is collected and used;
- highlight the benefits of data collection and use, and identify the potential consumer and competition problems that may arise in these markets; and
- help to influence developing regulation of this area, taking into account the need to balance consumer harms with the risks of damaging innovation that may ultimately be of benefit to consumers.

1.17 The remainder of this report is structured as follows:

- **Chapter 2** is a factual review of the way that consumer data is collected and used, how it is regulated, and the potential benefits created for firms, consumers and the economy as a result.

- **Chapter 3** describes the economic characteristics of consumer data, data markets and the ways in which competition concerns may arise in these markets, as well as the information received in the CFI regarding competition concerns, and concludes by setting out our high-level views.

- **Chapter 4** describes the harms that respondents to the CFI suggested may arise for consumers from this activity; presents information from published surveys and other relevant reports we looked at; and sets out our initial views.

- **Chapter 5** discusses proposals for additional regulation of consumer data, and the roles of different authorities. It also sets out how self-regulation can help improve standards. It describes information received in our CFI on the effectiveness of the regulatory regime and sets out the future role of the CMA.

2. Consumer data and the data value chain

Introduction

2.1 This chapter provides an introductory overview of the collection and use of consumer data, as well as the regulatory environment in which these processes take place. In **Section A**, we discuss the nature of consumer data and what we mean by the 'data value chain'. In **Section B**, we set out some of the main ways in which consumers and firms interact and how firms collect and share data. In **Section C**, we consider the role of data analysis, while in **Section D** we consider the uses of consumer data and the benefits generated. Finally, in **Section E**, we set out the regulatory framework and consumer protections, as well as some of the main self-regulation initiatives.

2.2 For this report, our definition of 'consumer data' relates to any information firms might collect from and about consumers that is used, or intended to be used, to support commercial activities.[15]

2.3 The scope of our definition is wide. We include data that:

- consumers offer voluntarily ('declared data') – for instance when transacting, or registering for a service;
- consumers generate and supply passively ('observed data') – for instance on social media, or when their online browsing activity is tracked; and
- is generated by first and third parties as a result of analysis or in combination with other data.

2.4 We also include data that is at the level of the individual (whether or not they are identifiable) and at an aggregate level across many consumers.

2.5 Many businesses want to know what their customers and potential customers want, when, why and how, so that they can build loyalty, drive up sales and establish a competitive advantage.

2.6 Until a few decades ago, businesses had limited opportunities to gather information on consumers other than through subscriptions, competitions, mail order and other forms of direct contact. Larger businesses commissioned

[15] In this report, our reference to 'consumer' data includes all data on groups of people and individuals that could be used for commercial purposes, whether or not it is initially generated when people are consuming or transacting.

or purchased market research and surveys to develop a general understanding of consumers' preferences.

2.7 In 1994, Tesco, one of the UK's main supermarket chains, launched a loyalty card scheme. The concept of loyalty schemes was widely adopted across the sector and transformed the nature of customer data collection in retailing. Customers who chose to hold a loyalty card received discounts and other offers as a reward for their custom. The cards were intended to help retailers build a more loyal customer base, but also provided them with detailed data on their customers and their purchasing preferences. This enabled the retailers to target individuals with tailored offers while providing aggregate data on their customer base (for instance to inform what to stock in specific stores given local demand).

2.8 Loyalty cards continue to be an important source of customer data for businesses. However, with the internet, the growth in scale and scope of commercial and social interactions has led to a substantial shift in the ability of firms to gather data on actual and potential customers. In the last decade, this has been accompanied by a rapid rise in online mobile connectivity through take-up of smart phones and tablets.

2.9 Alongside this 'online revolution', the falling costs of technology and storage, the significant advances in processing power and development of new analytical tools have underpinned the phenomenon of 'big data' (**Box 2.1**). The consequent advancement in the ability of firms both to gather and analyse huge volumes of consumer data has helped to fuel a growing commercial focus on this information.

Box 2.1: Big data

Reportedly first used by Silicon Valley developers 20 years ago, the term 'big data' typically refers to the huge growth in data generated as a result of the technological and digital revolution and the consequent development of new computing tools, techniques and skills required to analyse and make sense of this information.

The most cited definition of 'big data' emphasises the speed at which huge and diverse amounts of data are increasingly generated:

> 'Big data is high-volume, high-velocity and high-variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight and decision making.'[16]

The concept of big data refers to all types of information whether or not it relates to people – including, for example, weather data, traffic flow information, communications, industrial and agricultural information and data gathered in medical experiments.

One estimate suggests that in 2013, there were 4.4 trillion gigabytes of data produced globally and that this is doubling in size every two years, so that by 2020 it will reach 44 trillion gigabytes.[17]

The availability of huge data sets, coupled with greater processing power and storage capacity, has prompted the take up of complex analytics based on algorithms to spot patterns. Tools and techniques such as machine learning, modelling, simulation and data visualisation have rapidly evolved to make best use of the data.

2.10 Many respondents to our CFI noted this expansion in the ways in which data is being collected from consumers and the large volumes of data involved. They also identified a huge range of data types as well as many commercial purposes for which a growing number of firms are using this information.

2.11 Perhaps unsurprisingly, although offline data collection was within our scope, online connectivity and internet-related data collection were the primary focus of most responses to our CFI. For this reason, and because this is where most technological developments continue to take place, our report particularly centres on consumer data in the 'online age'.

---

[16] Gartner IT glossary, *Big data*.
[17] IDC, *The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things*, April 2014.

Section A: Consumer data and the data value chain

2.12 When considering the wide range of data that can be used for commercial purposes, two important dimensions are the content of the data and the type of data in terms of the extent to which individuals are identifiable.

The content of the data

2.13 The range of consumer information that can be used commercially extends well beyond the basic transactional data historically captured by retailers. **Box 2.2** includes a non-exhaustive list of such data.

Box 2.2: Data content

A very wide range of data can be collected by firms for commercial purposes, including:

- **financial** – such as information on income and credit ratings;
- **contact** – such as an individual's home or work address, their email address, and phone number;
- **socio-demographic** – such as age, ethnicity, gender, occupation and social class;
- **transactional** – such as purchases made with loyalty cards or completed online and the prices paid;
- **contractual** – such as service details and history maintained by utility suppliers;
- **locational** – such as location data share by mobile devices, vehicle telematics, GPS data, planned journeys entered into satnavs, and sensor data collected from radio-frequency identification (RFID) tags;
- **behavioural** – such as websites visited and adverts clicked on, data on consumers' use of games apps, and telematics data captured by motor insurance companies;
- **technical** – such as Internet Protocol (IP) addresses and device data such as the IMEI (International Mobile Equipment Identity);
- **communications** – such as entries in social media and in email exchanges;
- **social relationships** – such as the links between family members and friends;

- **open data and public records** – such as births, deaths, marriages as well as the electoral register, court and insolvency records and the Land Registry's records;
- **usage data** – such as energy usage captured by smart meters; and
- **documentary data** – such as audio and visual media and documentary files and records shared online, stored on PCs, tablets or the 'cloud'.

2.14 In practice, these data categories may overlap and interrelate. For example:

- behavioural and communications data may reveal consumers' preferences and their personal relationships;
- transactional information may include financial data and reveal preferences about products; and
- public data may contain relationships data.

The type of data

2.15 Data can be classified into two main types:

- **Personal data** (or personally identifiable information) is data that can be used alone or in combination with other data to identify specific individuals. Individuals may be directly identifiable from data such as their full name, address, National Insurance number, fingerprints, DNA, facial images and retinal scans. Or they could be identifiable from other data if it is combined for instance with their last name, age, gender, employment, postcode, marital status, nationality, education, disabilities, income or assets. The Data Protection Act 1998 defines personal data and the data protection principles which organisations using such data have to follow.[18] We consider these controls and other relevant regulations later in this chapter and in **Chapter 5**.
- **Non-personal data** does not contain personally identifiable characteristics and cannot alone be used to identify individuals. It may be:
  - **Anonymous data** – information that is collected or used without any personal identifiers and where identification is unlikely to take place. For example, market research information collected from consumers that simply asks about what shops they have visited without collecting

[18] *Data Protection Act 1998*. For more information, see the ICO website.

information about who they are. Data may be 'anonymised' by stripping out any information or identifier that might enable individuals to be identified. Data that is fully anonymised is no longer personal data.

- **Pseudonymous data** – information collected and used at the level of individuals, which may contain personal information such as age range and gender, but where personal identifiers are not present (for instance, because they have been stripped out and replaced with artificial identifiers or pseudonyms). Businesses can use this data to target specific individual people with an interest in, for example, anti-ageing products without the company knowing their identity.
- **Aggregate meta data** – this is data created by combining personal, anonymous or pseudonymous data for multiple individuals as a group. For example, data may be used by a business to select and target groups ('segments') of people with an apparent interest in sport.

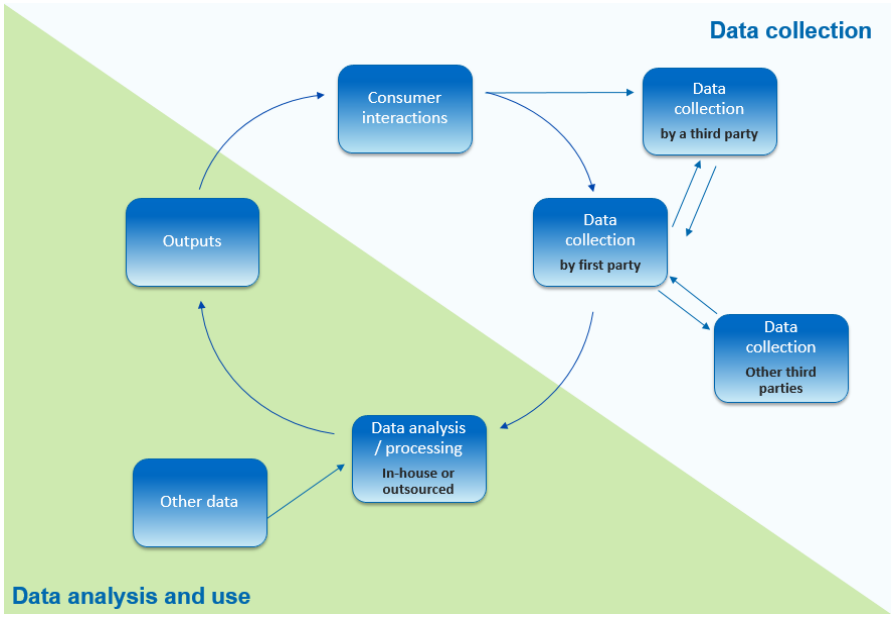
The consumer data 'value chain'

2.16 We next provide an overview of the consumer data 'value chain' – the series of interrelated actions by which consumer data is generated, collected and processed commercially to create value – and the relationships between the parties involved.

2.17 As part of their findings in the work we commissioned from them, DotEcon and Analysys Mason[19] identified a high-level common model data value chain which they used to illustrate the flows of data in the three sectors they examined (simplified in **Figure 2.1**).

[19] DotEcon and Analysys Mason, *The Commercial Use of Consumer Data – A research report for the CMA*, June 2015. For ease, in the rest of this report we refer to this as DotEcon's research.

Figure 2.1: The sectoral consumer data value chain



Source: Simplified version of the data value chain model developed by DotEcon and Analysys Mason.

2.18 We use this model in this chapter to provide a simple framework for our discussion of the key characteristics of consumer data collection and use. In brief, we address the ways in which data is collected and used:

- **Data collection**: Consumers provide information to firms actively (for instance when registering), or passively (for instance from mobile devices they carry providing location data). Firms may be collecting data directly from consumers as first parties, or as third parties without a direct relationship to the consumer. This information may be aggregated at this collection stage with data from other third party sources, or at the data analysis stage.

- **Data analysis and use**: First parties may conduct analysis on their own customers, but an area of rapid growth has been in third party analysis of data to identify patterns and relationships for sale to other businesses. The results of this data analysis may be used to support value generation from advertising, as well as product development and sales, which themselves help to generate further consumer data to feed the process.

2.19 In this chain of events, value can be generated from consumer information at a number of stages, which we discuss in this chapter. For example, value can be generated:

- from the sale, exchange or licensing of the data;

- by third parties selling their analysis, including of trends, customer insights and segmentation; and

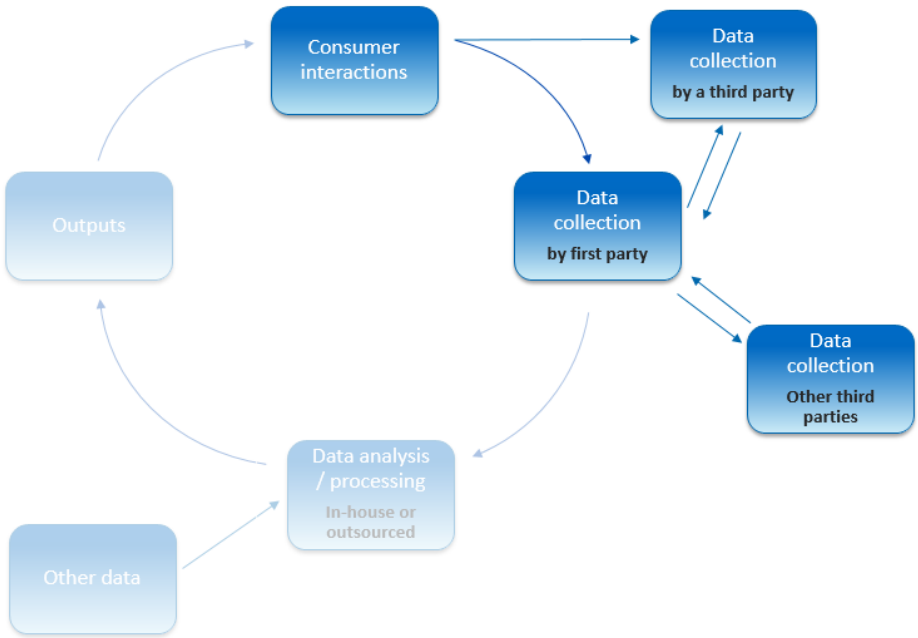
- from the use of data analysis, for example, to:
  - support targeted advertising;
  - build and maintain brand loyalty through special offers and improvements to service quality; and
  - develop improved, new and personalised products and services.

2.20 In practice, as DotEcon reports, sectors can vary quite significantly in how their data value chains operate. Furthermore, while the 'closed' model they set out is helpful in terms of describing data flows within a sector, in practice, data might be shared across sectors at various points.

Section B: Data collection

Consumer interactions and data collection

Figure 2.2: Interaction and data collection



Source: Simplified version of the data value chain model developed by DotEcon and Analysys Mason.

2.21 We start by looking at the initial generation of data by consumers and its collection (**Figure 2.2**). Consumers can generate and potentially share their data through offline or online contact.

- **Offline contact** – consumers can generate data in their dealings with organisations in person, by letter, in forms or over the phone.

In terms of the public sector, this includes registering on the electoral roll, or for births, deaths and marriages, as well as interactions with agencies such as the police and Land Registry.

Consumers provide data to businesses when they register for services (such as mobile phone contracts), or participate in questionnaires and quizzes. In particular, many consumers provide personal details and purchasing information to the operators of retail loyalty card schemes and to catalogue owners (see **Box 2.3**).

Box 2.3: Loyalty schemes

Research by Consumer Focus in 2012 illustrated the substantial penetration of loyalty cards into UK households, with almost all consumers (96%) holding a loyalty card, and two-thirds (67%) having three or more of the cards presented to respondents. The top three cards the respondents held were Tesco Clubcard, Nectar and Boots Advantage (held by 81%, 74% and 66% respectively).[20]

Recent Mintel research largely confirmed this picture, suggesting that 91% of internet users aged 16 and over were members of any scheme – with 73% members of Tesco Clubcard, 68% members of Nectar and 57% members of Boots Advantage. The next most cited scheme was Superdrug Beautycard at 22%.[21]

- **Online contact** – over the last decade, consumers have increasingly generated large volumes of data from their use of the internet – when browsing and providing information directly to websites via PCs, games consoles, tablets and smartphones, as well as when using 'smart devices' and through the use of social media and electronic communication (such as text and emails) – see **Box 2.4**.

  The public sector has been adopting digital strategies that enable consumers to register and update their details and requests online – for example for vehicle licensing and planning applications.

  In the private sector, consumers generate data when browsing for purchases and transacting online, as well as when using apps[22] on their tablets and mobiles, smart devices or cloud computing services. When using mobiles and satnavs, consumers may generate information on their location and even their destination, route, speed and places of interest. By

[20] Consumer Focus, *Consumer Focus Digital Behaviour Survey*, March 2012.
[21] Mintel, *Loyalty to Retailers - UK*, November 2014.
[22] Applications (or 'apps') are self-contained software programs that fulfil a particular purpose or enable a user to perform a task.

using social media, such as Facebook, Twitter and Linked-In, consumers provide often detailed information about their circumstances. Increasingly, consumers are able to login to websites via social media platforms, linking different sources of data.

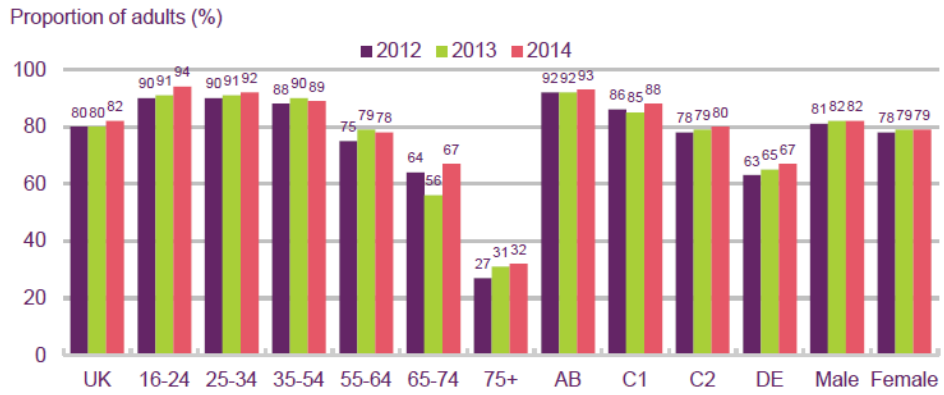
Box 2.4: Online and mobile interactions

In 2015, Ofcom reported that 86% of adults go online at home or elsewhere, and 69% of adults go online outside the home. Six in ten (61%) adults now use a smartphone to go online and 39% use a tablet to go online from home or elsewhere.

The claimed weekly hours of internet use amongst all adults stands at 20.5 hours on average. Nearly three-quarters (72%) of internet users have a social media profile, compared to 22% in 2007. Furthermore, four-fifths (81%) of these people use social media at least once a day; an increase from 30% in 2007.[23]

In 2014, Ofcom reported large differences between younger and older age groups in terms of internet access: 94% of those aged between 16 and 24 had access to the internet, compared to 32% of over-75s. In terms of social-economic group, 93% of respondents in social class AB had access to the internet compared to 67% in social class DE (see **Figure 2.3**).[24]

Figure 2.3: Home internet access by age, socio-economic group and gender



Source: Ofcom research, data as at Q1 2014.
Notes:
1. Base – all adults aged 16+.
2. QE2 – Do you or does anyone in your household have access to the internet/World Wide Web at home?

2.22 In interacting with firms, consumers may be sharing data with or without the involvement of a direct financial transaction, as follows:

- **Financial transaction** – much consumer data is generated as a result of consumers purchasing goods or services, for example via high street shopping and internet retailing. In most cases, the provision of data is a

[23] Ofcom, *Adults' media use and attitudes,* May 2015.
[24] Ofcom, *The Communications Market 2014*, August 2014.

necessary element for the completion of the transaction. Typically this involves people supplying financial information, but can also include their address details and subsequent product reviews that they might submit online.

- **No direct financial transaction** – there does not need to be a formal paid-for transaction to trigger the sharing of data between consumers and firms. Many firms that use consumer data provide products and services to consumers without an up-front or visible charge, while obtaining revenue from advertising or the use of consumer data. We consider 'free at point of use' services further in **Chapter 3**. Examples of 'free at point of use' online platforms include:
  - social networks, eg Facebook, Instagram and LinkedIn;
  - booking platforms, eg Expedia and TripAdvisor;
  - media sharing websites, eg YouTube and Dailymotion;
  - search engines, eg Google and Bing; and
  - price comparison websites, eg GoCompare and Moneysupermarket.com.

2.23 As set out in **paragraph 2.3**, consumers may be actively declaring information or passively supplying it, as follows:

- **Actively declared data** – consumers voluntarily hand over information about themselves when registering for services (for instance to use a mobile app), declaring public records, buying products, requesting quotes, participating in surveys or entering competitions. Consumers often have to supply some data, such as delivery address, contact and payment details as part of a transaction. While consumers will be aware that they are providing data, they may not always know the uses to which it might be put.
- **Passively supplied (observed) data** – consumers also generate data that is observed by businesses and collected in the background as they undertake actions. For example, the Automatic Number Plate Recognition (ANPR) records generated as people drive through some traffic zones, the location data generated by their mobiles and tablets, the movements of their mouse pointer on a web page and the search histories they leave as they browse the internet (sometimes referred to as 'exhaust' data).

2.24 There has been substantial growth in passive data collection. It is now commonplace for firms to collect data by using cookies – small text files stored on a user's computer or mobile device by websites they visit, which can, for instance, store information about the pages viewed. We consider the role of cookies further below.

2.25 More recently there has been rapid growth in the extent to which everyday objects are connected to networks and sharing data. This phenomenon is often referred to as the Internet of Things (IoT).

2.26 Ofcom reported in 2015 that over 40 million devices are already connected via the IoT in the UK, and this is forecast to grow so that by 2022 there could be 369 million devices and more than a billion data transactions a day.[25] Ofcom noted that these connections have the potential to deliver benefits across multiple sectors such as transport, health and energy.[26]

2.27 Ofcom's consultation paper noted that the IoT is a loosely defined term, often associated with machine-to-machine (M2M) communications. Basic definitions are as follows:[27]

- M2M relates specifically to the interconnection of devices, usually wirelessly – such as devices that track a car's location or monitor its engine's performance.

- IoT is a broader term, addressing the interconnection of M2M applications, potentially allowing data exchange across many sectors – for instance to manage traffic flows.[28]

2.28 In 2014, the Government Office for Science (GOS), in its review of how the UK can make best use of IoT, noted that: '…The scale of personal information, particularly locational and financial information, which is collected by existing technology, is huge. This data collected will only increase as we use more and more Internet of Things technologies…'.[29]

2.29 A number of respondents to our CFI, when asked to identify key future developments, likewise pointed to the growing adoption of newer technology that enables potentially large volumes of data collection and use (see

---

[25] Ofcom, *M2M Application Characteristics and their Implications for Spectrum*, May 2014.
[26] Ofcom, P*romoting investment and innovation in the Internet of Things - summary of responses and next steps*, January 2015.
[27] Ofcom, *Promoting investment and innovation in the Internet of Things*, July 2014.
[28] In this report, we use the term 'IoT' to cover both its broader meaning and constituent M2M communications.
[29] Government Office for Science, *The Internet of Things: making the most of the Second Digital Revolution - A report by the UK Government Chief Scientific Adviser*, December 2014.

Box 2.5). We consider in **Chapter 4** the extent to which consumers are aware they are sharing data and the implications of this.

Box 2.5: Internet of Things (IoT)

Respondents to our CFI identified various examples of devices collecting and transmitting consumer data, including:

- **Mobile phone and tablet location tracking** – shops, for example, may be able to pick up IDs unique to owners' devices and track them within and outside stores. Some apps in particular ask device owners to share their location data, and this information may be shared with other parties. Where consumers provide data to use Wi-Fi hotspots, this may be shared with third parties for marketing but also to track their in-store location. A retailer may also be able to cross-reference this information to a customer's use of its shopping app to improve its understanding of customer behaviour. A number of recent media stories suggest that retailers are testing ways in which they can record how long customers are in their stores and the routes they take, as well as to send targeted location-specific offers and discounts directly to their smartphones when visiting shopping centres.[30]

- **Facial recognition** – cameras and specialist software increasingly enable stores and advertisers to target people with particular characteristics (eg their age and gender). For instance, there have been reports of a UK grocery retailer installing face-scanning technology at its petrol stations to target advertisements to customers at the till.[31] Media stories have suggested that firms and other organisations will be able to match faces to the other data they hold on individual consumers (for instance from photographs on social media) to target them with special offers when they enter a shop or recommend particular products.[32]

- **Home automation ('domotics') and 'smart devices'** – increasingly, IoT devices such as smoke alarms, lights, washing machines, fridges, ovens and thermostats can be controlled online – for example, so that home owners can change settings while away, or to place orders (for instance so that a fridge can be restocked). Motion sensors can enable devices to react as users move around their homes. These devices are likely to be permanently connected and may share information with manufacturers or across devices.[33] Likewise, some smart TVs may share information on people's viewing that can be used to target advertising.[34]

---

[30] See, for example, the following: *(i)* Channel 4 News, *Inside the shopping centre that tracks your every move*, March 2014. *(ii)* Mobile Europe, *EE deploys Wi-Fi, heat maps to track Asda customers*, March 2014. *(iii)* Internet Retailing, *Beacons get vote of confidence with roll out across major UK shopping centre*, September 2014.
[31] See, for example: BBC News, *Tesco Petrol Stations use Face-Scan Tech to Target Ads*, November 2013.
[32] See, for example: BBC News, *Facial recognition: Shop where everybody knows your name*, December 2014.
[33] For further discussion of IoT, see: *Article 29 Data Protection Working Party Opinion 8/2014 on the Recent Developments on the Internet of Things*, September 2014.
[34] See, for example: Analysys Mason, *Report for Ofcom – Online data economy value chain*, February 2014.

- **Wearable technology and the 'quantifiable self'** – there has been a growth in wearable devices (sometimes called the 'quantifiable self'), such as watches that monitor health and glasses that record images and provide real-time location-based information. Media stories have reported how, for instance, a number of companies are seeking to use the data collected by the watches to monitor and analyse individuals' health indicators and offer tailored advice.[35]

How firms interact with consumers

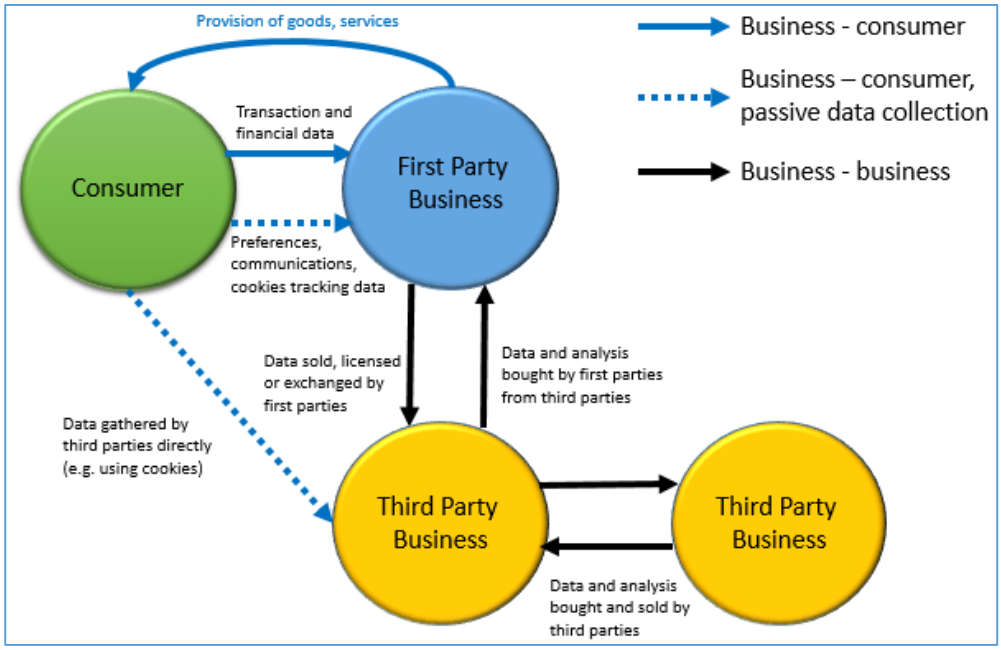
2.30 How businesses interact with consumers and each other depends on whether they have a first or third party relationship with the individual concerned (see **Figure 2.4**):

- **First parties** have a direct relationship with the consumer (ie business to consumer, B2C) and can collect data directly and exclusively from consumers through interactions – for example during a transaction for a product or service in a shop. Retailers collect electronic Point of Sale (ePOS) data which, combined with loyalty card data on the individual purchasers, can provide rich information on their transactional preferences and even personal circumstances. The internet has also enabled first parties to collect data by using cookies (see **Box 2.6**). Data gathered by first parties is often likely to be the most detailed and accurate form of consumer data.

- **Third parties** collect data from and about consumers in various ways. For example, a business may acquire data from a first party or another third party through purchase, licensing or exchange (ie a business to business, B2B, deal).[36] Third parties can also collect data by gathering publicly available data from public records or by analysing social media. In particular, however, they can use their own cookies which are installed on a user's device when they visit a first-party's website (see **Box 2.6**). Third parties may also process data and provide services to other businesses – for example, conducting analysis for other firms that may lack the required technical resources and skills. In this sense, they would be acting as an 'infomediary' – exchanging or processing data, typically on behalf of other market participants.

[35] See, for example: The Guardian, *The future of wearable technology is not wearables – it's analysing the data*, January 2015.
[36] Businesses that acquire data from first parties are sometimes called 'second parties' to reflect that they are likely to be using more accurate and detailed data than third parties.

Figure 2.4: The relationships in data collection and sharing



Source: CMA.

2.31 In practice, there are many ways in which consumers and first party firms interact depending on the sectors, products and services involved and this impacts on the nature of the data and its value. The research we commissioned illustrates how the timings and frequency of interactions can also vary by sector, as follows:

- In the motor insurance sector, the annual nature of most cover means that providers typically collect data from actual and potential customers as a snapshot once a year, close to renewal (unless a claim is made or policy details are changed). While historic data is important to developing predictive models of risk, annual data on individuals can degrade in value even within a year.

- In contrast, games developers may be able to collect information from consumers on an intermittent but on-going basis as they play games. This information can be used by the developers to update the games and provide 'fixes' when needed.

- Online clothing retailers may also have on-going but intermittent contacts with actual or potential consumers and for some they may build up a detailed dataset of their preferences over time. While data is valuable for retailers in terms of providing recommendations and personalisation, relatively recent data is more important – for example, one retailer said it only used data from the last six months.

2.32 One of the most significant developments in the last fifteen years has been the rapid rise in the volume of online behavioural data collected by both first and third parties. There are a number of ways in which information is collected from users of online devices, although 'cookies' remain the principal method (see **Box 2.6**). As we discuss below, a key use for this information is to assist targeted advertising, although there are other applications.

Box 2.6: Online data collection – cookies and beacons

There a number of methods firms use to gather information from consumers from devices connected to the internet – in particular, cookies and beacons:

- Cookies are small text files placed ('dropped') by a website's server on a user's device when they visit it and which can share contextual and behavioural information with the cookie's owner. Each cookie served is specific to the device receiving it and contains a unique anonymous identifier. 'Session cookies' are transient and automatically deleted once a browser is closed. 'Permanent (or 'persistent' cookies') may be retained on the user's device for a year or more (unless refused or deleted by the user), and can be used to track users across multiple sites. Cookies vary in the functions they perform. For example cookies may be:[37]
  - necessary – for example, remembering items in a shopping basket as users move from page to page;
  - functional – for instance, to improve a user's interaction with the site by recording their choices (eg their accessibility and display preferences, or their location to serve them with local weather forecasts);
  - performance-related – for example, recording analytical information about visitors such as what pages are most popular, how long pages are viewed, etc; and
  - advertising-related – for instance, recording when a user clicks on an advert served within the page they are viewing.
- **Beacons or pixels**[38] are single pixels embedded in a website or the body of an email and effectively invisible to users. When a web page or an email with such a pixel is opened, it sends a request to the pixel owner's server for an image – allowing the owner to track the event along with information such as the time it occurred.

[37] For more information, see the About Cookies website and the *ICC UK Cookie Guide*, November 2012, available on the International Chamber of Commerce website.
[38] Also known as a 'pixel tags', 'tracking pixels', 'web beacons' 'web bugs', or '1x1s'.

Cookies and beacons can be placed on users' devices by first party website publishers to help ensure interaction with the site and to gather information about users' behaviours that the first party might use to improve its services and products and to target users with offers, promotions and advertising.

However, many cookies and beacons are placed by third parties, with the permission of the first party. These enable the third party firms (such as advertising networks and analytical companies) to track users and their behaviour across multiple sites that use the same third party cookies. Examples of third party cookies include:

- Google Analytics – used to measure website activity and performance for search engine optimisation and marketing purposes; and
- Criteo and Struq – used to gather information to support re-targeting advertising.

Pixels can be used to transmit to a third party server that a user has registered for a service or completed a transaction (a 'conversion' pixel). Retailers can also install 'custom audience pixels' on their webpages that enable them to target consumers with adverts on social media networks such as Facebook.

Data sharing

2.33 Some data is readily available to any first or third party business for relatively low costs (for example, the electoral register and court judgements),[39] or may be available directly from an individual or a data controller. However, commonly accepted practice is that consumers should be informed, typically by first party Privacy Policies and Terms and Conditions that their information may be shared with third parties – although their level of detail may vary. We consider this issue further in **Chapters 4** and **5**.

2.34 In practice, there is a substantial amount of data sharing occurring between firms – for instance in support of first party service delivery. For example, first parties may commission third parties to gather data on their behalf and to inform their own commercial interests (such as advertising and product development) by, for example:

- enabling third parties to embed and control cookies on the first party's website to track the sites users visit;
- commissioning surveys and other market research; and

[39] For example, credit reference agencies are able to buy the full version of the electoral register (which can include names, addresses, national insurance numbers, nationality and age), while other businesses can buy the open (edited) register from which individuals can opt to have their personal details removed. Such data is typically non-rivalrous, in the sense that access to it by one party does not restrict the ability of other parties to access it.

- using specialist data collection tools, such as 'black box' telematics devices (see **Box 2.11**).

2.35 First parties may also share data with third parties for a wide range of reasons, including to:

- complete transactions – for instance to process payments or to share address details for a delivery);
- check customers' credit scores;
- prevent fraud;
- handle claims;
- maintain customer databases;
- conduct surveys; and
- inform marketing and advertising.

2.36 One respondent suggested that data sharing is common and often important for app development. For instance, restaurants might contract with developers to build apps that share data about customer preferences and demographics, and then use customer responses both to improve the app and provide analytical services to the restaurants.

2.37 Another respondent explained how the commercial use of consumer data is of growing importance in markets such as energy, where the roll out of smart meters will enable suppliers, network operators and consumers to collect more granular consumption data. Third parties such as price comparison websites and switching services may collect and, in some cases, retain consumers' data to provide alerts if potentially attractive service options arise.

2.38 Other intermediaries have emerged that provide IoT smart home management services (eg Nest and Hive), or seek to empower consumers by, for instance, helping them to manage their data use (eg Allfiled) or to make complaints (eg Resolver). We consider the role of personal information management services (PIMS) further below and in **Chapter 3**.

2.39 Third parties may also gather data from elsewhere and sell, license or exchange it with first or other third parties, such as the following:

- **Credit reference agencies** – these collect information from lenders on how people manage repayment commitments, as well as information on the electoral register, court judgements and insolvency records, to provide

businesses with this information on a subscription or pay-per-inquiry basis. These agencies, may also provide other services, including marketable contacts for campaigns.

- **Fraud prevention agencies** – these provide services to businesses to help them avoid and detect fraud. For example, as DotEcon notes, insurers can use the Claims and Underwriting Exchange (CUE) database[40] to check for multiple claims fraud or misrepresentation of claims histories, or the National Fraud Database managed by Cifas[41] to check for links to confirmed cases of fraud. In both cases, insurance providers are amongst those contributing data.

- **Demographic modelling** – a number of firms, such as Experian and Callcredit, combine anonymous socio-economic, demographic and other indicators to produce characteristics at household-level, which businesses can use in their product development and marketing.

- **Data brokers** – for example, motor insurers may source data on insurance renewal dates as possible 'leads' from third party data brokers.

- **Lead generation firms** – these may collect information through prize draws and surveys.

- **Public bodies** – these make some information available for commercial decision-making. For instance, DVLA data can help insurers validate information about consumers' driving entitlements and convictions through its MyLicence service.[42]

- **Price comparison websites (PCWs) and switching services** – these may collect information – for instance where this relates to consumers entering into an energy contract facilitated by the third party. In some sectors, these PCWs can play an important data collection role (see **Box 2.7**).

[40] See the Claims and Underwriting Exchange website.
[41] See the Cifas website.
[42] See the MyLicence website.

Box 2.7: Price comparison websites and motor insurance

In motor insurance, PCWs provide a platform for consumers to request quotes from over 100 insurers and brokers. In 2014, the CMA reported that around 77% of consumers used PCWs and around 55% of new motor insurance business was initiated through them.[43]

DotEcon notes that PCWs collect a large amount of information from consumers (about the drivers, vehicles and locations, as well as other data such as home insurance renewal dates) and share this securely and simultaneously with insurance providers. This has a number of implications, including that:

- insurance providers receive information about more consumers than they otherwise would, although only a fraction are converted to sales; and
- some insurers receive more information per consumer than they might otherwise have requested.

Data trading

2.40 Many respondents to our CFI commented that there is a large and growing trade in consumer data – whether the data is being exchanged, sold or licensed. One commented that '…almost any dimension of data can be purchased on users'. Some noted that it was possible to buy large lists of e-mail contact addresses for relatively little money. On the other hand, some respondents suggested that sharing remained limited, with many firms unsure how to use their own data, let alone engage with third parties.

2.41 Later in this chapter, we consider the value of data use to the economy, as well as some of the evidence on values placed by businesses and consumers on data types. However, as part of our high-level CFI we were not able to establish a detailed picture of the various arrangements between parties and the prices paid for different types of data. In its study of three specific sectors, DotEcon notes that, while it discussed commercial agreements in place with interviewees, information on exact values and volumes was not always available, in part because of commercial sensitivities.[44]

2.42 It is clear, however, that arrangements vary substantially depending on the parties involved and the type of data. One respondent noted that licensing the use of data was considered preferable to selling it, to ensure that the data collector retained control through the contractual arrangements.

---

[43] CMA, *Private motor insurance market investigation Final report,* September 2014.
[44] Our CFI was carried out under the CMA's general review function in section 5, Enterprise Act 2002. In carrying out a CFI, the CMA does not have compulsory information gathering powers.

2.43 There were some differences of view over whether first parties were likely to sell data wherever possible, or were more likely to regard it as too valuable to share with other firms. This suggests that there are several different business models in relation to data collection and use. We discuss below and in **Chapter 3** how some of these work.

2.44 However, it is clear that there is at least potential for some first parties to sell their data, or for third parties to sell on data they collect through their relationships with third parties. For example, in its report for us, DotEcon noted that:

- While for motor insurance, there was little concrete evidence to suggest that the sale of data to third parties was widespread at present, the FCA's thematic review of PCWs in the general insurance sector found that, while

  '…PCWs are remunerated primarily from fees they charge providers when a consumer buys a policy after getting a quote on the PCW. They may also earn income from providing data intelligence services or by selling consumers' data to third parties. PCWs generally did provide information on the basis on which they were paid but it was not always easy to find, as the information was provided separately from the quote process, in disclosures found elsewhere on the website'.[45]

- In clothing retailing, DotEcon understood that in most cases, data collected by third party service providers (for instance to provide size recommendations) was not shared with its clients or other third parties where the individuals are identifiable. However, third parties may share anonymised and aggregated data to provide customer insights. Also, in one case, the third party's privacy policy stated that it might share customers' profiles and email addresses with retail partners, service providers, subcontractors and manufacturers.

2.45 The revenue from the sale or licensing of consumer data could also be used to subsidise the cost of existing products or services available and allow a firm to compete more effectively on price with its rivals.

2.46 Apps generally were identified by some CFI respondents as a means by which their developers could collect a large range of information from users. As we noted at **paragraph 2.21**, consumers can login to websites via social media platforms and potentially link data across them. For example, as DotEcon notes, if a user logs into an app using their Facebook Login their public profile' information (including the name of the user, their Facebook link,

---

[45] FCA, *Price comparison websites in the general insurance sector*, July 2014.

profile picture, gender, location and time zone) is provided by default to the app developers.

2.47 DotEcon found that in principle, games app developers can request access to and collect a large range of data from devices – including device identifiers, data stored on the device (such as contacts, calendars and photos), sensor data (camera, microphone and location) and usage information (such as browsing and behavioural data). However, developers may limit such collection given the need to notify users about what they will collect. Furthermore, access to data is limited by the Operating System (OS) provider (see **Box 2.8**).

2.48 Its research suggests, therefore, that in practice the amount of data collected by games apps may be relatively limited – for instance pseudonymous data (linked to a unique user ID but not personally identifiable) combined with gameplay data. However developers may collect personal data directly if consumers can set up an account with them or connect to a game via a social network login.

Box 2.8: Games apps and data collection

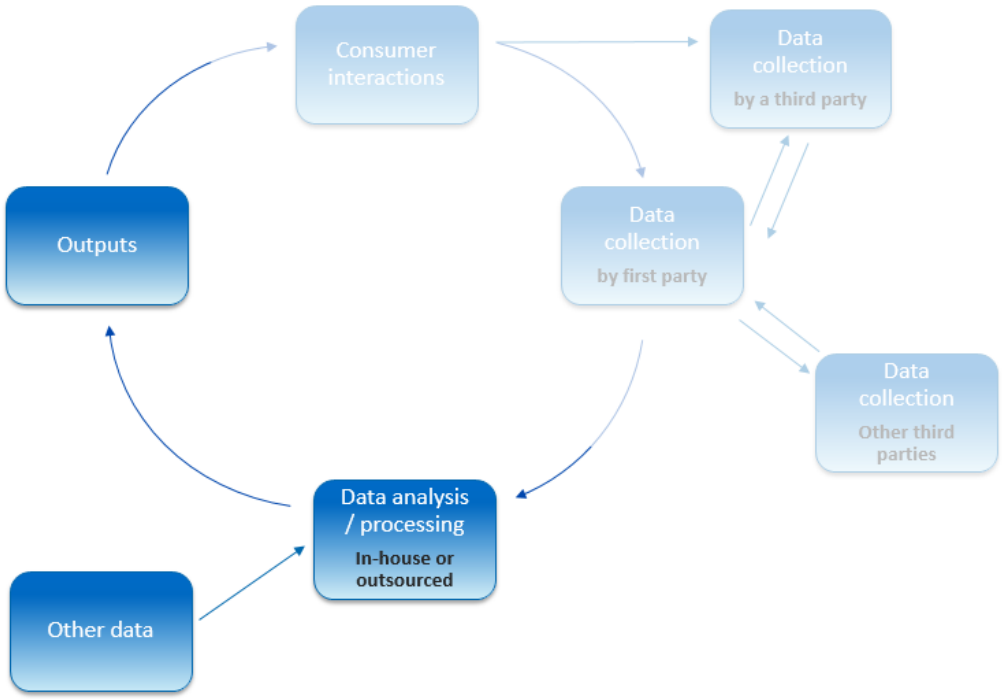
To collect data stored on devices, app developers need to interact with the Operating System (OS) of the device (such as Google's Android and Apple's iOS). These OS providers are responsible for the Application Programming Interfaces (APIs) which dictate how the software and hardware interact – including what information the app can access. APIs control the release of information according to the privacy controls in place at the OS level.

The app stores through which consumers can download games and transact, also sets guidelines for what data apps can collect, how this is shared and how consumers are informed. App stores also collect personal data, including payment card details and billing addresses to enable transactions (such as app purchases and in-app purchases). However, personal data related to payments is not passed to app developers; app stores process transactions on the developer's behalf.

Section C: Data analysis

2.49 In this section, we consider how first and third parties may use consumer data to conduct analysis and to generate value (see **Figure 2.5**).

Figure 2.5: Data analysis and outputs



Source: Simplified version of the data value chain model developed by DotEcon and Analysys Mason.

Data analysis and how data is used

2.50 Consumer data analysis, whether conducted by the first party in-house or commissioned by first parties from third parties, is an important input to firms' decision making – informing, for instance, business strategies, service provision, product development, pricing policies and advertising.

2.51 Some respondents identified a growth in sophisticated, real-time analytics occurring 'behind the scenes'. With advances in technology and storage, data can easily be stored for long periods and some data is also available to some bodies instantaneously (such as browsing data).

2.52 In 2014, GOS noted how important analysis was to extracting value from the rapid growth in data volumes resulting from the IoT: '…Although the Internet of Things can be conceived of billions of benign devices transmitting tiny

amounts of data, value will be generated from aggregating and analysing large quantities of it'.[46]

2.53 However, the usefulness and value of many types of data is likely to vary according to its age – for instance, information on an individual's immediate browsing behaviour is likely to carry more meaning than information on where they lived 30 years ago. Likewise, information such as consumers' names and dates of birth retain value for longer than their contact details (which change over time) or their current location.

2.54 Another characteristic of data is the extent to which it represents the past (for example, information that a consumer visited Paris last year) or has implications for the future (for example, information that a consumer intends to visit Paris). A number of firms responding to our CFI noted that the most immediately valuable data was 'predictive' – that is, relating to likely future purchases. Such data, however, was also likely only to have transitory value.

2.55 While data analysis may combine declared and observed data, it can also involve the creation of inferred data – that is informed suppositions generated on the basis of the available evidence. By analysing sets of data, firms may be able to infer broad characteristics about individuals to varying degrees of accuracy.

2.56 By its nature, inferred data is not generated directly by consumers but is derived from their data. One company we spoke to in the technology sector suggested that inferences built on general internet browsing data were only 59% accurate when predicting a user's gender, and only 32% when predicting their gender plus age.

2.57 In examining three case study sectors, DotEcon identified a number of examples of inferred data (see **Box 2.9**).

[46] Government Office for Science, *The Internet of Things: making the most of the Second Digital Revolution - A report by the UK Government Chief Scientific Adviser*, December 2014.

Box 2.9: Data analysis and inferred data

DotEcon identified examples of how inferred data might be used in the three sectors they looked at, as follows:

- In **motor insurance**, it was suggested that grocery retailers that also offer motor insurance might use purchasing data from loyalty schemes to draw inferences about household characteristics – for instance, to offer discounts to households that appeared from their shopping habits to be relatively low risk. Likewise, there are reports that firms consider possible correlation between individuals' financial behaviour and their driving behaviour, although such uses of inferred data may be relatively rare in the sector at present.[47]
- In **retail clothing**, firms may combine observed browsing data from cookies with information on items viewed, the time of day and data they hold about the customer including declared data (such as gender and age) and observed data from purchase and return history. From this, retailers can infer consumers' preferences – such as favourite brands, styles and colours. They might also be able to make wider assumptions – for example, a female customer who buys an item from a menswear store may be considered to be in a relationship.
- In **games apps**, firms may draw inferences about users' preferences to target in-app advertising. For example, players of sports games might be assumed to like sports generally and thus be a target for sports retailers' advertising.

2.58 Some respondents to our CFI noted that the growth of data collection and analysis has been accompanied by an increased used of algorithms to drive automated and instantaneous decision-making – for instance to make recommendations and to target offers on the basis of inferences. We consider some of the implications of these developments in **Chapter 5**.

First party data analysis

2.59 First parties may prefer to conduct their own analysis in-house, because of the extent to which it may provide a competitive advantage. DotEcon, for instance, noted that this appeared to be the case for many games apps developers and motor insurance providers.

2.60 First parties that collect data from consumer interactions may enrich this with data they already hold on those consumers, for instance in their Client Relationship Management (CRM) systems. For example, they may link account data with browsing behaviour to build a more detailed picture of an individual's interests and circumstances. DotEcon notes how some online

[47] See for example: The Telegraph, *Thrifty drivers could save on insurance premiums*, July 2014,

clothing retailers with an offline presence seek to draw together data on sales through both routes by using payment card information to link purchases made by a particular customer. Some also enable retail staff in stores to have access to customers' profiles (for instance using a tablet).

2.61 Respondents to our CFI also identified how they used data to understand their customers. For instance, a publishing company told us that it used insight gained from visitors to its website, apps and broader digital ecosystem to make advertising more relevant – enabling it to charge advertisers money, which in turn helped it keep the website open to all. Sometimes it also used its consumer data to profile consumers to send them tailored emails about its products and services.

2.62 First parties may also draw in data from third parties to inform their in-house analysis. For example:

- A number of respondents to our CFI noted that firms in insurance, financial and other sectors, may draw on data from credit reference agencies to validate the identity of consumers.

- DotEcon notes that motor insurers generally prefer to carry out the complex analysis underpinning their predictive risk modelling in-house. However, they have a strong incentive to collect more and more detailed information, because more accurate risk assessments can confer substantial commercial advantages. They may therefore seek to draw in external datasets (such as credit ratings and shopping records) to give themselves a competitive edge.

- In clothing retailing, some larger retailers have in-house IT teams and stylists that can provide tailored customer recommendations, or develop segmentation models to target types of customer based on purchasing history, spending patterns, favourite brands and styles. However, retailers may also buy in information from third party data brokers and aggregators to inform strategy – for instance, what garments sell best where and when; or data on the socio-demographic breakdown of catchment areas around their outlets, to inform store location decisions as well as stock.

- Games apps developers may have access to aggregate user data (for instance gender and age ranges) from the platform hosting their app, which they can combine with their own pseudonymous data so that they can optimise their games. For games played through social media, developers may also access information linked to the user's social network profile.

The role of third party analysts and infomediaries

2.63 A number of respondents to our CFI considered that many firms lack the expertise and technical resource to conduct some of the more sophisticated forms of consumer data analysis and application. Clothing retailing, for instance, comprises a large number of heterogeneous firms, and DotEcon reports a recent survey that suggests that while personalisation is seen as vital, many companies are held back by technology.[48]

2.64 Many first parties therefore choose to outsource some or all of the data analysis to third parties. In relation to consumer data, 'infomediaries' are third parties who share and process data – usually on behalf of other businesses. A growing number of such companies are providing other businesses with increasingly sophisticated data collection and analysis services. While some specialise in particular sectors, others operate across multiple sectors.

2.65 Many of these businesses aggregate data from multiple sources but have no direct relationship with consumers (although some have contact in terms of dropping cookies on their devices). For example:

- In clothing retailing, many retailers employ third parties to provide them with analytical capabilities so that they can offer personalised services to consumers. In doing so, they may also give third parties permission to collect consumer data directly (see **Box 2.10**). Even larger retailers may provide data brokers with access to their customer base (including declared and observed data), for instance to combine it with the latter's household-level demographic data to inform local stock policies.

- As we note above, motor insurers have a strong incentive to make use of new and detailed information to inform their risk assessments. One quite high profile example of new data collection and analysis has been in telematics (see **Box 2.11**).

- Third party analytics companies can collect game play data on behalf of app developers to help them understand user acquisition (for instance where users are coming from) and how gameplay might be improved to retain players (for instance, where game levels appear to lose players).

[48] E-Consultancy, *The Realities of Online Personalisation in association with Monetate*, April 2013.

Box 2.10: Third party data collection and analysis in clothing retailing

Given the wide range of choice and the personal nature of clothing, retailers in the sector make particular use of personalised search and recommendation tools. While some have the resources and expertise to develop and provide these services in-house, others choose to outsource them.

DotEcon identified a number of examples in clothing retailing of third parties collecting information directly from consumers and supplementing this with other data from first parties to provide them with analysis and tailored customer services using proprietary or customised algorithms. For example:

- personalisation / recommendation engines embedded in retailers' websites;
- visualisation tools to let customers see clothing on a virtual model reflecting their size and shape; and
- tools that use information provided by consumers on their measurements to help them find items of the most appropriate size and fit.

Third parties may also be able to combine this information with CRM and other data from the retailer on individuals' preferences, as well as aggregate data on brand, style and colour preferences to help provide personalised recommendations. One infomediary DotEcon spoke to explained that it also collects data itself, using an anonymous ID tag, on how consumers move around clients' sites as well as the referring website.

By offering such tools, retailers aim to increase conversions and order values, while reducing returns (the average return rate in the UK for online clothing is reported to be approximately 25%).

2.66 One large communications company responding to our CFI noted that it found that data from information services and research companies helped it to understand market trends and service penetration, while demographic information '…can be incredibly valuable to companies seeking to understand and better serve their customers.' It added that key to maintaining innovation was the encouragement of small, specialist firms who can provide analysis and insights.

2.67 Another company, in the publishing industry, explained that it might obtain consumer market research data from UK research agencies to better understand its audience or conduct research projects with similar purposes.

Box 2.11: Motor insurance and telematics

Telematics devices (or 'black boxes') can be fitted to vehicles by some providers to gather detailed data on consumers' driving behaviour. Smartphone apps can perform a similar function. Some insurers now offer these devices or apps on an opt-in basis to inform the premiums they charge. Insurers, may not be the only collectors of this information. For instance, the specialist technology firms providing the devices or apps may receive the data (and some car manufacturers may also collect such data).

Analysis of telematics information can be challenging. Large volumes of data may need to be contextualised using other information (for instance speed limits and the weather). For this reason, insurers may outsource the collection, processing and analysis of telematics data to specialists.

DotEcon also notes that the complexity of this information, combined with a lack of standardisation and the providers' reluctance to share data that can offer competitive advantage, means that consumers typically cannot access the full data and analysis or 'port' it to other insurance providers (unlike no claims discounts, which are typically transferable).

2.68 A number of third party firms also now offer tools and services that enable first parties to gain insights on how their brands and products are being discussed online (sometimes referred to as 'social listening', 'opinion mining' or 'sentiment tracking'). By analysing the extent to which they are mentioned in social media content (such as blogs, microblogs, forums, news sites and social network sites), whether trends are positive or negative and why, firms can adjust their marketing activity.

2.69 Users of these tools and services can collect consumers' views at an aggregate level and decide how to react – for instance by improving their products, by running more targeted campaigns, or by joining in conversations to seek to influence sentiment.

2.70 Social media data may also be useful at the individual level. For example, DotEcon noted that some motor insurance providers have been able to detect fraud using individual information from social media. More generally, social media data plays an important role in clothing retail (see **Box 2.12**).

Box 2.12: Social media in clothing retailing

DotEcon notes that some retailers interact directly with consumers who 'like' their pages on sites such as Facebook.

However, some also use specialised infomediaries to conduct 'social listening'. As we note in the next Section, this information can help firms quickly to understand and react to public opinion.

While much of the data collected is publicly available, it can also contain information such as names and other public information on consumers' profiles. Information such as tweets may also include the time and location at which they were made.

Section D: The uses and benefits of consumer data

2.71 As we note above, firms may sell or license data about consumers for others to use – thus directly generating revenue, which might be used to subsidise existing products or services available and allow them to compete more effectively on price, with subsequent benefits for consumers.

2.72 Responses to our CFI, as well as DotEcon's findings, suggest that, in addition to its sale or licensing, there are a number of common commercial uses for consumer data. These include:

- **growing sales through targeted advertising and offers** – to build loyalty and draw in new custom;
- **customer analysis** – for instance, to assess risks and prepare quotes;
- **personalised products and services** – for instance to make tailored suggestions more suited to individual consumers' interests;
- **product improvement and development** – for example to fix problems or create new products; and
- **business processes, strategy and efficiency improvements** – for instance to speed up transactions and reduce the likelihood of returns.

2.73 As a result of these activities, firms can generate revenue and value for themselves. However many respondents to our CFI also identified how consumers might benefit directly and indirectly from firms' using their data in these ways. We consider these issues further below.

Growing sales through targeted advertising and offers

2.74 Of all the possible uses of consumer data the most visible (and most frequently cited by respondents to our CFI) is its application to advertising. In particular, respondents noted its use to target advertisements to particular consumers, based on knowledge about their interests, preferences or other characteristics.

2.75 Firms use information about consumers to seek to increase consumption of their products and services by:

- targeted advertising, which can increase the conversion rate from advertisements to purchases of a range of products and services available; and
- using data on consumers' previous purchases or areas of interest to cross-sell related products and services (for instance 'you may also be interested in…' messages on websites).

2.76 The benefits from this are likely to arise in a wide range of markets but may be more likely to occur through online sales channels, due to the ease with which data on preferences and purchases can be acquired and specific advertisements and messages can be targeted to encourage consumption.

2.77 The internet and connected devices have provided both the means to display adverts to consumers, and to gather data on internet users to tailor the adverts displayed to their viewing habits. As a result, the value of online advertisements can be enhanced, because they are more likely to be of interest to the consumers in question and thus more likely to successfully prompt them to purchase the item.

2.78 Similarly, respondents noted that firms can avoid the wastage costs of poorly directed advertising while potentially reducing customer annoyance levels from irrelevant adverts and building loyalty by making tailored offers. The ability to measure the impact of advertising almost instantly and to analyse increasingly rich evidence on consumer views also allows firms to move at a faster pace to improve their service offers to match demand.

2.79 From the consumer's point of view, targeted advertisements can save them time and reduce annoyance levels, by ensuring they receive meaningful marketing and recommendations about services that are more likely to be of interest to them. The efficiencies and firms' savings from reducing ineffective advertising may also feed through to lower prices and special offers. Many online retailers also use data they hold about consumers to provide them with tailored suggestions when they visit their sites.

2.80 Respondents to our CFI suggested that data was also used in many markets to provide tailored offers – for instance, to inform loyalty scheme discount vouchers. Some noted that consumers can benefit significantly from these contextualised and sometimes real-time offers, although others raised concerns about potential discrimination. We consider these issues further in **Chapter 3**.

2.81 The importance of advertising (and thus of consumer data) can vary by sector. For instance, DotEcon reports the following:

- While in-app advertising is a means games developers use to monetise their games and cross-sell, it appears to be less important than in-app purchases as a source of revenue and the focus on consumer data is therefore particularly on understanding existing users' behaviour.
- For motor insurance, while consumer data-based advertising plays an important role, the nature of insurance as a product means that this is less developed than in some other sectors with a larger range of product types and more heterogeneous consumer preferences.
- In contrast, advertising is particularly important to the clothing retailing sector, where targeted email shots that display personalised recommendations and the use of cookies for online behavioural advertising is common. Some retailers also use data brokers or social media to find and target potential customers with particular characteristics.

2.82 Digital advertising spending has been growing rapidly.[49] IAB/PWC estimates that digital advertising spending grew by 14% from 2013 to £7.2 billion in 2014, and that this represented 39% of all UK advertising.[50]

2.83 Digital advertising comprises three main types of advertising: paid for search, classified and display (**Box 2.13**). Of these types of advertising, the one most associated with the use of consumer data is display advertising and, specifically, behavioural (or 'targeted') advertising, which is based on individuals' web browsing behaviour.

[49] Digital advertising comprises online advertising (viewed on PCs and laptops), mobile advertising (adverts tailored for viewing on mobile devices) and tablet (adverts tailored for viewing on tablet devices), as well as adverts on any other types of internet-connected devices (such as smart TVs and game consoles).
[50] IAB, *IAB / PWC Digital Adspend Full Year 2014 with WARC*, April 2015. These figures include advertising on PCs, laptops, mobile devices and tablets, but not on devices such as smart TVs and game consoles.

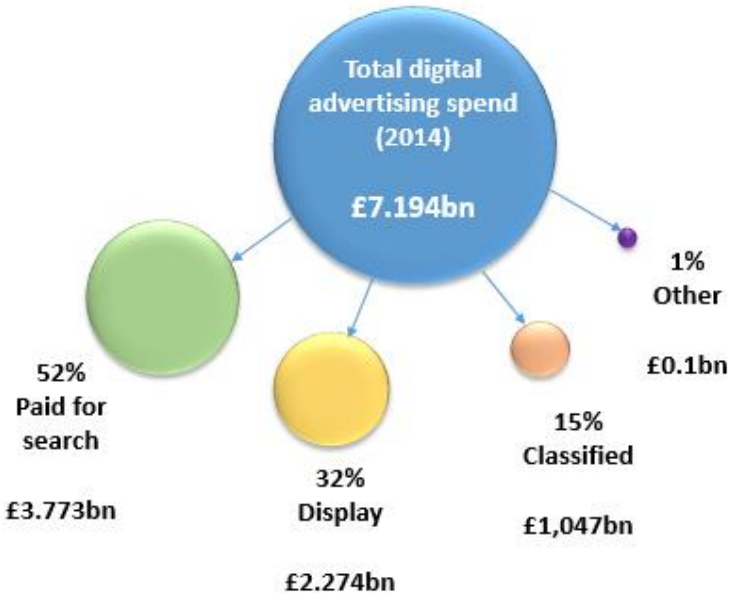
Box 2.13: Digital advertising

Digital advertising spend comprises:

- **Paid for search** – where an advertiser pays for its site to be included in a search engine's results for a specified term.
- **Classified advertising** – which includes websites that offer recruitment advertising, motor advertising and online directories of service providers.
- **Display advertising** – which includes banners and videos shown next to content on web pages and emails, and in-game advertising.

The IAB reports that display advertising has grown from £697m (21% of digital) to £2,274m (32%) in 2014 (see **Figure 2.6**).

Figure 2.6: Total digital advertising spend (2014)



Source: Based on data from IAB/PWC.

Display advertising itself includes a number of different advertising methods, including the following:

- **Contextual advertising** – where advertisements are served to reflect the context of the site or search engine query (for instance, a user sees an advert for sun lotion when booking a flight). This advertising is driven by the content of the page, not information on the user.
- **Content marketing** – also known as 'native' advertising, this includes paid for sponsorship and advertorials that fits with the surrounding look and feel of the site.

- **Demographic advertising** – where users are served advertisements whilst on a site based on information they have provided, for instance when signing up or filling in a form. While some information may be retained, individuals are not identifiable.
- **Behavioural advertising** – also known as online behavioural advertising (OBA), this involves serving display advertisements based on inferences drawn on users' website visit history across many sites (their searches, the sites they visit and the ads they click on), based on device identifiers such as cookies.
- **Retargeting** – where users are served adverts on sites they visit based on their previous visit to a different site on a device. The aim is usually to target consumers who appeared to be considering a purchase but left a site before doing so, to drive up sales conversions.

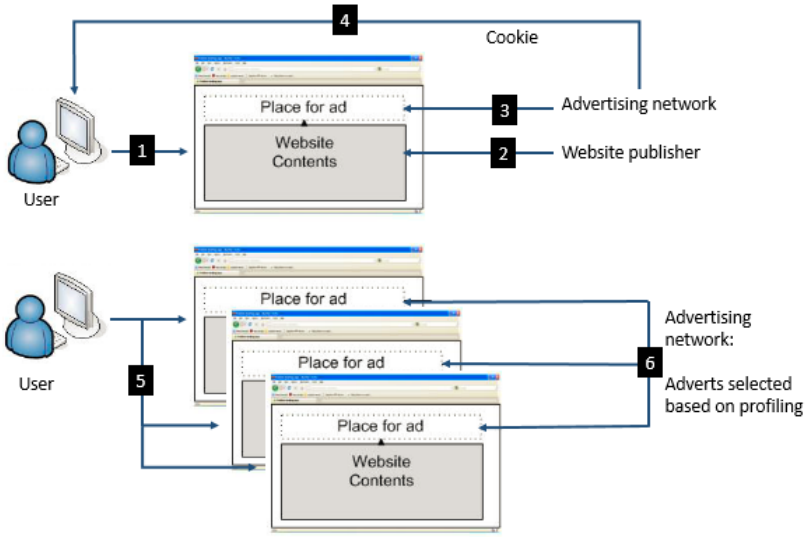
2.84 Put simply, digital display advertising relies on advertisers buying advertising space ('inventory') from sellers – that is, website publishers and app providers. Behavioural advertising and retargeting are the main forms of digital advertising that make use of consumer data to select more customised adverts to fill available inventory (see **Box 2.14**).

Box 2.14: Behavioural advertising

From the consumers' point of view, behavioural advertising can become apparent when they see adverts on their computer or device that appears to have some relationship to their recent online behaviour. For example, third party behavioural advertising could involve the following stages (see **Figure 2.7**):

1. A device user visits a website whose publisher has partnered with an ad network.
2. The site provides content.
3. The ad network places an advert, which initially may be contextual or content-based.
4. The ad network also drops an identifying cookie on the device.
5. The device user (or someone else using the device) visits other sites, some of which are part of the same ad network and which recognise the cookie (and thus device).
6. The ad network builds a profile linked to the device and can therefore select adverts from its clients most relevant to this profile.

Figure 2.7: Behavioural advertising



Source: CMA.

2.85 The business models and processes in digital advertising can be complex and involve a number of players and intermediaries. These models are also fast evolving. A number of respondents during our CFI, for instance, told us that the most significant recent development in display advertising has been the growth in programmatic advertising – the fully automated buying and selling of digital advertising space.

2.86 This real-time method of buying and selling inventory can enable adverts to be served to users' devices within milliseconds, offering increased accuracy by targeting refined audiences rather than the previous method of buying audiences in bulk tranches of thousands. The IAB estimates that in 2013, 28% of all digital display advertising was traded programmatically and that by 2017 this could increase to between 60% and 75%.[51]

2.87 We consider in **Chapter 4** the extent to which consumers are aware of the use of their data for advertising, as well as their attitudes towards this and the other uses of their data.

[51] IAB, *Programmatic accounts for 28% of UK display advertising*, June 2014.

Customer analysis and risk assessment

2.88 As we note above, the collection and analysis of consumer data is key to developing an accurate understanding of how to recruit and retain customers. In some sectors it can be a key competitive asset in targeting offers.

2.89 For example, the motor insurance sector has a long history of using consumer data to inform its risk profiling of individuals and to set premiums. Consumers, when requesting quotes or making claims, provide much of the information about themselves and their vehicles that the insurance firms need. However, insurers can also enrich this information with their own data or information from third parties to support risk assessments.

2.90 A number of respondents to our CFI operating in financial services noted the use of data from third parties to check customer information for possible mistakes or potential fraud. DotEcon suggests that the benefits from better fraud detection can be significant. According to the Association of British Insurers (ABI), fraud is estimated to add £50 to the average general insurance premiums,[52] so any savings could benefit both firms and consumers.

2.91 A number of CFI respondents also emphasised that not all consumer data collection is about generating revenue. Some firms need to collect and analyse data to meet regulatory obligations – for example checking financial transactions to spot suspicious activity and satisfy anti-money laundering requirements, or in support of the Priority Services Register.[53]

Provision of personalised services

2.92 One of the main reasons for the growing use of consumer data identified by respondents to our CFI was its value in informing the development of products and services tailored more closely to the needs of individual consumers.

2.93 DotEcon's analysis of the clothing retailing sector provides some illustrative examples of how data is being used in practice. Retailers use personal data (usually provided by customers directly) and pseudonymous data (such as browsing history)[54] to develop rich customer profiles and inferences about their preferences. DotEcon note how personalised search results and product

---

[52] ABI, *Fraud*.
[53] The Priority Services Register is a scheme run by energy suppliers which offers extra free services to people who are of pensionable age, are registered disabled, have a hearing or visual impairment, or have long term ill-health.
[54] Browsing data can be pseudonymous, but it might also be linked to specific individuals (for instance when a user is browsing the website while being logged in).

recommendations allow retailers to increase the conversion of consumer interest into sales and average order value.

2.94 Some respondents to our CFI mentioned that consumers benefited from being able to buy products more suited to their needs and interests, while others noted that customer services could also be improved by the use of consumer data to personalise this for individuals.

2.95 Consumers also benefit from reduced search costs and a better shopping experience, which could lead to improved sales for firms. For example, one third party provider of recommendation services suggested it could give retailers a sales uplift of 20% and increased average order value of 50%.

Product improvement and development

2.96 Consumer data can also help firms to identify potential gaps in markets and demand for products and services that do not exist, and to develop new ways to address them. For example:

- the analysis of consumer data could them develop products that otherwise would have been too risky to progress; and
- one respondent to our CFI explained that companies' research and development teams used customer segmentation analysis to identify where there might be gaps in their product range.

2.97 Another noted how real-time data collection and processing tools enabled companies to react quickly to customer needs. DotEcon provided examples of such data use in the three sectors it examined. In particular, it identified the following:

- In the games apps sector, ongoing analysis of user data is particularly important to optimising games – for instance to identify problems with levels and to set an adequate difficulty level that avoids both boredom and frustration on the part of players. Getting this right is often critical to how effectively the app developer can monetise the game (see **Box 2.15**).
- In the clothing sector, where for many retailers it is particularly important to stand out from competitors with new and popular designs, retailers make significant use of customer behavioural data and feedback (as well as social media listening) to inform product development and selection.

Box 2.15: Games apps and monetisation

DotEcon notes that the main use of consumer data by game developers is to gain insights about usage to inform game design and improve the user experience. There are a number of ways in which developers can earn revenue from their games, including:

- charging for initial download;
- advertising within their games; or
- offering ad-free versions of games for a fee.

However, the primary method of monetisation is by offering games for free, but allowing users to make purchases within games (in-app purchases) if they want to – for instance to make a level easier. This 'freemium' model accounts, for example, for 90% of revenue generated from the 'games' category apps in the Apple app store. In practice, only a very small minority of players make in-app purchase, and app developers are particularly keen to acquire 'whales' (players with a high propensity to make such purchases).

There is, therefore, an important relationship between consumer behaviour and how effectively app developers can drive up their revenues. By optimising the user experience, developers aim to increase engagement and keep users playing for longer – so increasing the volume of in-app purchases.

Business processes, strategy and efficiency improvements

2.98 Respondents to our CFI suggested that consumer data was also used to improve internal processes and efficiency. For example, by retaining and using consumers' details, retailers can:

- make transactions more streamlined and frictionless by, for example pre-filling forms and avoiding the need to request information more than once (simultaneously improving the consumers' experience);
- improve how they communicate with consumers – avoiding unnecessary or inappropriate communication (for instance where consumers have moved or died); and
- tailor content and provide advice – for instance, helping consumers gain quicker access to particularly relevant online services, or making it easier to navigate to areas of interest in a large online site.

2.99 As well as benefitting consumers by improving the quality of interactions, firms can identify strategic and efficiency improvements. For example, as we noted above in the clothing sector, firms can use consumer data to:

- fine-tune warehousing and logistics practices to match where particular products are most in demand;
- identify where best to locate stores, according to local area socio-demographic data;
- decide what products to stock where and when, according to localised data on demand and what products or brands are popular (for instance based on complaints about lack of stock), or are underperforming; and
- reduce the likelihood of returns by making recommendations more suitable.

2.100 One respondent suggested that in utility sectors, such as energy, more granular data from smart meters could, for example, help distribution network companies manage the connection of new load, plan the reinforcement of the existing network and investigate supply issues.

2.101 Firms can also use data from social listening services to gauge public reaction to marketing campaigns and sentiment about brands; identify potential 'PR' concerns and enable businesses to handle (or prepare to handle) consumer complaints.

Other ways consumers may benefit from their data

2.102 Many of the benefits for consumers suggested by respondents effectively reflected the 'flipside' of the benefits identified for firms (for instance from targeted advertising and product improvement). However, some were specific and potential benefits to consumers from the use and aggregation of their data, including 'free at point of use' services and personal data services.

2.103 Many respondents identified how consumers were able to make use of services such as search, social media and email without having to pay for them. Internet users can, for example, explore freely on the internet without having to pay directly for content on every site they visit. Some, however, added that whilst such tools appeared to be free, they were in effect being 'paid for' by consumers sharing data. We discuss in **Chapter 3** the implications for competition in these markets and consider in **Chapter 4** the extent to which consumers are aware of this form of 'value exchange'.

2.104 Some respondents to our CFI noted that consumers could use services such as personal credit checks and references to enable them to prove their identity, access services and make purchases.

2.105 Others pointed to the development of consumer-facing intermediaries sometimes referred to as Personal Information Management Services (PIMS). A number of new services have emerged that seek to enable consumers to manage the storage and control of their data from one location (eg Mydex and Allfiled).

2.106 These 'personal data stores' may, for instance, charge companies a fee to access consumers' data. They offer users a range of services, including safe record keeping; automatic form completion; a central digital letterbox for sharing information with, and receiving data from, suppliers; controls to help consumers manage and filter what information they share with which organisations; and personal profiles that consumers can more easily share and can use to make more informed decisions about their needs.

2.107 Some personal data services also aim to help consumers monetise their data, for instance by 'renting' it to brands (eg Datacoup and Handshake), some of which also enable consumers to derive value directly from their information by sale or licensing.

2.108 In April 2011, the then coalition government instituted the midata programme to encourage organisations to give their customers access to their data in an easy-to-use, secure and portable way.[55] The initiative focused on energy, personal current accounts, credit cards and mobile phones – selected as sectors where consumers have long term and frequent interactions with suppliers and where it is hard for them to compare costs.[56]

2.109 In March 2015, as part of the midata initiative, Gocompare.com launched an online comparison tool to enable customers of the UK's six largest current account providers to upload their statements and find out if they could switch to a current account that might better suit their personal banking history.[57]

2.110 It was suggested to us during our CFI that personal data management services represent a potentially significant development. For instance, Ctrl-Shift has suggested that a mature market for PIMS would be worth £16.5

[55] BIS, *The midata vision of consumer empowerment*, November 2011.
[56] BIS, *Review of the midata voluntary programme*, July 2014.
[57] HM Treasury, *Is your bank giving you the best deal? Find out using new online comparison tool*, March 2015.

billion, making up 1.2% of the UK economy.[58] Some of the issues around the development of this market are considered in **Chapter 3**.

The value to the UK economy

2.111 The discussion above demonstrates the broad range of benefits from the collection, analysis and use of consumer data that can accrue to both consumers and firms.

2.112 Where such benefits are large and apply in large markets or across multiple markets in the economy, they could have a positive impact on UK economic growth. This could arise as the efficiencies from competitive markets allow firms to use fewer resources to generate a specific level of output, thus freeing existing resource to be used in generating new products and services.

2.113 As we note above, better advertising can generate increased consumption. It can also help enable firms to cross-sell products and services to consumers based on their preferences and other purchases. Moreover, the use of consumer data to generate innovative new products and services can affect economic growth directly.

2.114 Various studies have considered how to measure the benefits from the use of data and we report some examples in **Box 2.16**. We have not sought to assess in detail or replicate this analysis. However, estimating the value of consumer data use is very hard given the various ways in which it is used within and across multiple sectors for a wide variety of reasons, as well as the lack of comparable and reliable data. In practice, therefore, it is unlikely that any single methodology can produce a complete and robust estimate of the value of consumer data to the UK economy.

Box 2.16: The value of consumer data to the UK economy

At the level of individuals and differing data types, various studies have suggested ways in which values might be assigned – whether from firms' or consumers' points of view.

For instance, OECD (2013) suggested a number of possible methods for measuring the monetary value generated by the use of consumer data, including the following:

- Market capitalisation per individual record – for example, the implied market capitalisation per Facebook user was between US$40 and US$300 at different times between 2006 and 2012.

[58] Ctrl-Shift, *Personal Information Management Services: An analysis of an emerging market*, July 2014.

- Revenue or net income per record/user – for example, Facebook and Expedia's annual revenue per record/user (ie total net income of the company divided by the total number of US users) was approximately US$4–7.

- Available evidence on market prices at which personal data are sold – for instance, OECD reported that at the time of its report, examples of prices in the United States for personal data ranged from US$0.50 for a street address, US$2 for a date of birth, US$8 for a social security number, US$3 for a driver's license number and US$35 for a military record.[59]

In addition, Orange (2014) found that UK consumers assigned different values to their personal data depending on the type of data and level of familiarity with the organisation collecting it. For instance, they reported that survey respondents on average valued their full name and date of birth at £12.14 if sharing with a familiar organisation, but £15.02 if an unfamiliar organisation. Likewise they valued their location at £13.99 for a familiar organisation but £17.66 for an unfamiliar one.[60]

We have not assessed the robustness of these methodologies, but there are likely to be significant limitations to them. For instance, market capitalisation and firms' revenues are affected by many factors unrelated to consumer data; and it is likely to be hard for consumers to place values on their data. However, these suggestions serve to underline the difficulties in assigning value to data and the wide range of estimates.

At an aggregate level, in 2012, Boston Consulting Group[61] estimated that in 2011 the direct revenues of data-driven businesses across the EU were €58 billion, while the value extracted from personal data was €315 billion. Given that UK GDP accounts for approximately 16% of the EU total, the value extracted from personal data covering UK consumers in 2011 could have been approximately €50 billion.

We have not considered in detail the methodology and robustness of this estimate. Such calculations across the EU can be very complex, given the different structures of the member states and their governments, and that assumptions appropriate for estimates in one member state may not be appropriate in another.

Also in 2012, Cebr estimated the UK economy-wide benefits from 'big data', finding this to be worth £216 billion over the six years from 2012 to 2017. Divided evenly between those six years this suggests a figure of £36 billion annually. Cebr noted that:

> 'The economic model used to quantify the macroeconomic impact of data equity was designed to analyse three broad sources of benefits:
>
> - Enterprise-level business efficiency gains from big data…

---

[59] OECD, *Exploring the Economics of Personal Data. A survey of methodologies for measuring monetary value*, April 2013.
[60] Orange, *The Future of Digital Trust: A European study on the nature of consumer trust and personal data*, September 2014.
[61] Boston Consulting Group, *The Value of our Digital Identity*, November 2012.

- Enterprise-level business innovation gains from big data…
- Enterprise-level business creation gains from big data.'[62]

We have not reviewed this analysis in depth and note that its consideration of big data may be broader than the definition of consumer data that we have adopted. The value of £36 billion annually is, however, of the same order of magnitude as the figure suggested in the research undertaken by the Boston Consulting Group.

Section E: The regulatory environment

2.115 In this section, we set out the key regulations and elements of industry self-regulation which may apply to the collection and commercial use of consumer data.

2.116 The enforcement of regulations falls to a number of organisations, including ICO, Ofcom and the CMA. In **Chapter 5**, we consider their role and regulatory issues highlighted by respondents to our CFI, including new developments such as the General Data Protection Regulation (GDPR).

Data protection regulation

2.117 Two key laws in this area are the Data Protection Act 1998 (DPA) and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR).

Data Protection Act 1998

2.118 The DPA implements the Data Protection Directive.[63] It requires organisations to handle personal data fairly and legally. **Box 2.17** provides further details.

[62] Cebr, *Data equity: Unlocking the value of big data – Report for SAS*, April 2012.
[63] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Box 2.17: Data Protection Act 1998

Key requirements of the DPA relevant to this CFI include that:

- Businesses must collect and process personal data fairly. Consent is not necessarily required, for example if the processing is necessary for the performance of a contract or is in the legitimate interests of the data controller and this does not prejudice the legitimate interests or fundamental rights of the data subject, including the right to privacy. A balance must be struck between these competing rights.[64]

- Where consent is the condition under which data is processed, it must be a freely given, specific and informed indication of the data subject's wishes by which the data subject signifies his or her agreement to personal data relating to him or her being processed. 'Passive' consent is not sufficient.

- Providing information about the identity of the data controller, the purpose(s) for which the data are to be processed (particularly if the purpose is unexpected or intrusive), and any other necessary information, will go towards making the processing fair.

- Personal data which has been collected for one purpose should not be used for a different and incompatible purpose. If a data controller wishes to use data for a different purpose then they should assess whether it is incompatible with the original purpose. They need to be transparent about this, ensuring individuals are appropriately informed and provided with the opportunity to give their consent to the new processing in appropriate cases.

- Personal data must be held securely and not retained for longer than necessary.

- Data subjects have a number of other rights: the right to obtain their data; the right to prevent processing likely to cause damage or distress; the right to prevent processing for direct marketing; rights in relation to automated decision making; and, in appropriate cases, rectification, blocking, erasure and destruction.

There are additional protections for the processing of sensitive data. Sensitive personal data includes, among other things, physical or mental health or condition, and racial or ethnic origin.

PECR

2.119 PECR implements, in part, the Directive on privacy and electronic communications.[65] It provides protections against nuisance marketing in the form of live marketing calls and spam. In particular, the regulations apply to

---

[64] The relationship between privacy rights and data protection has been considered by the CJEU most notably in the recent 'right to be forgotten' case (see **footnote 354**).
[65] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. PECR was amended in 2004 and 2011. See ICO, *Privacy and Electronic Communications Regulations*.

the use of cookies (see **Box 2.18**). We discussed the role of cookies earlier in this chapter.

Box 2.18: PECR

PECR provides various protections against nuisance calls, texts and email. In addition, it applies to the use of cookies or similar technologies to store information (or access stored information) on a user's device: the so-called 'cookie law'.[66]

Under the cookie law, before businesses use cookies, they must:

- provide clear and comprehensive information; and
- obtain freely given, specific and informed consent

unless it is 'strictly necessary' to provide the service.

These requirements do not only apply to cookies which store personal data but to the storage of all forms of data.

Consumer protection

2.120 Key consumer protection regulations which may govern practices in this area include:[67]

- the Consumer Protection from Unfair Trading Regulations 2008 (CPRs);
- the Unfair Terms in Consumer Contracts Regulations 1999 (UTCCRs);
- the Consumer Contracts (Information, Cancellation and Additional Charges) Regulations 2013 (CCRs); and
- the Consumer Rights Act (CRA) which, from October 2015, will replace a number of existing laws and consolidate the existing consumer protection legislation on unfair terms.

[66] For convenience, we refer generally to cookies but the principles apply equally to similar technologies such as locally stored objects (flash cookies) and device fingerprinting (see Data Protection Working Party, *Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting*).
[67] A range of other legislation could also apply in this area, for example the Equality Act 2010, which prohibits discrimination in the supply of goods, services or facilities based on 'protected characteristics' of age, disability, gender reassignment, pregnancy and maternity, race, religion or belief, sex or sexual orientation, could apply in the case of businesses which may discriminate, for example, through the analysis of data to target individuals based on racially discriminatory algorithms.

2.121 The main scope of each of these regulations, with a particular focus on how they may apply in this area, is described below.[68]

CPRs

2.122 The CPRs prohibit unfair commercial practices which distort consumers' transactional decisions.

2.123 Broadly speaking, the CPRs require firms not to treat consumers unfairly, and prohibit misleading or aggressive commercial practices, where these are likely to have an impact on a consumer's transactional decision. Certain practices are considered unfair in all circumstances and are prohibited. See **Box 2.19**.

Box 2.19: CPRs

Businesses may infringe the CPRs if they engage in the following categories of commercial practices, namely those which:

- fall short of an objective standard of acceptable behaviour (professional diligence) and which have, or are likely to have, an effect on the economic behaviour of the average consumer (reg 3(3)). This is known as the general prohibition;
- are misleading actions (reg 5) or misleading omissions or are aggressive (reg 6) and which, in each case, cause or are likely to cause the average consumer to take a different 'transactional decision' that he would not have done otherwise; or
- 'are in all circumstances considered unfair' (Schedule 1), with no assessment needed whether they may affect the decision-making of the average consumer,[69] for example, claiming to be a signatory to a code of conduct when the trader is not, or displaying a trust or quality mark without proper authorisation (practices 1 and 2 of Schedule 1).

A 'transactional decision' under the CPRs has broad scope. It has been interpreted by the CJEU to include a range of pre-purchase and purchase decisions, such as a decision whether or not to enter a shop with a view to making a purchase.[70] In the opinion of the CMA, in the online environment, it may also encompass a decision whether to visit a website of one particular trader over another when seeking to purchase similar products.

[68] The fact that certain aspects of the regulations are not highlighted here does not mean that they may not have potential application in future cases.
[69] These practices are deemed always to materially distort the decision-making of average consumers.
[70] *Trento Sviluppo srl v Autorità Garante della Concorrenza e del Mercato,* Case C-281/12 [2013] 00000; [2014] 1 WLR 890. Paragraph 36.

Breach of the CPRs may be a criminal offence and may also be enforced by way of civil enforcement.[71]

Unfair Terms in Consumer Contracts Regulations 1999

2.124 The UTCCRs protect consumers against unfair standard terms in contracts with sellers or suppliers of goods and services. See **Box 2.20**.

Box 2.20: UTCCRs

The UTCCRs implement the Unfair Terms Directive.[72] All suppliers[73] using standard contract terms[74] with consumers[75] must comply with the Regulations.

The OFT produced guidance in 2001 (updated in 2008) which has been adopted by the CMA.[76] This guidance is presently being revised to reflect the provisions of the Consumer Rights Act which is expected to come into force in October 2015.

The principal intention behind the legislation is to protect consumers against one-sided standardised contracts which favour businesses, for example 'small print' terms. A consumer is not bound by a standard term in a contract with a seller or supplier if that term is unfair, subject to certain exceptions.

The main exception is that the fairness test does not apply to terms that set the price or define the main subject matter of the contract (usually known as 'core terms') provided they are in plain and intelligible language. The Regulations also do not cover terms that reflect mandatory statutory or regulatory provisions, for example terms which reflect statutory compensation limits (provided the terms adequately reflect the law).

Under the Regulations, a standard term is unfair 'if, contrary to the requirement of good faith, it causes a significant imbalance in the parties' rights and obligations arising under the contract, to the detriment of the consumer'.[77]

Schedule 2 to the Regulations provides an illustrative and non-exhaustive list of types of terms which may be regarded as unfair insofar as they have particular objects or effects. This is commonly called 'the grey list' to reflect the fact that such terms are not necessarily unfair.

---

[71] OFT1008, *Consumer Protection from Unfair Trading*, August 2008.
[72] EC Directive 93/13/EEC on unfair terms in consumer contracts.
[73] 'Seller or supplier' means any person or organisation acting for the purposes of their business. This includes any trade or profession, and the activities of government and other public bodies.
[74] Standard terms are those devised by a business in advance, not individually negotiated with the consumer.
[75] A consumer is an individual not acting for the purposes of his or her trade, business or profession.
[76] OFT311, *Unfair contract terms guidance - Guidance for the Unfair Terms in Consumer Contracts Regulations 1999*, September 2008.
[77] Regulation 5(1).

CCRs

2.125 The CCRs implement parts of the Consumer Rights Directive (CRD). Broadly, these Regulations provide that certain pre-contract information must be provided by traders to consumers (see **Box 2.21**).

2.126 The CCRs apply whether or not the consumer pays with money (for example if the product is being provided in exchange for personal data). The pre-contract information includes the functionality of digital content.

Box 2.21: CCRs 2013

The required pre-contract information includes, among other things, the main characteristics of the goods, services or digital content (to the extent appropriate to the medium of communication and to the goods, services or digital content) and, where applicable, the functionality, including applicable technical protection measures, of digital content.

The CMA takes the view that functionality which involves tracking or personalisation may fall within these pre-contractual information requirements.

Consumer Rights Act

2.127 The CRA will replace a number of existing laws relating to B2C transactions including the Sale of Goods Act 1979 and the Supply of Goods and Services Act 1982. It will also consolidate existing consumer protection legislation on unfair terms which is currently set out under the Unfair Contract Terms Act 1977 (UCTA) and the UTCCRs. It will clarify and amend the law to streamline consumer rights and remedies into a single regime.

2.128 Of particular relevance to our CFI is that:

- consumers who buy digital content under a contract will have statutory rights that such digital content will be of satisfactory quality, fit for a particular purpose and 'as described';
- these rights and remedies are based on those for goods (this is intended to clarify the previous uncertainty as to whether digital content is a good or a service);
- these rights will apply only to digital content which has been paid for with money, directly or indirectly. They do not apply where the digital content is supplied under contract in exchange for something else, such as personal data;

- however, the Act expressly reserves the right in future to extend these protections to digital content contractually supplied in exchange for something other than money if it is appropriate to do so because of significant detriment caused to consumers (section 33(5));

- under the unfair terms provisions in the CRA, fairness assessments apply to consumer notices as well as contractual terms, and whether or not payment has been made, for example, non-contractual privacy policies and end user licence agreements which may not clearly be part of the consumer contract; and

- the protections in the 'grey list' are largely unchanged from those in the UTCCRs.[78]

Self-regulation

2.129 The OFT, one of our predecessor bodies, noted that self-regulation[79] can offer '…benefits for consumer protection and adds real value to the functioning of efficient markets'.[80]

2.130 For this report, we did not conduct a detailed review of all self-regulatory activities as they relate to the collection and use of consumer data. However, we note that industry has developed a number of initiatives that have a particular relationship to consumer data and which aim to supplement data protection regulation.

2.131 These initiatives operate predominantly in advertising, marketing and market research. This is unsurprising given that data is an essential element of market research and, as we note in this chapter, advertising is increasingly informed by consumer data.

2.132 The main initiatives we considered[81] were the:

---

[78] See CMA, *Draft guidance on unfair contract terms – consultation document*, January 2015.
[79] When referring to 'self-regulation' in this report we mean initiatives by groups of businesses within an industry (including industry bodies, professional bodies and coalitions from industry) to modify their behaviour in order to improve quality standards (including, but not limited to the quality of the product or service itself, customer service, information provided and aftersales care). Self-regulatory initiatives may aim either to achieve compliance with consumer law or to go beyond what the law requires. Self-regulation is usually achieved through a set of rules (such as a code of practice), through voluntary standards, or through accreditation. It may also include arrangements for the provision of industry guidance material and for action to address particular compliance problems.
[80] OFT1115, *Policy statement: The role of self-regulation in the OFT's consumer protection work*, September 2009.
[81] We also identified self-regulation in particular sectors that address specific issues in data collection, storage and use, such as the BSI Kitemark for Secure Digital Transactions, which operates in the financial sector.

- Advertising Standards Authority (ASA) in relation to the Committee of Advertising Practice's (CAP's) mandatory UK Code of Non-broadcast Advertising, Sales Promotions and Direct Marketing (the CAP Code);[82]

- Interactive Advertising Bureau (IAB) in relation to its Framework for Online Behavioural Advertising (OBA), the European Interactive Digital Advertising Alliance (EDAA) 'trust seal' and 'AdChoices' icon;[83]

- Direct Marketing Association (DMA) in relation to its Code of Conduct (the DMA Code) and 'DataSeal';[84] and

- Market Research Society (MRS) and its Code of Practice (the MRS code) and 'Fair Data Mark'.[85]

2.133 The ASA is the UK's independent regulator for advertising across all media and plays an umbrella role. The ASA administers the CAP Code which, unlike the other codes, is mandatory (for all UK advertisers). The CAP committees are made up of representatives of advertisers, agencies, media owners and other industry groups.

2.134 In addition to the mandatory CAP Code, there are other voluntary codes such as the MRS Code and the DMA Code which reflect their specific areas within advertising, marketing and market research. The IAB Framework for OBA also regulates the collection and use of data for the purposes of OBA and these rules are incorporated into the UK CAP Code, with the ASA handling consumer complaints.

2.135 Self-regulatory initiatives tend to reflect some common principles, such as:

- consumer control and/or consent – consumers should be given the chance to exercise choice and either consent to or opt out of the collection and use of their data;[86]

- transparency – consumers should know about the collection and use of their data;[87]

---

[82] CAP, *The CAP Code - The UK Code of Non-broadcast Advertising, Sales Promotion and Direct Marketing*, Edition 12, September 2010.
[83] IAB, *IAB Europe EU Framework for Online Behavioural Advertising*, April 2011.
[84] DMA, *The DMA Code*, August 2014.
[85] MRS, *The MRS Code of Conduct*, September 2014.
[86] These have been taken from principles which are listed in the respective codes and where there are no principles listed, from the provisions themselves. In relation to consumer control and/or consent, see for example MRS code principle 1: 'Researchers shall ensure that participation in their activities is based on voluntary informed consent'.
[87] For example, DMA Code Desired Outcome: 'Customers always know who is collecting their data, why it is being collected and what it will be used for.'

- minimisation – only data needed for the purpose should be collected;[88] and

- data security – data should be held safely and securely.[89]

2.136 The initiatives themselves commonly consist of a code or framework of principles, as well as practical guidance to members, and various enforcement mechanisms when breached. Many include the provision of a trading seal or icon for complying members and some extend this to businesses that are independently verified according to a similar set of principles or requirements and pay a fee to display the seal or icon (see **Box 2.22**).

Box 2.22: Key self-regulation codes

ASA CAP Code

This sets out rules for all non-broadcast advertisements, sales promotions and direct marketing communications. Two sections are particularly relevant to consumer data:

- Section 10 is dedicated to database practices. It sets out 16 rules that relate only to databases used for direct marketing purposes.

- Appendix 3 is dedicated to the OBA rules and, amongst other things, sets out the following:

  - Those collecting and using data for OBA purposes must give notice that they are doing so on their website, and in or around the display advertisement delivered using OBA. The notice should be linked to a mechanism which allows the user to opt out of collection and use of web viewing behaviour data for OBA.

  - Those collecting and using data must obtain explicit consent from users before using technology to collect and use information about all, or substantially all, websites that are visited by users on a particular computer in order to deliver OBA to that computer.

[88] For example MRS Code, rule 33(f): 'Members must take reasonable steps to ensure all of the following…(f) that personal data collected are relevant and not excessive'.
[89] See for example IAB Framework for OBA principle 3:'Companies should maintain appropriate physical, electronic, and administrative safeguards to protect the data collected and used for Online Behavioural Advertising purposes,' and '…companies should retain data that is collected and used for Online Behavioural Advertising only for as long as necessary to fulfil a legitimate business need, or as required by law.'

IAB OBA Framework, 'AdChoices' and the 'EDAA trust seal'

The OBA Framework lays down a structure for codifying industry good practices and establishes principles intended to apply consumer friendly standards to OBA and the collection of online data in order to facilitate the delivery of advertising based on the preferences or interests of web users.

The Framework is based upon seven key principles: notice; user choice; data security; sensitive segmentation; education; compliance; and enforcement and review. The OBA rules were added to the CAP Code in February 2013, with the ASA handling consumer complaints.

EU businesses signed up to the IAB Framework can apply for an EDAA trust seal to demonstrate their compliance (which is independently verified by a third party auditor).

A key aspect of this initiative is the 'AdChoices' icon, which appears in or around advertisements on sites and on site pages themselves. If a user clicks on the icon they will be able to find out more about the information collected and used for this purpose and use a control mechanism to choose not to allow such data collection.

DMA Code and 'DataSeal'

The DMA Code is a principles-based code that seeks to achieve a standard of behaviour beyond what is required by legislation. It is supported by channel-specific guides.

The Code sets desired outcomes relevant to direct marketing services with the aims of raising standards industry wide, including:

- customers have a clear understanding of the value exchange;
- companies are upfront and clear about why they collect data and how they intend to use it;
- customers always know who is collecting their data, why and what it will be used for; and
- all customer data held by companies is accurate, up to date and not held longer than needed.

All DMA members have to comply with the DMA Code of Practice. The DMA also offers a 'DataSeal', which is an additional voluntary standard that members of any trade association in the advertising, marketing and communications sectors can apply for. While its Code focuses on data use and sharing, the DataSeal is about data security.

MRS Code and 'Fair Data Mark'

The Code is designed to support individuals and companies engaged in market, social or opinion research in maintaining professional standards and reassure the general public that research is carried out in a professional and ethical manner.

It sets out overarching ethical principles supported by rules of conduct which prescribe how members collect and use consumers' data. Among other things, these require researchers to obtain voluntary informed consent, and to be straightforward, honest and transparent as to the subject and purpose of data collection.

A broader range of firms are also able to sign up to the MRS Fair Data Mark which is a recognisable mark to show that accredited organisations can be trusted to use personal data in an ethical way.

3. Consumer data, markets and competition

Introduction

3.1 The growth in the collection and use of consumer data has created new opportunities for firms to develop and amend existing products and services. As a result there is an ongoing debate about how data is affecting competition. In this chapter, we describe the issues that have been raised and set out our emerging thinking.

3.2 The main issues that we consider are:

(a) whether consumer data and markets that include consumer data differ from other markets across the economy; and

(b) how the collection and use of consumer data may generate competition concerns.[90]

3.3 In our CFI, we sought information about competition issues across any markets that use consumer data. Because the project was broad in scope, we received high level information and we have not sought to draw detailed conclusions about competition in specific markets. Rather, we have used the evidence received to consider how economic theory applies to consumer data and data markets in order to develop our understanding and reach high-level conclusions.

3.4 In this chapter we discuss the characteristics of consumer data (**Section A**); we describe the different markets where data is used (**Section B**); and we set out the evidence we have received in the CFI on the way these markets are operating (**Section C**). These three sections examine the extent to which data, data markets,[91] and competition in these markets may be different from other markets in the economy, with the intention of reaching a preliminary view on whether the competition tools available to the CMA are sufficient to address any competition concerns that may arise. The question of whether existing competition rules are sufficient to examine concerns in consumer

[90] We refer in this chapter to 'competition concerns' as conduct that may amount to an abuse of a dominant position under Chapter II of the Competition Act 1998 and/or Article 102 of the Treaty on the Functioning of the EU, and/or that may amount to a feature of a market which, alone or in combination with other features, prevents, restricts or distorts competition in connection with the supply or acquisition of goods or services in the UK, or any part of the UK within the meaning of sections 131 and 134 of the Enterprise Act 2002.
[91] We note that we have not reached formal conclusions in this report concerning how any particular market would be defined in the circumstances of any future potential investigation by the CMA under the Competition Act 1998 or the Enterprise Act 2002. Accordingly, we refer in this chapter to 'data markets' and 'intermediary markets' for convenience only.

data markets has been mentioned by a number of stakeholders as part of discussions related to the Digital Single Market.

3.5 We conclude this chapter by suggesting four indicators that could be used to assess the likelihood that a particular data market may generate competition concerns in practice (**Section D**).

Section A: The characteristics of consumer data

3.6 There are a number of characteristics of consumer data that differentiate it from many other goods and services in the economy. In this section, we outline some of the main characteristics and consider the likely implications for competition:

(a) **Simultaneous use** – the same consumer data may be used by more than one person at the same time. In economic terms the use of consumers' data is non-rivalrous. For example, consumers' browsing history can be collected by a number of different cookies and used by collectors simultaneously. However, restrictions can be placed on access to consumer data, for example through contractual conditions. This implies that efficient markets may involve sharing data beyond those involved in the initial transaction to minimise the costs in multiple firms collecting, storing and processing the same data multiple times. It also means that failing to share, sell or license consumer data may, in addition to the potential to generate competition concerns, be a further source of inefficiency in data markets, leading to increased costs for consumers and firms.

(b) **Cost structure** – the collection, storage, processing and analysis of consumer data is likely to involve relatively substantial fixed costs and low or negligible marginal costs. In markets with this structure, economies of scale and scope are common. This means that larger firms are likely to have cost advantages over smaller firms in collecting, storing and processing more and different types of data. These advantages can act as barriers to entry and expansion in markets, particularly where they are significant and where data is a key input into the products and services being developed. This suggests that some markets where data is important may be more likely than others to experience higher levels of concentration and so potentially lower levels of competition.

(c) **Diversity in value** – there is significant diversity in the types of consumer data collected and used. Some types of data (such as name or date of birth) will have enduring value and as such only need to be collected once by a specific firm. Other types of data (such as the particular products a

consumer has been searching for) will be more transient in value, being relevant over a shorter period of time. The extent to which data holds its value over time may impact on the extent to which it is sold and the availability of alternatives sources and may therefore be a relevant factor to consider in assessing whether competition concerns may arise.

Section B: The nature of consumer data markets

3.7 In **Chapter 2**, we describe a variety of ways in which consumer data is used and a wide range of different types of market that have developed to use it. In this section we describe, at a high-level, the broad types of market structures that have developed.

3.8 One characteristic of data markets, which is common across many different sectors, is the speed with which the products and services offered in these markets, as well as the firms in them, can change. This is driven by the growth in the collection and availability of consumer data, together with increased processing power allowing for new and more sophisticated uses of consumer data to arise, as discussed in **Chapter 2**.

3.9 The broad categories of markets that use consumer data are:

- **markets in which data is collected directly from consumers** – for example, social media websites or loyalty schemes. In some cases, this can involve transactions with payment, while in others, consumer data may be transferred to firms in return for the provision of a service without an explicit, upfront or transparent transaction and associated payment;

- **intermediary markets** in which a variety of firms buy and sell consumer data and use other sources of data to gain insights about a range of different consumers. There are a wide range of data intermediaries involved in activities including, for example, the supply of online targeted advertising. These firms do not generally have a direct relationship with the consumer; and

- **personal information management firms** that seek to act as agents of consumers in holding data and allowing consumers to control which firms are able to gain access.

3.10 Each of these have different characteristics which we explore, together with the implications for competition below.

Markets in which data is collected directly from consumers

3.11 Within this category of markets are three sub-categories of data markets in which firms seek data directly about consumers, based on the nature of the interaction between consumers and firms:

(a) **Consumer data can be collected as part of a transaction between the consumer and firm**. For example, when purchasing a product and making the associated payment from an online seller, firms will typically collect information about the consumer to enable them to fulfil orders (for example to take payment and deliver the item) and to understand more about their customers.

(b) **Consumers make use of an online service, for which there is no transparent and upfront charge, but where the collection and use of consumer data is a key source of revenue for the firm** – typically through presenting targeted advertising to users. For example, many social media websites have a business model of this type.

(c) **A variant of the two models above** involving limited access without charge and some specific charges for certain areas of the service such as premium content, or where usage of the service exceeds a certain volume.

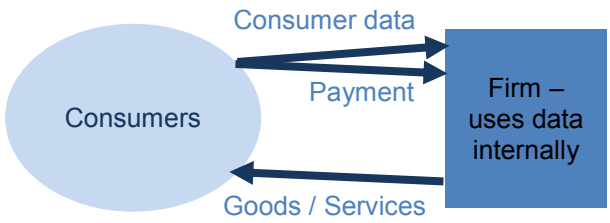
3.12 The key characteristics of these business models are explored further below.

Consumer data collected as part of a transaction between the consumer and firm

3.13 There are two main ways in which firms seek to use the consumer data they collect. In **Figure 3.1** below, the firm in question collects consumer data purely for its own use, and does not share this further.

3.14 The consumer data collected can allow, for example, a retailer to understand and monitor the purchases of its customers, enabling it to cross-sell other products from its range and offer benefits like price reductions or add-on services that are targeted at the customer's particular needs or interests. The data can also be used to understand the nature of demand for products, giving the firm useful information for developing existing or innovative new products. This type of use, in a competitive market, can generate efficiencies with consumers benefitting from lower priced or higher quality products and services than would be the case if no data was collected.

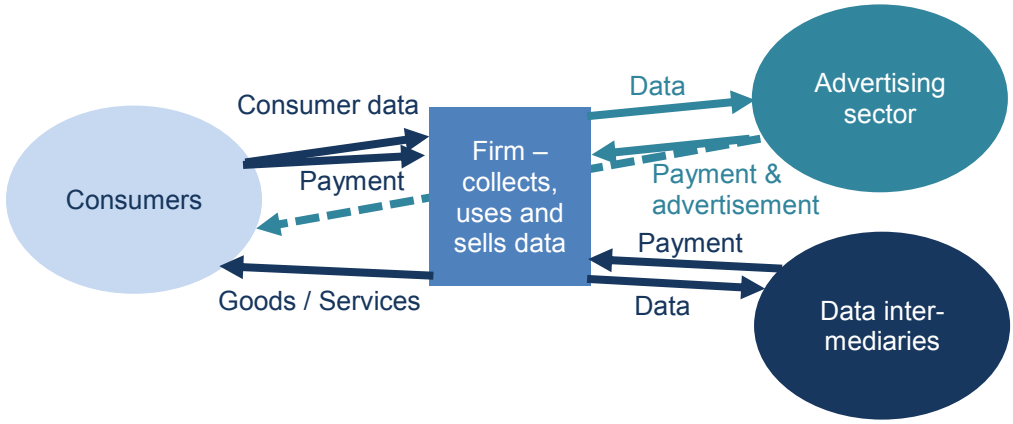
Figure 3.1: Transactions where consumer data is used internally



Source: CMA.

3.15 **Figure 3.2** below shows the case where at least some data is passed on to other businesses for example, to give an advertising firm enough information about a particular consumer's attributes to allow a targeted advertisement to be served. Firms in this position have more than one separate group of customers and are typically referred to as multi-sided platforms. A firm with consumers and advertisers as sources of revenue, for example, would be a two-sided platform, as it interacts with these two groups of customers.

Figure 3.2: Transactions where consumer data is re-used



Source: CMA.
Note: This diagram does not seek to model accurately the complexities in the advertising or other data intermediary sectors, but shows the basic interactions with the two-sided platform.

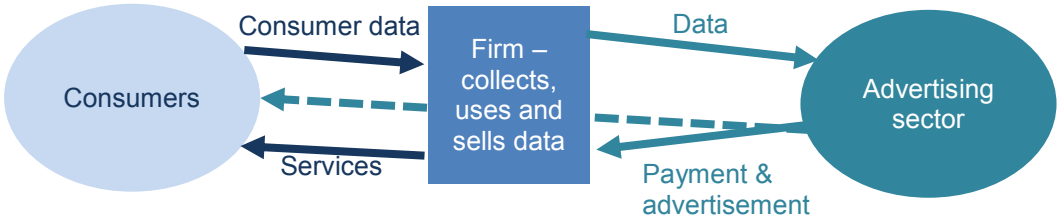
3.16 Because two-sided platforms have more than one potential source of revenue, consumers may benefit from the re-use of their data in advertising through paying lower prices for the products and services purchased. The extent of these benefits will depend on the willingness of both consumers and advertisers to pay the platform.[92]

[92] Willingness of consumers and advertisers to pay will depend on the value advertisers attribute to consumers, and the value that consumers derive from advertisements.

Collection of data in relation to a service with no transparent and upfront charge

3.17 There are a number of online firms that provide services to consumers without an explicit and transparent up-front charge. In order to fund these services, firms typically generate revenue from the data collected from consumers. One of the more common ways to generate this revenue is by using data to target particular advertisements for consumers on the pages they view. This is illustrated in **Figure 3.3** below:

Figure 3.3: Collection of data in the provision of services without charge



Source: CMA.

3.18 While this is similar to the structures discussed above, in **Chapter 4** we discuss the evidence on consumer attitudes to this business model, including levels of awareness that they are paying an implicit price for the service by providing data which is used for targeted advertisements. We also discuss their attitudes to replacing this form of transaction with one where they pay an explicit charge.

3.19 In these markets, firms collect data directly from consumers, and therefore, in theory at least, consumers should be able to discipline providers over the level of privacy or the extent to which their data is used. However, in practice, consumers in these markets may find it difficult to assess whether they are engaging in a beneficial transaction with a firm when sharing data because:

- some consumers may be unaware of the value of their data to firms;[93] and
- the collection of data online is relatively routine and so consumers may be unaware of the different uses to which this data is put and whether it is part of the payment for a service or not.

3.20 One implication of this is that, without knowing the value of the data they are sharing and how much of their data is being used, consumers are unable to understand the price for the data-funded transactions they engage in. This may mean that firms have limited incentives to compete over the privacy

[93] This means it would be difficult for those consumers to understand how much data needs to be provided and used to fund services either completely or on a partial payment basis.

protection they afford to consumer data, that is the minimum amount of data they need to collect to generate sufficient revenue to fund the service to consumers. Concerns about how consumers can control the data they share with firms and the terms under which they do so are considered further in **Chapter 4**.

3.21 Some stakeholders consider that privacy is a new non-price variable over which firms can compete.[94] The presence of competition over privacy is a useful indicator, not only of firms' willingness to adapt to consumers' desires, but also consumers' understanding of the use of their data in that market, and the effectiveness of competition in the market in question.

3.22 There are a number of positive developments with some examples in practice of firms developing improved consent mechanisms. These are discussed in more detail in **Chapter 4,** specifically in relation to graduated consent notices for cookies. However, the extent to which such developments are driven by the competitive process remains unclear.

Competition and concentration in two-sided markets

3.23 Two-sided markets can be complex, with linkages between customers on each side of the platform, or firm, meaning demand among one group of customers is related to that among customers on the other side. These linkages, where one user of a good or service has an impact on the value of that product or service to other people are referred to as network effects or network externalities in economic theory.

3.24 Two-sided markets, as with other markets with network effects, often have high levels of concentration, as customers gravitate toward companies that already have large numbers of customers. Two-sided data markets may therefore feature large firms holding a position of market power. In some cases this may arise where one firm is an early innovator and builds up a strong market position on the basis of a first mover advantage. In other cases, there may be intense competition between a number of firms initially, as they vie to become established as preferred network.

3.25 Competition and innovation in some data-rich two-sided markets can involve new developments that offer more functionality or a better service than that previously available. In this way, an innovative new provider can seek to overcome the difficulties of market entry and attract enough users and advertisers to make their platform operate effectively. Examples include the

[94] The Federal Trade Commission (FTC) recognised that privacy can be a competitive variable in its statement regarding Google/DoubleClick (FTC 071-0170) 20 December 2007.

development of Facebook gaining the previous customers of a similar service Myspace, and the entry of Google's search engine compared to the established rivals at the time.

3.26 Analysing the competitive constraints in two-sided markets can be challenging. However the concept of two-sided markets is not exclusive to consumer data or online markets. Competition in two-sided markets has been considered in depth in a number of competition investigations in the past, including, for example in markets involving payment cards.

Businesses that combine partial payment and use of consumer data

3.27 There are a number of firms that use a combination of the models above for their business activities. For example, the online versions of some newspapers provide limited content without direct charge, funding this through advertising (which may or may not be targeted at individual consumers) and charging consumers directly for either reading more than a certain number of articles, or to access full length articles and some additional premium content. Since the key characteristics of each part of this are examined above, we do not analyse this business model separately.

Intermediary markets involving consumer data

3.28 We describe how intermediary markets are working in **Chapter 2**. The role that intermediaries are playing is also described in work Analysys Mason carried out for Ofcom and is developed further in the DotEcon research.[95] The concept of a data intermediary is relatively broad and can encompass a number of different roles, which can include the following:

- **A focus on collecting data** from a variety of sources, including direct collection, using cookies for example, or the purchase of data that others have collected.
- **Data storage and basic processing** firms can provide specific facilities in which to store data collected by their clients and undertake basic processing to ensure this data is made available in a usable format.
- **Data analysis** firms can focus on the specialist skills involved in analysing different data sets, including combining data from different sources and generating valuable insights from it for their clients.[96] Consumer-facing

[95] Analysys Mason, *Report for Ofcom – Online data economy value chain*, February 2014. The work carried out by the FTC on data brokers describes in detail the way that these markets in the context of the USA.
[96] See, for example: Analysys Mason, *Report for Ofcom – Online data economy value chain*, February 2014.

firms may seek to use the skills and experience of this type of intermediary where they lack such skills themselves.

3.29 The approach taken by different data intermediaries to the collection of data, whether done directly, through a contract with a consumer-facing firm, or though purchasing consumer data, may depend on a number of factors including:

- the nature of the data sought – the more sensitive the type of data the less likely it is to be available from an intermediary;
- whether the firm has an existing customer-base – that could provide the data directly; and
- the cost of collecting consumer data – compared to the cost of purchasing this.

3.30 In general we expect these activities and the firms carrying them out to be less visible to consumers than markets in which consumers interact directly with firms. One exception to this may be credit reference agencies such as Experian, Equifax and Callcredit, which are firms with which some consumers may have direct contact, or be aware of some of the services they provide.

3.31 While many of the larger firms that interact directly with consumers have established brand names that are well-known, understood and trusted, this is less likely to be the case for data intermediaries. In theory, without such direct contact with consumers, these intermediaries would not have the same incentives to protect consumer data and may have greater incentives to sell and use the data to the fullest extent possible, with less chance of consumers seeking to discipline their actions.[97] However, we have been told that when firms with a direct relationship with consumers contract with data intermediaries, they can include terms in contracts to incentivise intermediaries to protect the data shared with them. Whether this resolves the issue entirely, or merely mitigates its effect would depend on the nature of the contract and the implications of any breaches for the intermediaries.

3.32 The Analysys Mason report suggests that there are a number of data intermediaries and the sale and purchase of consumer data is an active area of business. We received evidence in the CFI that there have been a number

[97] Data intermediaries using consumer data would however be subject to regulatory restrictions as set out in **Chapter 2** and discussed further in **Chapter 5**.

of acquisitions in this sector, but we have not sought, as part of this CFI, to assess the level of competition faced by data intermediaries.[98]

Personal information management services

3.33 Personal information management services (PIMS) act as intermediaries for consumer data between consumers and firms. The rationale behind these services is that it can be cheaper for one intermediary to hold data on consumers than for multiple firms to seek to collect this and hold it separately and for consumers to have to provide this on multiple occasions, as set out in Section A above. Respondents to the CFI noted that it may be easier for consumers to exercise control over the accuracy of their data, and choose which firms are able to have access to and use it.

3.34 The presence of this type of intermediary may, in theory, also allow consumers to auction their data to firms and receive compensation directly, although in practice it may be some time before this becomes a reality for many people. Consequently, the use of these services may allow for both savings to firms and benefits to consumers.

3.35 Although there are a number of providers of these services in the UK, usage is currently limited. There may be a number of reasons for this, including the following:

- **The two-sided nature of PIMS makes growth challenging** – the value of PIMS for consumers is dependent on the number of firms that make use of the data provided, and similarly, the value for firms is dependent on the number of consumers that provide data. In markets with such characteristics, it can take time for a new service to grow and replace a different way of holding data, as consumers and firms may take time to realise the potential benefit from the service. This may be linked with the growth and establishment of larger firms in the sector.

- **The risk-averse nature of consumers and trust in suppliers** – consumers are likely to be relatively risk-averse in seeking to supply their data to a new intermediary, as they would want to be sure that such firms protect their data appropriately. Establishing a reputation for trust in any market can be difficult, so new brands that are unknown to consumers

[98] In order to understand more about the potential incentives of data intermediaries, and whether, in theory, competition among these firms may work in a similar way to that in other markets that do not involve consumer data, we commissioned research from Alexandre de Cornière, from the Department of Economics and Nuffield College, Oxford University. His working paper is available at this link.

may take many months or years to gain the trust of a large number of consumers.

- **Lack of engagement with firms** – some stakeholders told us that the lack of growth was due to firms not seeking to use PIMS, and therefore, with few firms signed up, the benefit and incentives for consumers to join would be low.

- **The benefit of common standards of data holding and transmission** – having successful PIMS relies on firms being willing to accept and transfer data in a standard way when interacting with PIMS firms. Without clear standards over the way in which data is transferred and used, such services may find it challenging to integrate with a significant number of firms that, at present, have control over how, and in what format, the data is stored.

- **Whether PIMS are necessary to resolve existing concerns** – we heard from some stakeholders that the lack of growth in PIMS may be due to a lack of sufficient consumers perceiving a need for it. They said that PIMS might be a proportionate solution in the event of more systematic and wide-scale exploitation of consumers' data, but that they were not currently perceived to be necessary. Others suggested that consumers were not willing to engage with these services and were not willing, in the main, to take on the role of being their own data controller.

3.36 This sector could represent an interesting way in which consumer data collection and use could be structured. We consider that its growth in the future is likely to depend on the extent of concerns among consumers and the willingness of both firms and consumers to consider the benefits of using these services.

Section C: Evidence on competition concerns

3.37 In this section we review the evidence that we received from the CFI on these markets before drawing some conclusions about this evidence in Section D.

3.38 We note that data markets are fast moving and can evolve quickly. As a result, while we cover both static and dynamic competition in the section that follows, we devote significant attention to dynamic competition issues such as barriers to entry and exclusion.

3.39 The main issues that we considered in the CFI were as follows:

- Whether there are **barriers to entry and expansion in data markets** such that entry and expansion in these markets may be challenging, reducing the competitive discipline on incumbent firms over time. This may make new firms less likely to consider entry, even where they might be able to offer a better product or service to the incumbents.

- Whether **data collection or holding gives rise to or exacerbates market power** such that consumers may suffer from higher prices or lower quality products and services than may be expected in a competitive market.

- Whether the collection of a broad range of data about consumers can give some firms the ability to **leverage market power** from one market into a separate but related market.

- The use of consumer data to **exploit at least some consumers either through charging them different prices, or altering other product characteristics** with the intention of gaining increased profitability.

Barriers to entry and expansion in data markets

3.40 Barriers to entry and expansion may affect competition in the long term, restricting the growth of smaller firms and the entry of new firms. These potential barriers fall within the following categories:

(a) **Structural barriers** – arise from basic industry conditions, such as the structure and costs of production including the potential for economies of scale[99] and scope,[100] the technology used or other similar factors needed to become established in a market. The impact of these costs may be more significant where they are not recoverable on exit (sunk costs).

(b) **Strategic barriers** – where incumbent firms intentionally create or enhance the advantages they have over new or smaller rivals from their established position. This can arise from brand and reputation, experience, first-mover advantages, pricing strategies and the presence of network externalities.

[99] The cost advantages that firms obtain from the size, output, or scale of their operations. The cost of production typically decreases with increasing scale as fixed costs are spread over increased volume of output.
[100] The cost advantage that arises from firms undertaking a range of activities, where the average cost across the range of activities falls as volume of output increases.

(c) **Absolute barriers** – these include legal barriers and technical advantages including preferential access to intellectual property.

Structural barriers

3.41 As discussed above, one of the properties of collecting, storing, and analysing consumer data is that the costs are typically mostly fixed, with low marginal costs of increased consumption, collection, storage and analysis. This gives rise to the presence of economies of scale and scope in these activities.

3.42 The issue of economies of scale and scope were mentioned both explicitly and implicitly in a number of responses as barriers to entry and expansion. However, we did not receive much detail on the nature of investments needed to enter these markets, so it is difficult to conclude on the likely extent to which the fixed costs in data markets may be sunk, and therefore the extent to which they are likely to raise entry barriers is likely to vary across markets.

3.43 One respondent noted that in relation to storage, the costs of cloud storage for data would not discriminate against smaller firms, and we note that this may help alleviate concerns around economies of scale in some areas. Another respondent thought that economies of scale were more of a concern, having focused on the significant scale of data to which small or new firms would need to gain access in order to be able to compete effectively with large incumbents in some key online markets.

3.44 Another respondent focused on the challenge in collecting data across a number of linked but separate markets in order to compete effectively with incumbent firms in some cases due to economies of scope.

3.45 We note that barriers to entry and expansion may be more significant in two-sided markets, specifically, in those two-sided markets where consumers only use one provider in the market (single-homing). This is because of the difficulty, in such markets, for small and new firms to gain sufficient numbers of customers on both sides of a two-sided platform, due to both customers and sellers being attracted to the largest network. Where consumers do not single-home, it is less likely that a two-sided market would have an impact on barriers to entry and expansion.

Strategic barriers

3.46 One important potential barrier relevant to consumer data is first-mover advantage, which in data markets may be related to issues around trust, reputation and brand recognition. While online markets are relatively new compared to many other markets, some online firms have been in existence

for a number of years and are used regularly by a significant number of consumers so have developed strong brands and reputations.

3.47 We note that research by the Direct Marketing Association in 2012 showed that trust in a brand was one of the top three factors stated by over half of survey respondents to make them most willing to share personal information.[101] These factors may, in some data markets, represent barriers to entry and expansion. In particular, we consider above that the lack of brand and reputation in the PIMS sector may be one reason that the sector is currently relatively small in the UK. Despite the importance of trust indicated by this research, we received no direct evidence from respondents to the CFI concerning the brand and reputation of firms using consumer data.

3.48 In theory, pricing strategies of incumbent firms could be barriers to entry and expansion where these are difficult or excessively costly for small or new firms to replicate. Such strategies may include discriminatory pricing, where a firm uses consumer data to separate different groups of customers and offers a different price to each group.[102] Small or new firms would not have a substantial fixed base of existing customers, and so may be unable to compete as successfully to target customers through offering them lower prices. We received no direct evidence in the CFI on the use of pricing, or more specifically, discriminatory pricing, as a barrier to entry.

3.49 Beyond pricing strategies by incumbent firms to seek to make entry and expansion more difficult, the decision on whether to allow consumer data to be sold and used by others may also be a strategic choice by firms that could represent a barrier to entry or expansion where that data is valuable to the production process and where there are few substitutes available. One respondent mentioned a concern arising from the lack of a standard format for storing and sharing consumer data. This was because there was a possibility of firms changing the data supply interface or changing the format of it and generating costs for smaller rivals.

3.50 Where consumer data is particularly important for the production of a good or service, incumbent firms may decide to allow other firms, including data intermediaries and rivals access to the data and benefit from the fees charged for this access.[103] Alternatively, firms may choose to restrict access to the consumer data they collect and use it internally, with the potential for this to give it better products or services and a competitive advantage over rivals.

---

[101] Direct Marketing Association (DMA), *Data Privacy: What the consumer really thinks*, June 2012.
[102] Firms need at least some degree of market power to be able to separate consumers and discriminate in this way.
[103] Subject to consumers' consent for such use.

3.51 We received a number of comments from firms that did not have access to consumers to collect data directly themselves, and commented that a lack of access to data at a particular scale, or of sufficient breadth to equal that of an incumbent was a barrier. Respondents' comments related to a variety of markets including online search, advertising and marketing. One respondent noted that the challenges posed by a lack of access to data were magnified by the two-sided nature of the markets and the presence of large established firms.

3.52 Another stakeholder noted that a lack of access to data can also impede intermediary markets and choice tools including price comparison sites. Another noted that a lack of access to data was creating barriers for small firms that are seeking to give consumers greater control and visibility of their data.

3.53 However, views from respondents differed across the various markets in which data is used. Some noted that there were instances where a lack of access to data would not be a barrier, as in areas such as direct marketing, where new firms could contact potential customers directly to tell them about a new product or service and seek information related to it. Others noted that those firms without direct access to data could, in some cases, purchase relevant data from intermediaries to overcome the lack of a database of customers and still understand the likely profile and preferences of their target customers.

Absolute barriers

3.54 While there are relatively few absolute barriers in data markets, all firms that collect, purchase, store or use consumer data need to comply with the relevant data protection requirements.[104] Meeting these requirements will involve a cost for all firms. Such regulations are designed to protect consumers' interests and the presence of such regulation and its enforcement aims to ensure the data that is collected about consumers is protected and used appropriately, avoiding consumer detriment and misuse of data. In addition, this regulatory regime is intended to be a disincentive to firms with no intention of safeguarding consumer data or complying with such regulations from entering the market.

3.55 There could be a concern that the financial burden imposed on small or new firms as a result of complying with these regulations might discourage them from entering the market, reducing the competitive constraint and limiting the

[104] The details of these regulatory requirements are explored in **Chapters 2 and 5**.

potential for innovative new products and services. We received a small number of comments at a high level about the cost of complying with regulatory requirements.

Market power and restricting access to consumer data

3.56 We consider that restrictions in the access to consumer data, particularly where data is an important input in the production of a good or service, have the scope to generate barriers to entry and can in some cases lead to the creation of a position of market power, or can exacerbate an already existing position of market power.[105] In addition, the two-sided nature of some data markets can increase concentration. This arises as consumers and firms see greater value and are attracted to platforms with the greatest number of users on both sides of the platform.

3.57 Consumer data could be an important input into some goods and services as discussed in the section on barriers to entry above. Control of that input may confer market power as it places the holder in a strong bargaining position relative to those that require access to the input. A number of respondents to the CFI highlighted market power as a potential concern, for example, noting that a firm might be able to foreclose rivals by cutting off access to vital data. However, respondents did not provide specific examples of market power in practice, other than referring to the EC's ongoing investigations into Google described below.

Ability to exploit a position of market power

3.58 We considered that in the following circumstances, firms may be able to exploit market power as a result of having access to important consumer data that others do not have:

- where other firms do not possess and cannot freely and easily access the data, which means it cannot be substituted for or collected or purchased elsewhere; and
- where the data has considerable value in the process of making a product or offering a service, such that an attempt to make the product or offer a service without the data results in an inferior product or service, or this production is not possible absent the data.

[105] Where a firm has a position of market power, it may be in a dominant position. The abuse of a dominant position is a breach of Chapter II of the CA98, or Article 102 TFEU.

3.59 We note the European Commission's ongoing investigations into Google for alleged breaches of a dominant position under Article 102 TFEU. These cases illustrate the kinds of conduct being pursued in data markets. The investigations are described in **Box 3.1** below.

Box 3.1: European Commission antitrust cases against Google

On 30 November 2010, the Commission announced it had launched an investigation into allegations that Google had abused a dominant position in online search, in violation of Article 102 TFEU. This followed complaints by search service providers about unfavourable treatment of their services in Google's unpaid and sponsored search results coupled with an alleged preferential placement of Google's own services.

On 15 April 2015, the Commission sent a Statement of Objections to Google alleging the company has abused a dominant position in providing general online search services in the European Economic Area (EEA) by systematically favouring its own comparison shopping product which artificially diverts traffic from rival comparison shopping services and hinders their ability to compete. The Commission's preliminary view is that Google's conduct infringes Article 102 TFEU because it operates to the detriment of competing comparison shopping services, and consumers, and also stifles innovation.

In addition, on 15 April 2015, the Commission formally opened a separate investigation into Google's conduct with regard to its mobile operating system, Android. This investigation is focussed on whether Google entered into anti-competitive agreements and/or abused a possible dominant position by hindering the development and market access of rival mobile operating systems, mobile communication applications and services in the EEA.

Leveraging market power

3.60 Firms that have market power in one market may seek to leverage that market power into another related market. This type of behaviour is often described in terms of bundling and tying, where a firm ties or bundles a good or service sold in a market with a good or service sold in a related market.

3.61 For example, a large firm with market power gained from the creation of a valuable dataset may seek to enter the market for data analytics by tying the purchase of its dataset with the use of its analytics service. We note that in some cases, this bundling or tying may bring efficiency benefits to firms and consumers. However, in other circumstances it could give rise to harm to competition where it has the potential to foreclose rival firms within the more competitive market or where it removes the incentives for new firms to enter the market (as they cannot compete without providing the full range of services provided by the firm with market power). One respondent noted that

data was a significant potential source of power in some online areas and the data collected from some online services could be used to expand the service offered into other linked markets.

Consumer data and discrimination

3.62 This section explores the ways in which firms may seek to use consumer data to discriminate between consumers either individually or as groups. This discrimination can take place using a variety of different competitive variables, but the most common examples are price or quality based discrimination, where consumers, either individually, or as a group are offered different prices for the same product (or where consumers are charged the same price for different levels of quality) based on firms' assessments of their willingness to pay for the product or service. **Chapter 4** describes other ways in which consumer data may be used to discriminate between consumers.

3.63 The outcome of price discrimination is not always clear. In some cases, it can be used to increase the number of consumers using a service, by offering those with a low willingness to pay a lower price, and may therefore have a positive effect on welfare overall. However, in other cases, it could be used to exploit a position of market power to the detriment of consumers. In addition, even where the overall effect on consumer welfare is positive, there may be occasions when harm is caused to vulnerable groups of consumers, and this may represent a concern.

Box 3.2: OFT's call for information on personalised pricing

In 2012, the OFT considered the practice of personalised pricing, which is a form of price discrimination. The OFT found that personalised pricing was technically possible but that firms did not appear to be using information about individuals to set higher prices to them. The OFT reported that firms were offering personalised discounts, and increasingly using information collected about consumers in order to refine their pricing strategies.

The OFT found that, based on economic theory, online price discrimination is more likely to be harmful when:

- it is carried out by a monopolist;
- the form of price discrimination is very complex and/or consumers are not aware of it;
- it is costly for firms to implement and so it pushes up costs; and
- it leads to a fall in consumers' trust in online markets.

Evidence of price differences across consumers in the CFI

3.64 There are a number of examples of consumers being offered different prices that are not in practice price discrimination. The first of these is risk-based-pricing. This is where consumers face a price based on their consumer data. This differs from discrimination, as the data is not typically used to estimate the costs involved in providing the service to them. Such pricing is common-place in a number of insurance and financial services markets, where consumer data has been used for many years to estimate the risk of default on a loan, or the risk of a claim being made on an insurance policy. The use of consumer data in this way can generate a number of benefits, including providing firms with greater information revealing the characteristics and risks taken by consumers. This additional information may help to alleviate problems of adverse selection in insurance markets and allow insurers to price their products more accurately.

3.65 One example is the use of in-car telematics devices, which are black boxes installed in consumers' vehicles and are used to record a number of metrics on a consumers' driving. This data, when analysed can generate better information on the risk an individual customer poses and can be used to offer a more personalised insurance quotation. Further details on the use of consumer data in insurance can be found in the DotEcon research covering motor insurance.

3.66 The second example is that there are a significant number of firms that use consumer data about, for example, previous purchases, or items that consumers search for to provide them with a number of targeted discounts on products likely to be of interest to them. In this way, certain consumers receive targeted offers of lower prices on a number of items. Such pricing practices have been used in loyalty schemes and by a number of online retailers in an attempt to increase sales and loyalty among consumers. While this is a form of price discrimination, and we have received evidence regarding its use, we have not examined the impact on consumers compared to a situation where a uniform price was offered.

3.67 While the opportunity for consumers to benefit from the availability of offers is acknowledged, some respondents have raised concerns. In particular, one respondent considered that the increased use of offers and promotions targeted at consumers may have the long term effect that consumers would have less visibility or knowledge of the going rate for a particular good or service.

3.68 In addition, another respondent has stated that while there are significant benefits for consumers from personalised offers, these may adversely impact

some vulnerable groups of consumers, in the event they suffer some form of exploitation.

3.69 While respondents informed us of instances of these pricing practices being used, we did not receive a clear indication of examples where price discrimination using consumer data was being used to the likely detriment of consumers.

3.70 There may be reasons why price discrimination is not seen widely in practice. Firms may be wary of damaging their reputation or brand value by being seen to do this. Consumers would be likely to respond negatively if it became apparent that firms were engaging in this practice. We did not receive evidence on this from the CFI, but the OFT's personalised pricing report provided an example of the negative reaction by consumers of being charged different prices by Amazon, depending on whether they were new or returning customers.[106]

Other types of discrimination

3.71 Firms could also seek to discriminate between customers using competitive variables other than price including changes to the quality of an existing product or service, or producing a number of similar products but with differing quality. In this way, a firm may increase the profit it is able to extract from a set group of consumers.

3.72 The practice of varying quality of service is relatively common and, in many cases, consumers will be able to self-select the price and quality of service bundle that is most appropriate for their needs.[107] Beyond this, the collection of consumer data may enable firms to make judgements about the lowest level of quality needed by consumers/groups of similar consumers. This may enable a firm to engage in quality discrimination where quality differences are not reflected in the prices of goods or services. Firms may do this by restricting the products that are displayed to consumers or by varying the order in which products are listed on their website to display relatively poorer or better quality products first depending on the information they collect about consumers. This raises the possibility of some consumers being exploited

---

[106] BBC, *Amazon's old customers 'pay more'*, 8 September 2000. Consumers found that they were able to obtain cheaper prices for certain DVDs by posing as new customers rather than returning customers. However, Amazon stated at the time that it was carrying out a test and that prices were assigned randomly. The BBC news article reports that consumers had branded the pricing behaviour as unethical and sneaky.

[107] A typical example is that of printers, where a firm offers printers of varying quality (such as speed of printing and the double-sided printing functionality) and consumers select a quality and price level bundle that suits their needs. Similarly, cameras are available with varying picture quality, which enables consumers to select the product that best suits their needs.

with low quality products that are sold at the same price as higher quality products.

Section D: Conclusions

3.73 We have identified a number of important characteristics of consumer data and data markets which may differ to other markets:

- While consumer data can be used simultaneously, firms can be prevented from using it through licences and other controls. This gives rise to a risk of exclusionary behaviour by firms' preventing access to and use of data at reasonable prices.
- The cost structure of the collection, storage and processing of consumer data can generate economies of scope and scale. This can generate barriers to entry and expansion, leading to data markets having fewer and larger firms than would otherwise be the case.
- A number of data markets are two-sided which can lead to these markets having fewer and larger firms and can also generate barriers to entry. This could arise where links between the two sides of the market are strong, and particularly in cases where consumers do not use multiple providers.
- Given the relatively fast evolution of data markets, competition assessments should examine both the level of competition prevailing at the time of assessment and the likely ways in which the market may evolve.

3.74 We received mixed evidence about barriers to entry across a range of data markets. However, where concerns were raised, the most common concern was whether firms could gain access to consumer data, and the difficulties experienced by small and potential new entrants in some markets that arise from the economies of scale and scope.

3.75 Respondents raised concerns about the potential for consumer data to be used to generate or exacerbate market power in a single market, or being used as a source of power that could be leveraged into a related market. We have not received evidence in the CFI that indicates an abuse of dominance in breach of Chapter II of the CA98 and/or Article 102 TFEU has been, or is being committed.

3.76 We also considered whether consumer data might be used by firms to discriminate between consumers in a way which would be detrimental to at least a proportion of them. While we received evidence of instances of

targeted price discounts, for example in loyalty schemes in grocery retailing, we did not receive evidence of consumers suffering detriment from such practices.

3.77 Given the number of different types of markets using consumer data and the variation in the use of data within these markets, we would need to understand the specifics of the market or markets in order to reach a view on whether the collection and use of consumer data is beneficial for competition or more likely to be damaging.

3.78 However, we have identified a number of market indicators that suggest a greater likelihood of competition concerns:

- **Markets in which data is a significant input into products and services produced**. The ability and incentives to exclude competitors by denying access to data, and/or the barriers to entry arising from consumer data, will be stronger where the data is a significant input into the quality or other attributes of a product or service. Concerns related to possible leverage of market power may arise where consumer data obtained in one market is a significant input to products and services produced in a related but separate market.

- **Markets where there are few substitutes for the data collected by firms**. Firms are more likely to be able to exclude competitors by either preventing or restricting access to and to use of consumer data where there are few or no substitutes for this data.

- **Firms with existing market power that control the collection of consumer data in a market**. Where a firm or firms in a market already have a position of market power, their ability and incentives to exploit further power over the collection of consumer data may be stronger.[108]

- **Markets in which firms do not compete openly over data privacy and transparency of their uses of consumer data**. An absence of competition over privacy may indicate data markets failing to deliver what consumers want. This may occur where the implicit price of data used by firms is unclear, and where consumers are unable or unwilling to drive competition and incentivise firms to consider and improve the degree to which consumers' privacy is protected.

[108] We note that a firm must be in a dominant position in order to be found to have abused that position under Chapter II of the CA98 and Article 102 of TFEU.

3.79 For each of these characteristics, a competition assessment would need to differentiate between the use of consumer data to generate efficiencies for firms and consumers, and the collection and use which might lead to competition concerns.

3.80 Based on our analysis of consumer data and data markets, as well as the information received in our CFI, we consider that there are some characteristics that set data and data markets apart from other products, services and markets. However these characteristics are not unique to consumer data and the markets in which it is collected and used. Consequently, we see no reason, at present, why our existing competition and markets tools would not be effective at tackling conduct that gave rise to competition concerns in these markets.

4. Consumer issues

Introduction

4.1 In this chapter we focus on the main consumer-related concerns and potential harms arising from the collection and use of consumer data. We describe the responses we received on these issues and discuss the extent to which there may be harms arising now and the potential for them to arise in the future. We draw out some potential implications for consumers, firms and regulators.

4.2 Responses to our CFI, as well as the wider public debate underway on consumer data suggested the following key areas of potential concern:

- **Awareness and understanding** – consumers differ in their levels of awareness of data use, and a lack of transparency on the part of firms restricts their ability to make informed choices about sharing their data – potentially limiting their ability to consider and maximise the benefits to them from sharing their data. We consider these issues in **Section A**.

- **Attitudes, concerns and trust** – many consumers are concerned about sharing their data and how it will be used. Consumers have a range of concerns, including potential data loss, data misuse and unexpected data sharing. While they often share data despite these concerns, trust may be fragile and at risk if negative perceptions about new developments in data use take hold. We consider these issues in **Section B**.

- **Consent and control** – there are weaknesses in the mechanisms by which consumers are asked to share their data, and consumers lack effective control over how their data is used. These limitations and concerns potentially inhibit consumers' willingness to engage with businesses where data sharing is involved. We consider these issues in **Section C**.

4.3 We did not conduct our own research for this report – relying instead on secondary evidence and the responses to our CFI. There is a large volume of survey evidence, which, in itself, indicates widespread interest in these issues. **Appendix A** lists the evidence we have referred to in this and other chapters.[109]

[109] We primarily draw on survey and other evidence published since the start of 2011. For this short CFI, we have not sought to undertake a comprehensive identification, assessment and review of all evidence, but instead have drawn on the most frequently acknowledged and the most recent evidence where possible.

4.4 The extent to which secondary evidence sources are comparable is limited by their differing methods and samples, when they were conducted, the reasons they were commissioned, the definitions they used and the questions they asked.[110] Furthermore, data collection and use is a rapidly evolving topic, where technological advances and social changes may mean quite significant shifts in people's awareness, attitudes and behaviour. Nevertheless, our analysis suggests that some common messages can be identified.

Section A: Consumers' awareness and understanding

4.5 To make informed decisions about whether to share their data, consumers need a reasonable level of awareness and understanding that it is being collected and used, as well as how, why and the benefits to them.

4.6 There was widespread agreement in responses to our CFI that although most consumers know their data is being collected and could be used to target them with marketing, they are less aware of the various ways in which their data can be collected, or how else it might be used. Many respondents also suggested consumers lacked information on the wider benefits to them.

4.7 In this section, we therefore consider the evidence for consumers':

- awareness of data collection and the methods used;
- understanding of how their data is being used;
- views on the potential benefits of data collection and use; and
- views on how well businesses explain why they collect data.

Consumers' awareness of data collection and the methods used

4.8 Survey evidence typically supports the contention that most consumers are aware that companies collect their data. For instance, Consumer Focus (2012) found that almost all consumers (98%) thought that some personal data and information was collected by 'free-to-use' online services and social media.[111] In the same year, Demos reported research showing that 85% of

[110] These are important caveats. For example, how interviewers explain what they mean by 'consumer data' in a survey could have an important impact on how respondents interpret and reply to their questions. Furthermore, we rely in some cases on how research results have been reported and it is not always possible to know whether these reports provide full and accurate accounts of all their findings.
[111] Consumer Focus, *Consumer Focus Digital Behaviour Survey*, March 2012.

people were aware that their online purchasing history data was being collected and used, and 81% were aware of supermarket loyalty schemes.[112]

4.9 Respondents to our CFI suggested that high levels of general awareness were likely to reflect firms' requests for consumers to agree to data sharing in privacy notices and terms and conditions, as well as the requirements on firms to inform consumers of the use of cookies and provide opt-out options.

4.10 While general awareness is high, it seems to vary by age and social grade. For instance, Deloitte (2012) found that although 82% of people were fully aware, or aware, of data collection by companies and public sector bodies, 15- to 17-year-olds were the least aware (despite many having social media accounts), as were people in social grades D and E.[113]

4.11 Boston Consulting Group (2012) also suggested that consumers' levels of awareness of data collection can vary considerably by sector.[114] For example, 79% of respondents knew banks were collecting data they considered 'private'. In contrast, 65% thought social networking sites were collecting such data, and 57% said online shops were, but only 32% said retailers generally were doing so.

4.12 As **Chapter 2** notes, respondents to our CFI suggested that the range of data companies collect on consumers is wide and growing. Consumer Focus (2012) found consumers may also have quite wide ranging expectations of what data companies gather. For instance, over 70% of users of 'free-to-use' online and social media services thought these would be gathering their search history, sites visited, 'likes', location and purchases.[115]

4.13 Likewise, a GfK/Guardian survey in 2013 reported that 83% of consumers believed companies collected data about them from a wide variety of sources. But a much lower proportion (22%) claimed they understood what sorts of data companies captured about them in addition to information they already provided.[116]

4.14 This aligns with research for the Communications Consumer Panel (CCP) in 2011 which suggests that while consumers appeared to have generally high levels of awareness of data collection, their knowledge of *how* their data was being collected particularly reflected their experience of transacting with

---

[112] Demos, *The Data Dialogue*, September 2012.
[113] Deloitte, *Data Nation 2012 – Our Lives in Data*, July 2012.
[114] Boston Consulting Group, *The Value of our Digital Identity*, November 2012. Note that these findings were based on a survey in three European countries that did not include the UK (Netherlands, Germany and Poland).
[115] Consumer Focus, *Consumer Focus Digital Behaviour Survey*, March 2012.
[116] GfK and the Guardian Media Network, *Big Marketing - Executive Summary: The case for marketing to react to consumer opinions on personalisation*, October 2013.

businesses: 85% of internet users recognised registering their details and opting whether to receive marketing from first party companies as a way in which firms collected their data. A lower proportion, 64%, were aware of the use of 'cookies' to gather information; 59% had heard of companies using information from social networking profiles; and 45% were aware that mobile apps can collect personal data.[117]

4.15 Qualitative research supports the view of some CFI respondents that consumer awareness of passive data collection is lower. For instance:

- Ofcom (2013) reported that: '….most [participants] had little or no awareness of how and why their information was used, stored and transferred online, and many participants lacked any real understanding of cookies and targeted advertising';[118] and
- The Economic and Social Research Council (ESRC) and the Office for National Statistics (ONS) (2014) found that '…most [participants] spontaneously spoke about the provision or collection of personal data that happens when a person fills out a form or survey...They usually had to be prompted to start thinking about more passive forms of data collection, for example cookies or data on travel or purchasing patterns'.[119]

4.16 Some respondents to our CFI suggested, however, that awareness would rise with ongoing growth in more explicit data-driven services such as recommendations based on consumers' previous purchases, or 'people like you', as well as developments such as the IoT and roll out of smart meters.

Consumers understanding of how their data is used

4.17 Many potential uses of consumer data benefit firms in ways that may not be visible to consumers. As we noted in **Chapter 2**, respondents to our CFI cited many ways in which firms use consumers' data – including service improvement, transaction efficiency and fraud prevention. Principal amongst the uses cited, however, was marketing and advertising.

4.18 Advertising, by its nature, is intended to secure public attention. Consumers are also often asked whether they are content to receive marketing materials. It is therefore unsurprising that consumers have relatively high levels of awareness that their data is used to support marketing. For instance, in 2014,

---

[117] CCP, *Online personal data: the consumer perspective*, May 2011.
[118] Ofcom, *Being online: an investigation of people's habits and attitudes*, June 2013.
[119] ESRC and ONS, *Dialogue on data: Exploring the public's views on using administrative data for research purposes*, March 2014.

a survey by the Royal Statistical Society (RSS) found that 77% of respondents were aware of online retailers looking at their previous webpage visits and sending them targeted adverts.[120]

4.19 However, consumer awareness of the other uses of their data seems lower. Demos (2012) reported that while the public was aware that personal information and behavioural data were used for commercial purposes, their understanding of what this meant was limited and it varied by type of data and its collection. For example, while 85% were aware that online purchasing history data was collected, workshop participants '…knew and understood much less about how data were collected and used'.[121]

4.20 Likewise, Ofcom (2013), reporting findings from discussion groups, found that generally, participants '…had only vague ideas about what happened to their personal data online'.[122]

4.21 We consider in **Section B** consumers' attitudes to the use of their data – including that most consumers dislike the concept of it being used for targeted advertising. If their primary understanding of the use of their data is that it will be used to market products to them, they may be expected to be more likely to have negative attitudes about sharing data generally.

Views on the potential benefits of data sharing

4.22 Respondents to our CFI identified a wide array of benefits for consumers from the use of their data, including personalised and customised services, wider choice and new services, better provision of existing services, more relevant advertising and targeted offers (see **Chapter 2**).

4.23 Some respondents suggested there was growing consumer awareness of how they benefited from sharing their data. Most of those commenting, however, thought consumers were unlikely to recognise all the potential benefits proposed above.

4.24 Survey evidence also suggests people have a narrower perception of how they might gain from sharing data. For instance:

- When prompted to consider the main reasons companies collected their data, 70% of respondents to Consumer Focus' 2012 survey agreed the information might be sold to other companies so these companies could advertise to them. In contrast, one in five (19%) agreed that companies

[120] Royal Statistical Society (RSS), *Public attitudes to the use and sharing of their data*, July 2014.
[121] Demos, *The Data Dialogue*, September 2012.
[122] Ofcom, *Being online: an investigation of people's habits and attitudes*, June 2013.

needed it to improve their service and less than one in ten (8%) thought it was needed to ensure the service worked properly.[123]

- RSS (2014) found that 15% of respondents agreed that they benefitted from companies using their personal data – for example by getting a quicker service, or recommendations for products they would not have thought of. In contrast, 44% disagreed.[124]

4.25 While consumers may have limited awareness of the various ways in which firms use their data to their potential benefit, a number of CFI respondents suggested that many consumers were increasingly aware that they were part of a mutual 'value exchange' – in effect, recognising that, in return for sharing their data with businesses, they also received some form of reward. These rewards may be overt (for instance, gifts, a discount voucher or entry into a prize draw), or they may be less obvious (for instance, provision of a 'free at point of use' service, such as social networking).

4.26 Some respondents suggested that most consumers pragmatically weigh up the benefits of sharing data on a case-by-case basis. Others suggested that as consumers became more aware of the value of their data, they could increasingly see the exchange as unfair.

4.27 Survey evidence suggests that when asked directly about sharing their information in exchange for clear personal benefits, some consumers do identify a value exchange relationship. For example:

- in the 2011 EC survey, when asked specifically about 'free' email and other services that operated thanks to targeted marketing based on information about their online activities, although 45% of UK respondents were uncomfortable, 49% were comfortable;[125] and

- Deloitte (2014) reported that 64% of consumers either did not mind or were happy to share their personal information if it led to direct benefits for them, such as financial savings, product improvements and personalised services.[126]

4.28 There is some evidence which suggests that consumers generally appear unwilling to pay for 'free at point of use' services. For example:

---

[123] Consumer Focus, *Consumer Focus Digital Behaviour Survey*, March 2012.
[124] RSS, *Public attitudes to the use and sharing of their data*, July 2014.
[125] European Commission, *Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union*, June 2011.
[126] Deloitte, *Data Nation 2014 – Putting customers first*, November 2014.

- Consumer Focus (2012) found that 66% of consumers would not be willing to pay for the 'free at point of use' service they used most frequently; and almost all of those who would be willing to pay (8% of the respondents) were prepared to pay up to £50 per year;[127] and

- Research by ComRes for Big Brother Watch (2015) likewise found that 75% of people would not be willing to pay anything for a 'free at point of use' service if it meant their data would not be collected and used by the provider.[128]

4.29 Survey evidence also suggests that consumers typically are uncertain about the value of their data. Many would be willing to pay to keep their information private – although the amounts they would pay vary. For instance:

- Consumer Focus (2012) found that 15% of consumers thought that their personal data and information was worth nothing to the service they used most frequently, and 61% did not know. Of those who thought their data had worth, there was little consensus on its value. However, 62% agreed that they should be paid a fee by organisations using their data;[129] and

- DMA (2012) reported that over a third of people saw their personal information as an asset that could be used to negotiate better prices and offers with companies, with this rising to over 40% among those aged 25 to 34.[130]

4.30 Furthermore, consumers apparently consider that it is businesses that benefit the most from the use of their data. For example:

- Orange (2014) found that 80% of respondents considered their data had a value to businesses;[131] and, in a related study, that 71% of UK respondents believed organisations benefitted most from gathering information on customer purchases or history;[132] and

- RSS (2014) reported that 78% of survey respondents agreed that 'companies use my personal information for their benefit, not mine', with only 4% disagreeing. Only 6% agreed that '…companies have my best

---

[127] Consumer Focus, *Consumer Focus Digital Behaviour Survey*, March 2012. 25% responded that they did not know if they would be willing to pay anything.
[128] ComRes, *Big Brother Watch Online Privacy Survey*, March 2015.
[129] Consumer Focus, *Consumer Focus Digital Behaviour Survey*, March 2012.
[130] DMA, *Data Privacy: What the consumer really thinks*, June 2012.
[131] Orange, *The Future of Digital Trust: A European study on the nature of consumer trust and personal data*, September 2014.
[132] Orange, *The Future of Digital Trust: A European study on the nature of consumer trust and personal data*, February 2014.

interests at heart when they use my personal data', with 71% disagreeing.[133]

4.31 There is, however, some evidence that younger and more experienced internet users have more positive attitudes to how they and society more generally benefit, which may have implications for the evolution of consumer attitudes over time. For example:

- DMA (2012) reported that a third of people agreed that the exchange of personal information was essential for the smooth running of modern society, but 50% of younger respondents agreed this was so; [134] and
- RSS (2014) found that younger people, and those with social media accounts, were more likely to feel they benefited from companies using their personal data – for example, 22% of 16 to 24-year-olds agreed compared with only 8% of 55 to 75-year-olds.[135]

Views on how well businesses explain data collection

4.32 A number of CFI respondents suggested that firms provide insufficient explanation of what information they are gathering and why. Survey evidence suggests that many consumers share the same view:

- The 2011 EC survey found that when joining a social networking site or registering for a service online, 59% of UK internet users said they were always or sometimes informed about the conditions and uses of their personal information, but 24% said they were rarely or never informed. 53% of UK respondents felt sufficiently informed, but 42% did not.[136]
- Deloitte (2014) reported that 72% of respondents felt companies were not telling them how they use their personal information.[137]
- A 2014 global survey by the Global Privacy Enforcement Network (GPEN)[138] reported by ICO examined over 1,200 mobile apps and found that 85% failed to clearly explain how they were collecting, using and

[133] RSS, *Public attitudes to the use and sharing of their data*, July 2014.
[134] DMA, *Data Privacy: What the consumer really thinks*, June 2012.
[135] RSS, *Public attitudes to the use and sharing of their data*, July 2014.
[136] European Commission, *Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union*, June 2011.
[137] Deloitte, *Data Nation 2014 – Putting customers first*, November 2014.
[138] GPEN is an informal network of privacy authorities which aims to foster cross-border cooperation.

disclosing personal information; and 59% of the apps 'left users struggling to find basic privacy information'.[139]

4.33 More generally, some respondents to our CFI questioned the extent to which firms are transparent about who they share data with. There are no standardised explanations and policies often refer to 'selected third parties' and 'trusted partners'.

4.34 On this point, DotEcon's research noted from its review of some example privacy policies that these explained '…in varying degrees of detail how it [consumer data] is used, who it is shared with and why…'. It found that there was '…sometimes ambiguity within privacy policies with respect to the role of third parties and the degree to which data may be shared with third parties (eg 'we may share this data with third parties for purposes including analysis')).' [140]

4.35 DotEcon suggested that some firms may deliberately be non-specific when describing with whom they will share data and why, to enable them more easily to flex what they do in practice to meet business needs and new opportunities. We consider consumers' attitudes to firms sharing data further below.

4.36 Many respondents to our CFI also highlighted the importance of educating consumers about how their data was being used, so as to increase trust and their willingness to share their information. We consider some of these activities further in **Section C**. Some also pointed to a number of ways in which commercial bodies were informing consumers – including cookie notices, privacy statements, educational pages and the role of self-regulatory initiatives such as AdChoices.

4.37 There is some evidence that consumers would be more willing to share data if firms were more transparent about data use, but also if they explained how consumers would benefit from how their data is used:

- Deloitte (2013), for example, reported that

  '…people who are confident that companies tell them how their personal data is used are between two and three times as likely as the average respondent also to be confident in other areas. For example, they are more confident that their data is kept secure, is used to offer better levels

[139] ICO, *Global survey finds 85% of mobile apps fail to provide basic privacy information*, September 2014. As a member of GPEN, ICO examined 50 of the top apps released by UK developers.
[140] DotEcon and Analysys Mason, *The Commercial Use of Consumer Data – A research report for the CMA*, June 2015.

of service or relevant products, and is shared with third parties only with their knowledge and in an anonymised form.'[141]

- In 2014, a GfK survey found that 77% of people would provide companies with more information if they could be sure the companies were not going to share it without their explicit permission. Furthermore, 71% of consumers would provide more information if it helped them to save money and 60% if they received a service better tailored to their needs.[142]

Implications

4.38 The evidence broadly supports the contention that, while their awareness of data collection for advertising purposes is quite high, consumers' wider understanding of how and why their data is collected is more limited. Consumers' awareness of data collection largely reflects what they actively volunteer, and they see advertising as a key purpose for collecting their data.

4.39 Some consumers identify a 'value exchange' from sharing data, but most feel they lack information on how they benefit and perceive firms benefit more than they do. Furthermore, many consumers appear unhappy with how well firms explain why they collect data and consider that more could be done to improve transparency.

4.40 Low consumer awareness and limited or negative perceptions about the benefits of sharing data have a number of potential implications, including:

- reduced ability on the part of consumers to make informed decisions when deciding whether and how to engage with firms;
- limits on consumers' ability to exert control over their data and to hold firms to account; and
- lower consumer willingness generally to share their data than would otherwise be the case.

4.41 These could result in some people choosing not to engage or to minimise the information they share, impacting in turn on firms' business strategies and growth. Furthermore, as we note in **Chapter 3**, if consumers are limited in their ability to make informed decisions and to challenge firms over the use of their data, this may mean that firms have limited incentives to compete over the protection they afford to consumer data.

---

[141] Deloitte, *Data Nation 2013 – Balancing growth and responsibility*, August 2013.
[142] See: Marketing Week, *People Power*, March 2014.

4.42 On the other hand, there is some evidence that consumers will be more willing to share data if they understand how it will be used and how they might benefit. This suggests that companies need to be clear about what consumers are being asked to provide, how they will use this data and what benefits consumers will get from the exchange.

Section B: Consumers' attitudes, concerns and trust

4.43 Despite evidence that most consumers are concerned about what might happen to their data, many people continue to share their data (the 'privacy paradox'). In this section, we consider:

- consumers' attitudes to the collection and use of data;
- the nature and extent of consumers' concerns;
- consumers' specific fears;
- potential consumer harms; and
- consumer behaviour and the 'privacy paradox'.

Consumers' attitudes to the collection and use of data

4.44 Consumer data has a high profile, reflecting the huge growth in online data sharing discussed in **Chapter 2**, but potentially also often driven by media stories about privacy concerns, data breaches and unwanted communications from both legitimate firms and rogue traders.

4.45 It is therefore perhaps unsurprising that the protection of their data is a key issue for many UK citizens. The 2011 EC survey found disclosing personal information to be a big issue for 67% of UK respondents.[143] Likewise, ICO's 2014 Annual Track survey found that protecting privacy was an important issue for many respondents, with 21% citing it as a top three concern.[144]

4.46 A closer look at consumers' attitudes, however, reveals some important differences in willingness to share information. In particular, some studies have identified a spectrum of public attitudes to how people perceive their

[143] European Commission, *Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union*, June 2011.
[144] ICO, *Annual Track*, September 2014.

personal data and their level of comfort in sharing it. For example, Demos (2012) classified people into five groups (**Box 4.1**).[145]

Box 4.1: Consumers' willingness to share data

Category	*%*	*Profile*
Non-sharers	30	'Non-sharers' are very cautious about technology and sharing their data, and tend not to be experienced at using technology. They view their data as personal, and take proactive measures to keep them private: unsubscribing, deleting their browsing history, and alerting companies to possible violations. This attitude towards privacy is not just internet specific: non-sharers often list their number as ex-directory. As a group, they are knowledgeable about data protection and receptive to ideas that allow them to withdraw their data.
Sceptics	22	'Sceptics' do not have a single view about whether information is personal or impersonal, but are sceptical about whether government and companies can be trusted. Unlike non-sharers they do not use online services much, and tend to be older. They are cynical about the benefits of sharing data. They sometimes buy into 'value exchange' transactions when personal benefits are clear, but would welcome measures to give them simple, direct and regular control over their data.
Pragmatists	20	'Pragmatists' do not know all the details of how their data are used, but take small measures to protect their privacy. They prefer efficient services to complete privacy – seeing benefits from the sharing of personal information – so their trust in the companies or institutions that hold their data is key.
Value hunters	19	'Value hunters' understand the financial value of their data and consider that sharing it can save money and time. They tend to be young, and are often early adopters of technology. They are not overly concerned about data sharing and are reasonably comfortable with it being used.
Enthusiastic sharers	8	'Enthusiastic sharers' categorise a lot of the information about them as impersonal, and subsequently are comfortable with sharing it. They understand 'value exchange' transactions, seeing the benefits of sharing information, and are amenable to sharing even more in the future. They have some concerns about the ways in which their data might be misused, but are comfortable if data use is specified.

Source: Adapted from Demos, *The Data Dialogue*, September 2012.

4.47 DMA (2012) identified a broadly similar breakdown of consumers by their willingness to share data, suggesting a three-way split that, according to their report, was largely unchanged from a similar study in 1997, as follows:

- 31% (25% in 1997) were 'privacy fundamentalists' – consumers who are unwilling to provide personal information, regardless of any enhanced service they may receive in return.
- 53% (60% in 1997) were 'privacy pragmatists' – 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.
- 16% (15% in 1997) were 'privacy unconcerned' – expressing no worries about the collection and use of personal information about them.[146]

4.48 Whether or not the population can be so clearly segmented, however, it is apparent that broad categorisations mask more detailed socio-demographic

[145] Demos, *The Data Dialogue*, September 2012.
[146] Direct Marketing Association (DMA), *Data privacy: what the consumer really thinks*, June 2012.

differences between consumers, which may have an impact on their attitudes to data sharing and perhaps the extent to which many make pragmatic decisions on a case-by-case basis.

4.49 Given the take up of the internet, there may be some relationship between level of experience of its use and consumers' level of comfort in data sharing. For example, as **Chapter 2** noted, older people are typically less likely to have home internet access. They are also less likely to use social media than younger people. Very broadly, older people also tend to be less comfortable sharing their data than younger people.

4.50 Ofcom (2014) reported, for instance, that while only 17% of all respondents agreed with the statement 'I don't really think about the personal information I am providing to companies online', this rose to 24% of those aged 16-24 but was only 13% for those aged over 65.[147]

4.51 There is no one set of definite evidence setting out which factors most influence consumers' views on data sharing. However, survey and other evidence suggests that key variables include the type of data involved and who is collecting this information. We consider these further below.

Type of data

4.52 While survey findings differ, it seems clear that consumers do not see all data in the same light. In particular, they appear to attach a higher sensitivity and a lower willingness to share data such as financial and medical information (**Box 4.2**). Contact details, such as home address and phone number also rate quite high as data consumers particularly care about.[148]

4.53 Broadly, as Sciencewise (2014) noted, consumers tend to rate their behavioural data (such as social networking posts and purchasing history) as less personal or sensitive than information about who they are (such as name and address).[149] However, some more recent evidence (eg ICO, 2014) suggests relatively high proportions of consumers rate their search history and location as extremely sensitive.[150]

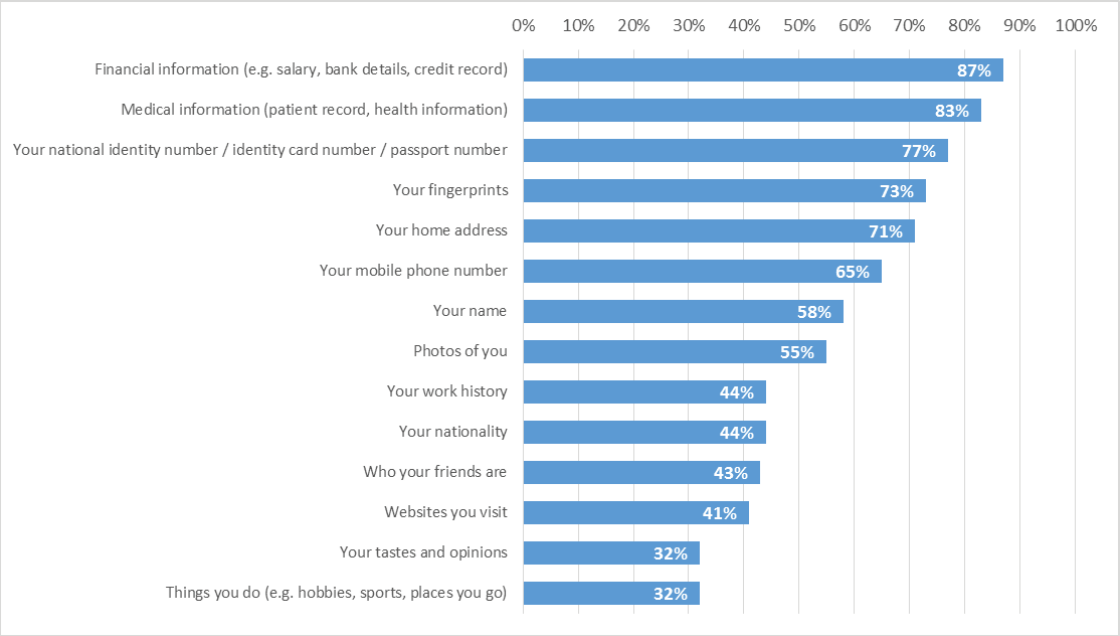
---

[147] Ofcom, *Adults' Media Use and Attitudes Report 2014*, April 2014.
[148] It should also be noted that consumers' varying attitudes to different types of data and their views on what information they consider most sensitive may have important implications for any consideration of the survey evidence in this area. For instance, evidence on how consumers responded to general questions about their 'data' could be influenced by what types of data they were thinking about when they replied.
[149] Sciencewise, *Big Data - Public views on the collection, sharing and use of personal data by government and companies*, April 2014.
[150] ICO, *Annual Track*, September 2014.

Box 4.2: What types of data do consumers care most about?

Eurobarometer (2011) reported that for the UK (in common with other member states), financial and medical information were the items considered personal by the most respondents. Many UK respondents also identified contact details, such as home address and phone number as personal. A lower proportion (41%) identified website visits as personal, but this was higher than the average across the EU (25%). See **Figure 4.1**.[151]

Figure 4.1: Information and data considered personal



Source: Based on European Commission, *Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union*, June 2011.

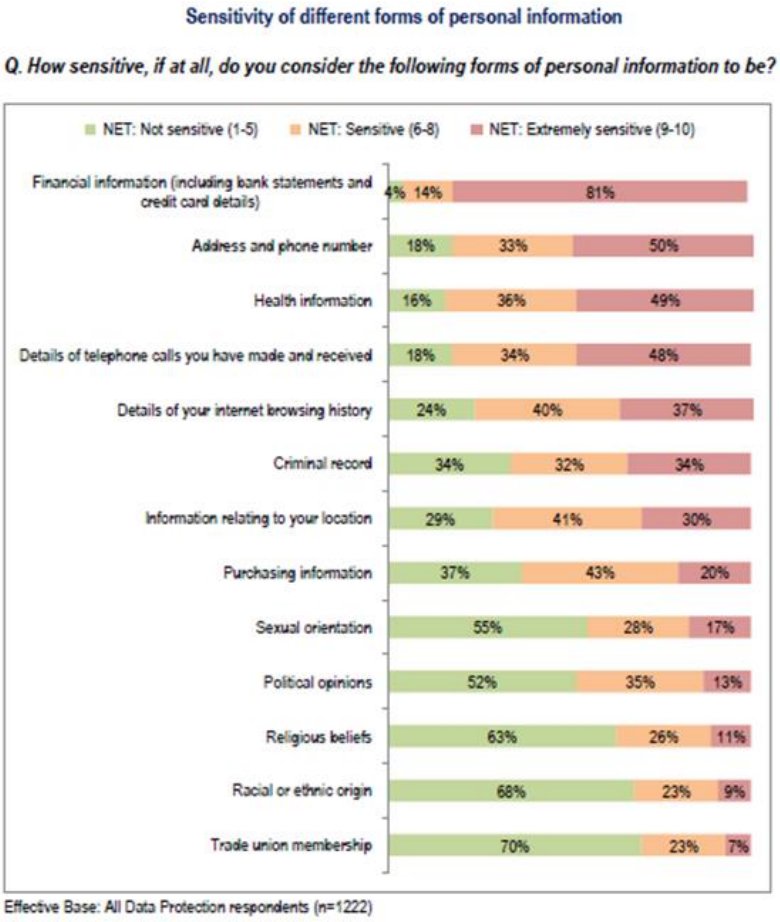
Demos (2012) concluded that what constitutes personal information varied by individual and that '…there is no clear set of principles or ideas that marks certain types of information as personal or non-personal'. However, the public appeared more likely to consider information about their personal lives (such as health records, sexual orientation and friends), or that could allow them to be identifiable (such as phone number or email address) as 'personal information'. In contrast, fewer people viewed behavioural information (such as frequent purchases, favourite websites, or films, books and music they like) as 'personal'.[152]

The 2014 ICO Track also reported that financial data in particular was seen as sensitive, followed by address details and health information. Over one-third (37%) of the survey respondents, however, identified internet browsing history as 'extremely sensitive' (see **Figure 4.2**).[153]

---

[151] European Commission, *Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union*, June 2011.
[152] Demos, *The Data Dialogue*, September 2012.
[153] ICO, *Annual Track*, September 2014.

Figure 4.2: Sensitivity of different forms of personal information



Source: ICO.

4.54 Qualitative research by the Wellcome Trust (2013) similarly found that whilst participants considered financial data, such as credit history, to be sensitive, they also rated internet search history as such. Key criteria the participants used to distinguish between data types included the perceived degree of seriousness/risk if the data were misused or stolen and the level of security of the data; whether the data was anonymous or personally identifiable; and the extent to which its value to themselves or others was clear.[154]

4.55 Respondents during our CFI also suggested that consumers' levels of sensitivity could be related less to specific data items and more to:

- data combinations – how consumers' perceived individual data items might be combined to compile a profile; and

[154] The Wellcome Trust, *Summary Report of Qualitative Research into Public Attitudes to Personal Data and Linking Personal Data*, July 2013.

- the context – for example address data was likely to be more sensitive to a vulnerable person seeking refuge from a violent relationship.

4.56 However, consumers' attitudes may be changing as they use social media and become more aware of how 'cookies' can track browsing behaviour, or mobile phones can provide location data. For instance:

- the Wellcome Trust (2013) reported that 'categories' of data, as perceived by the public, are 'fluid/overlapping';[155]
- DMA (2012) found that two-thirds of respondents agreed their definition of privacy was changing due to the internet and social media;[156] and
- MRS (2015) reported that 70% of its survey respondents considered the privacy of their personal information to be more important to them now than it was five to ten years ago, with only 5% saying it was less so.[157]

The organisations collecting data

4.57 In terms of the organisations that collect and use data, consumers appear typically to trust public bodies with their data more than they do commercial companies (**Box 4.3**). This accords with evidence that people are more willing to share data where they perceive societal gain (for instance to develop cancer treatments, improve transport scheduling or prevent crimes), but more likely to oppose its use for commercial gain.[158]

4.58 However, consumers also appear to have differing views according to the type of commercial body – in particular, rating financial institutions, online retailers and supermarkets above mobile phone companies, internet companies and social media in terms of levels of trust.

4.59 Survey evidence suggests that consumers' awareness of the data collector also has an important influence on their willingness to share their information. For instance, DMA (2012) found that trust in the organisation was the main driver for sharing information, with over half the respondents agreeing; and 30% agreeing that previous purchasing experience was also a factor.[159]

---

[155] The Wellcome Trust, *Summary Report of Qualitative Research into Public Attitudes to Personal Data and Linking Personal Data*, July 2013.
[156] DMA, *Data Privacy: What the consumer really thinks*, June 2012.
[157] MRS, *Private Lives - Putting the consumer at the heart of the privacy debate*, March 2015.
[158] Department for Business, Innovation and Skills and the Economic and Social Research Council, *Public Attitudes to Science (PAS)*, March 2014.
[159] DMA, *Data Privacy: What the consumer really thinks*, June 2012.

4.60 Orange (2014) also suggested that familiarity might influence consumers' attitudes – with 48% of all respondents stating that they would never share their full name or date of birth with an unfamiliar organisation, compared to 35% who would never share this with a previously-known company.[160]

4.61 We consider below the extent and nature of consumers' concerns. However, it seems clear that, overall, consumers' views on their data varies from individual to individual, and case-by-case, suggesting that there is no one size fits all approach to addressing any concerns they may have. As Citizens Advice suggested in a recent report, '…people's general attitudes…are contextual and dependent on the circumstances, organisations, types of data, links with other data and purpose of use. In short, privacy is a personal setting, with only the individual knowing what they are comfortable sharing on what basis…'.[161]

Box 4.3: Consumers' trust in different types of data collector

Consumer Focus (2012) found higher levels of trust in banks as well as institutions such as the NHS and police service. Non-banking commercial bodies were ranked below the government departments in their list and the Post Office. Even within the ranking of commercial bodies there were also apparent differences - with consumers placing higher levels of trust in supermarkets, than technology or social media companies.[162]

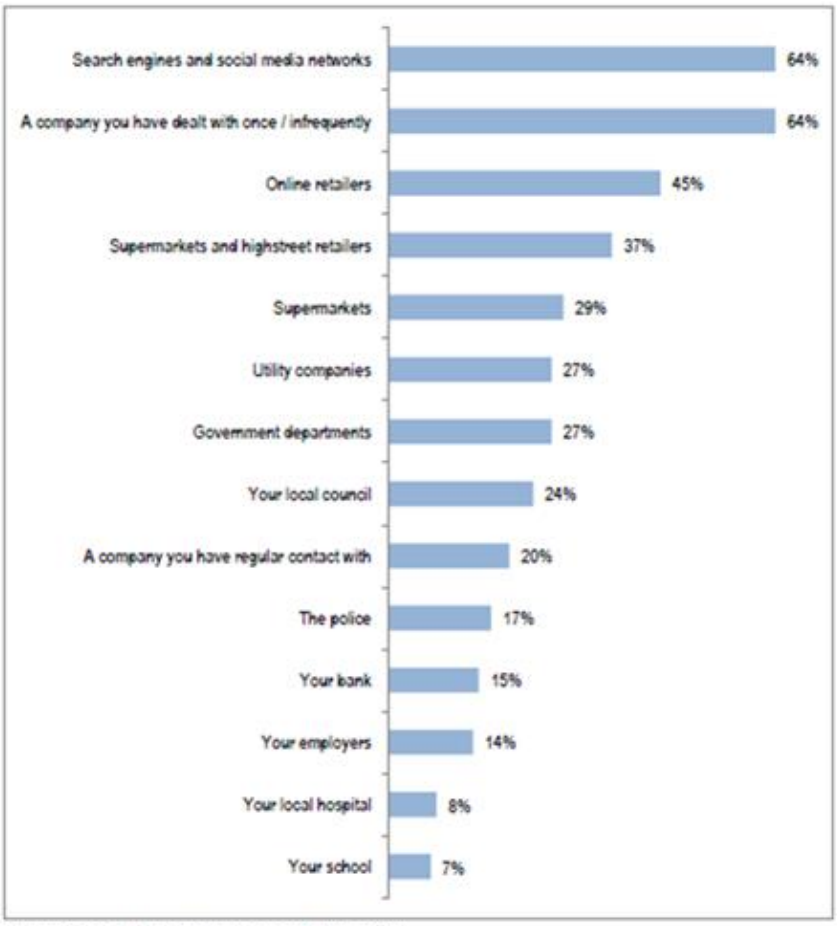
RSS (2014) reported that trust in data use was low for all institutions especially for 'companies that rely heavily on data'. The survey again suggested that people ranked institutions such as medical and police services higher than telecoms and internet companies and social media, but it also suggested a higher level of trust in online retailers than in supermarkets or insurance companies.[163]

In 2014, ICO reported that search engines and social media networks and companies dealt with infrequently stood out as the organisations people were most concerned about holding their personal information (see **Figure 4.3**).[164]

[160] Orange, *The Future of Digital Trust: A European study on the nature of consumer trust and personal data*, September 2014.
[161] Citizens Advice, *Personal data empowerment – Time for a Fairer Data Deal?*, April 2015.
[162] Consumer Focus, *Consumer Focus Digital Behaviour Survey*, March 2012.
[163] RSS, *Public attitudes to the use and sharing of their data*, July 2014.
[164] ICO, *Annual Track*, September 2014.

Figure 4.3: Which organisations are people concerned about holding their personal data?

Q. Which, if any, of the following organisations would you be most concerned about holding your personal information?



Effective Base: All Data Protection respondents (n=1222)

Source: ICO

The overall level of consumer concern

4.62 Sciencewise reports that '…the public's immediate reaction to the collection and use of their data by companies or government appears to be one of opposition'.[165] Survey evidence confirms that many consumers have substantial reservations about sharing their data and how it might be used.

4.63 As we noted above (**paragraph 4.46**), some studies identified segments into which consumers can be categorised according to their willingness to share data. These suggested a large proportion of the population had some concerns about data sharing which could inhibit their interaction with

[165] Sciencewise, *Big Data - Public views on the collection, sharing and use of personal data by government and companies*, April 2014.

companies. These consumers could be further sub-divided into those unwilling to share data and those who do so on a case-by-case basis when they considered the perceived benefits outweighed the perceived costs.

4.64 Other surveys have found high, and apparently persistent, levels of concern when asked specifically about how happy they were for companies to collect their data (**Box 4.4**).

Box 4.4: Consumers' concerns about companies collecting their data

Deloitte (2012) found that more than two-thirds (71%) of people were opposed to the use of their data by companies, with only 8% in favour.[166]

Demos (2012) reported that whilst overall the public was uncomfortable with every type of information and data use they were asked about, the highest level of comfort was with supermarket loyalty schemes (27%), and the lowest with internet-based uses such as cookies for advertising or the scanning of email content for the purposes of targeted advertising.[167]

In 2015, Big Brother Watch found that while 19% considered that 'consumer experiences are being enhanced by big companies gathering large amounts of their personal data for internal use, 46% considered consumers were being harmed by such data gathering; and 21% considered neither scenario was the case.[168]

Also in 2015, TRUSTe reported that the proportion of British internet users worried about their privacy online was 92% compared with 89% in 2014 and 88% in 2013.[169]

4.65 With data increasingly being collected and used online, consumers' attitudes to their privacy over the internet is a key issue with survey evidence suggesting high and persistent levels of concern. For example:

- TRUSTe (2015) reported that 34% of its survey respondents worried frequently or always about their privacy online and that nearly half (48%) disagreed that they trusted companies with their personal information online. The same survey also found that 33% were more concerned about their online privacy than they were a year ago;[170] and
- Big Brother Watch (2015) reported similarly high levels of public concern, with 79% very or fairly concerned about their privacy online.[171]

[166] Deloitte, *Data Nation 2012 – Our Lives in Data*, July 2012.
[167] Demos, *The Data Dialogue*, September 2012.
[168] Big Brother Watch, *UK Public Research - Online Privacy*, March 2015.
[169] TRUSTe, *2015 TRUSTe UK Consumer Confidence Index*, January 2015.
[170] TRUSTe, *2015 TRUSTe UK Consumer Confidence Index*, January 2015.
[171] Big Brother Watch, *UK Public Research - Online Privacy*, March 2015.

4.66 A feeling of a loss of control appears to be a core theme, perhaps helping to explain consumers' specific fears about how their data might be used. For example:

- EC (2011) reported that 25% of UK respondents who had disclosed personal information when shopping online felt that they had no control over this information (for instance to change, delete or correct it);[172]
- in ICO's 2014 annual track survey, nearly two thirds (63%) of the public considered that they had lost control over the way their information is collected and processed;[173] and
- MRS (2015) reported that one in ten survey respondents felt in complete control over what of their personal information is kept private, with 44% feeling that they had no, or not very much, control.[174]

4.67 Survey evidence also suggests that consumers expect that the extent to which they provide data will increase and that many expect to continue to feel uncomfortable about this. Demos (2012) found that 48% of respondents expected to be sharing more information with companies in ten years' time, compared with 19% expecting to be sharing less; and 45% expected to feel less comfortable about this, compared with 20% who expected to feel more comfortable.

Consumers' specific concerns

4.68 A number of studies have sought to identify consumers' main concerns. Broadly, this evidence suggests their main fears relate to uncertainty and concern about how their data might be used, rather than how it is collected. For instance:

- Deloitte (2012) found the main reason given by respondents who opposed organisations' use of their personal data was that they lacked confidence or awareness about what would happen to it (51%), while 42% considered their information was 'none of the companies' business';[175]
- ESRC/ONS (2014) reported qualitative research that '…personal data security was very important to participants…They were particularly concerned about identity theft, and personal data being sold on to other

[172] European Commission, *Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union*, June 2011.
[173] Information Commissioner's Office (ICO), *Annual Track*, September 2014.
[174] MRS, *Private Lives - Putting the consumer at the heart of the privacy debate*, March 2015.
[175] Deloitte, *Data Nation 2012 – Our Lives in Data*, July 2012.

organisations. Often the main objection to the latter was the profit companies make from using their data, rather than the privacy implications….';[176] and

- RSS (2014) found that 65% of respondents said their mistrust of internet companies' data use was based on their view that these companies would use their personal data for other purposes which they would not be told about.[177]

4.69 This and other evidence (**Box 4.5**) suggests that consumers are essentially concerned about losing control of their personal information and that their data will be lost or stolen, shared without their approval, or used to support unsolicited marketing.

Box 4.5: Consumers' concerns about data collection and use

EC (2011) reported that the main risks perceived by UK online shoppers in relation to sharing their data were that they might be a victim of fraud (65%), at risk of identity theft (56%), that their information might be used without their knowledge (34%), or shared with third parties without their agreement (33%).[178]

Deloitte (2014) found that 63% of adults were not confident companies kept their personal data secure from loss and theft; and 22% were confident companies inform them about selling or sharing their personal data with other organisations.[179]

Likewise, Demos reported in 2012 that losing control of personal information was the main concern – for instance, personal data being used without permission (80%), being sold to third parties or lost by companies (both 76%).[180]

[176] Economic and Social Research Council (ESRC) and the Office for National Statistics (ONS), *Dialogue on data: Exploring the public's views on using administrative data for research purposes*, March 2014.
[177] RSS, *Public attitudes to the use and sharing of their data*, July 2014.
[178] European Commission, *Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union*, June 2011.
[179] Deloitte, *Data Nation 2014 – Putting customers first*, November 2014.
[180] Deloitte, *Data Nation 2012 – Our Lives in Data*, July 2012.

ICOs' 2014 Tracker survey reported that the public's main concerns about organisations holding their data was that their information might be shared without their consent (70%), held without their knowledge (62%), or held insecurely (61%). Only 22% of respondents agreed that online companies collected and kept their personal details in a secure way; and 19% that organisations handled their information in a fair and proper way. Most people registered high levels of concern that organisations holding their personal details might pass or sell this information to other organisations (75% very concerned), not collect and keep their details secure (60% very concerned), or send or make unwanted emails, faxes, letters or telephone calls (59% very concerned). Three quarters of people (75%) were very concerned about their personal information being stolen by criminals hacking into large websites. Two-thirds (67%) were very concerned about their personal information being lost by organisations not looking after it properly, and a similar proportion (64%) were very concerned about nuisance and 'cold' calls. Over half (53%) were very concerned about spam emails and leaks.[181]

4.70 There is also an apparent public dislike of their data being used for targeted marketing. For example:

- Deloitte (2012) found that 17% of respondents were happy to receive tailored communications, adverts or offers for products or services that were based on items previously bought or looked at, with 45% saying they were unhappy and 38% either undecided or did not know;[182] and
- in 2014, RSS found that 71% of respondents felt that retailers should not be looking at their past pages and sending them targeted advertisements, with 13% agreeing that they should.[183]

4.71 We noted in **Chapter 2** the growth in digital advertising and, in particular expected growth in programmatic advertising, which involves the automated buying and selling of online advertising using processes such as real-time bidding. Aside from the likely efficiencies in advertising, these developments may have implications for consumer data. For instance:

- the ability increasingly to monetise previously unsold (or cheaply sold) inventory in real-time could fuel more demand for consumer data; and
- the targeting of advertising appears likely to continue to be increasingly based on a more granular understanding of individuals (sometimes called the 'segment of one').

[181] ICO, *Annual Track*, September 2014.
[182] Deloitte, *Data Nation 2012 – Our Lives in Data*, July 2012.
[183] RSS, *Public attitudes to the use and sharing of their data*, July 2014.

4.72 More generally, there is evidence that consumers may be finding how companies handle their data to be unsettling. For instance GfK (2015) reports a survey finding that 69% of consumers find it 'creepy' the way companies use information about them.[184] Other research suggests that once companies exceed a certain level of personalisation, consumers may feel increasing levels of discomfort and even recoil (sometimes called the 'uncanny valley' effect).[185]

4.73 Consumers concerns and attitudes about the use of their data could have important implications for whether and how they engage with firms – and thus implications for firms' success (**Box 4.6**).

Box 4.6: The implications of consumers' concerns for their behaviour

Deloitte (2012) reported that 70% of respondents would consider breaking off their relationship with a company if it failed to keep their personal data safe or lost it, and 56% said that they might do the same if the company sold data to other companies, even if this information been anonymised.[186]

Deloitte (2014) reported that the proportion of people likely to stop transacting with companies that sold their anonymous data had risen to nearly two-thirds (64%).[187]

ICO (2013) found that 62% of app users are concerned about how apps can use their personal information and 49% have decided not to download an app due to their concerns about privacy.[188]

Consumer Futures (2013) reported that privacy concerns could undermine consumer confidence in using price comparison websites (PCWs) for purchasing and switching decisions, with 30% of consumers reluctant to provide them with their personal details.[189]

RSS (2014) found that failing to keep safe or losing data ranked alongside providing a poor service as a reason for consumers to stop using a company (agreed by 72% in both cases). A substantial minority (35%) said that they would still care about how their data was used, even if they could not be identified from it.[190]

TRUSTe (2015) found that 89% of British internet users avoid companies that they do not believe protect their privacy online.[191]

---

[184] GfK, *For love or money: how to win the battle for customers*, January 2015.
[185] See for example: Colin Strong, *The Human Side of Big Data: Exploring the way Data Shapes Consumer-Brand Relationships*, October 2014.
[186] Deloitte, *Data Nation 2012 – Our Lives in Data*, July 2012.
[187] Deloitte, *Data Nation 2014 – Putting customers first*, November 2014.
[188] ICO, *ICO warns consumers about the need for caution when downloading mobile apps this Christmas*, December 2013.
[189] Consumer Futures, *Price comparison websites: consumer perceptions and experiences*, July 2013.
[190] RSS, *Public attitudes to the use and sharing of their data*, July 2014.
[191] TRUSTe, *2015 TRUSTe UK Consumer Confidence Index*, January 2015.

TRUSTe (2015) reported that 80% of survey respondents were concerned about the idea of personal information collected by smart devices and 26% mentioned concerns about the security or privacy of the data collected as a reason why they do not currently own a smart device.[192]

4.74 Other actions some consumers say they might take which could have the effect of inhibiting effective transaction-making, include supplying the minimum information or even lying. For example:

- the 2011 EC survey reported that 66% of UK respondents protected their identity by giving the minimum required information, whilst a small proportion (5%) provided wrong information to protect their identity;[193] and
- more recently, Deloitte (2014) reported that 38% of UK consumers had admitted to lying when giving information.[194]

Potential consumer harms

4.75 We asked respondents to our CFI to identify potential risks and harms ('detriment') to consumers from the collection and use of their data. The most cited potential risks for consumers largely aligned with the concerns identified in the survey evidence above, including:

- data loss and identity theft;
- unexpected or unapproved data collection;
- unexpected or unapproved data sharing and use; and
- nuisance contacts.

4.76 Respondents also identified some other risks to consumers, including:

- the potential for the discriminatory use of data; and
- the potential for detriment through loss of trust and self-exclusion.

4.77 Just as it is hard to quantify the value or benefits of data use (see **paragraph 2.114)**, it would be hard to quantify these harms and risks, and we did not

[192] TRUSTe, *Privacy and IOT 2015*, January 2015.
[193] European Commission, *Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union*, June 2011.
[194] Deloitte, *Data Nation 2014 – Putting customers first*, November 2014.

seek to in this CFI. However, we consider the most cited sources of consumer harm in more detail below.

Data loss and identity theft

4.78 Although we did not address data storage and protection for this study, it is clear that fears about companies losing personal data or being hacked are a significant concern for consumers and, often their primary worry. The results of an ICO survey in 2013 suggest that more might be done in this regard, finding that 65% of private sector organisations surveyed knew of the obligation to keep personal data secure.[195]

4.79 Data breaches may have detrimental impacts on consumers. For instance, in 2011 the Sony PlayStation Network Platform was hacked, compromising millions of consumers' personal information and leading to a fine from ICO of £250,000.[196]

4.80 Some data loss may entail identity fraud. In 2015, ICO fined Staysure, an online holiday insurance company, £175,000 after IT security failings allowed hackers to access customer records and more than 5,000 customers had their credit cards used by fraudsters.[197] CIFAS, the UK's Fraud Prevention Service, reported in 2014 that the abuse of people's identity details accounted for over 60% of all fraud in 2013 with over 129,500 victims of identity-related crimes.[198]

4.81 Overall, in 2013/14, ICO investigated a record 1,755 data protection cases (an increase of 385, or 28% on the previous year).[199] At the time of writing, the most recent statistics for the last quarter on reported cases suggest that theft and loss of data as well as hacking accounted for 36% of breaches.[200] Many incidents however were in the local government and health sectors and involved, in particular, the erroneous disclosure of personal data.

4.82 High-profile examples of firms' personal data losses and hacking are likely to undermine consumer confidence. Deloitte (2014), however, suggested that perceptions of data breaches might be skewed by media coverage. For instance, it said that only 1% of data breaches reported to ICO between April 2013 and March 2014 originated from retailers, but that this sector was mentioned in 35% of news stories about data breaches in that period.[201] It should however be noted that breach reporting is not currently mandatory in

---

[195] ICO, *Annual Track 2013 Practitioners*, June 2013. Responses were unprompted.
[196] ICO, *Sony fined £250,000 after millions of UK gamers' details compromised*, January 2013.
[197] ICO, *ICO fines insurance firm after hacked card details used for fraud*, February 2015.
[198] CIFAS, *Fraudscape – Depicting the UK's fraud landscape*, March 2014.
[199] ICO, *Annual Report and Financial Statements 2013-14*, July 2014.
[200] ICO, *Data breach trends*, April 2015.
[201] Deloitte, *Data Nation 2014 – Putting customers first*, November 2014.

law (except in relation to personal data breaches by communication service providers[202] under PECR). However, there are some information governance requirements placed upon public bodies to report breaches to ICO which is likely to account for the relatively high number of public sector breaches reported to ICO.[203]

4.83 While data loss and theft can lead to real harm, survey evidence suggests that a minority of people consider they have experienced it directly.[204] For example:

- 49% of UK respondents to the 2011 EC survey had heard about data losses and identity theft from the media and internet in the previous year. Fewer had direct experience of the issues in that period: 7% said it had affected a member of their family and 5% had been directly affected;[205] and

- Consumer Focus (2012) reported that 11% of respondents said they were aware of a loss or breach of their data by a company. Most had been informed by the company or institution, with the remainder finding out through the media.[206]

4.84 Some firms and trade bodies responding to our CFI suggested that businesses recognised significant reputational risks from failing to protect their customers' data and this alone encouraged them to take action.

Unexpected or unapproved data collection

4.85 A number of respondents to our CFI considered that data was increasingly being *taken* from consumers without them realising. **Chapter 2** noted that the extent of data collection seems likely to accelerate, with new technologies enabling firms passively to collect data.

4.86 We also noted in **paragraphs 4.14 to 4.15** that many consumers are unaware of passive data collection. However, there is some evidence that where they *are* aware, consumers are uneasy about it. For instance:

- CCP (2011) reported that respondents had reservations about companies collecting information using the methods suggested to them (mobile phone apps, cookies, social networking and registration opt in/out requests). For

---

[202] Such as Internet Service Providers (ISPs) and telecoms companies.
[203] Further information about breach reporting to ICO may be found on ICO's webpages.
[204] It is possible that some data loss and theft goes unnoticed or unreported.
[205] European Commission, *Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union*, June 2011.
[206] Consumer Focus, *Consumer Focus Digital Behaviour Survey*, March 2012.

all cases, except when opting in/out of marketing material from the company itself, most people were 'never happy' for companies to collect information about them in these ways. 76% were never happy for companies to use mobile phone apps to collect location data and information on products or services they were interested in, while 74% were never happy for companies to use information from social network profiles to provide adverts or special offers;[207] and

- Boston Consulting Group (2012) suggested that consumers were more willing to share when they actively provided the information voluntarily (for instance on a form or to secure service delivery) than when it was acquired passively (for instance location data transmitted by their smartphone).[208]

4.87 There are enforcement cases that have involved firms misrepresenting data collection and uses. For instance, in 2008, OFT obtained undertakings under the CPRs in relation to a Dutch-based company (Sky Connection BV). This business placed advertisements in UK newspapers offering consumers a 'free' psychic forecast when the evidence showed that one of the purposes of the adverts was to obtain personal details for onward sale as a 'target list' for astrology/clairvoyance offers. The undertakings were sought partly on the basis that the overall presentation of the advertisement was likely to deceive recipients about the motives for the commercial practice.[209]

4.88 In 2013 and 2014, a number of media stories identified flashlight apps[210] for mobiles and tablets as examples of firms potentially accessing large amounts of data (including the users' calendars, location and photos) to sell to third party advertisers – in some cases without this being made sufficiently clear to consumers.[211] In 2013, the Federal Trade Commission (FTC) settled a case against the company behind Brightest Flashlight, prohibiting it from misrepresenting how consumers' information was collected and shared, requiring it to delete existing data, to provide just-in-time disclosure about its data collection and to request consumers' express consent.[212] It also settled a case against Snapchat for misrepresenting the extent to which it maintains the privacy, security, or confidentiality of users' information.[213] In August 2012, it

---

[207] CCP, *Online personal data: the consumer perspective*, May 2011.
[208] Boston Consulting Group, *The Value of our Digital Identity*, November 2012. Note that these findings were based on a survey in three European countries that did not include the UK (Netherlands, Germany and Poland).
[209] OFT, *OFT stops misleading psychic adverts*, November 2008.
[210] A 'flashlight app' is a software application which adjusts a device's screen backlight to high levels of intensity to provide a flashlight function similar to a torch.
[211] See for example: Wired, *The hidden privacy threat…of flashlight apps*, October 2014.
[212] See: FTC, *Android Flashlight App Developer Settles FTC Charges It Deceived Consumers*, December 2013.
[213] See: FTC, *FTC Approves Final Order Settling Charges Against Snapchat*, December 2014. Under the terms of the settlement, Snapchat is prohibited from misrepresenting the extent to which it maintains the privacy, security, or confidentiality of users' information. In addition, the company will be required to implement a

entered into a settlement with Facebook regarding charges that Facebook had misrepresented that information on Facebook would be private and then allowing it to be shared and made public.[214] Prior to the acquisition of WhatsApp by Facebook it also sent a letter in April 2014 reminding both firms that WhatsApp must continue to honour the privacy promises given to its customers regardless of the acquisition.[215]

4.89 Some surveys have found consumers consider that they have been asked for excessive amounts of information to be able to access a service. For example:

- EC (2011) reported that 41% of UK respondents said that they always or sometimes had to provide more personal information than necessary. Of these people, 80% were very or fairly concerned;[216] and
- in recent years, apps have become a particular focus in terms of the extent to which they might collect data. The 2014 GPEN global survey found that almost one in three apps appeared to request an excessive number of permissions to access additional personal information.[217]

4.90 In addition, consumers may take note of media stories about how data is being gathered reportedly without users of products or services being made aware. For instance:

- **'smart devices'** – recent press stories highlighted examples of Smart TVs with terms and conditions for use that allowed them to gather information on people's viewing and online browsing behaviour. In one case, TVs were reportedly 'listening' to conversations, although the company involved was reported as saying that the aim had been to assist its voice recognition facility.[218] Other reports suggested a 'smart doll' could be listening to children and sending recordings to third parties;[219] and

---

comprehensive privacy program that will be monitored by an independent privacy professional for the next 20 years.

[214] See FTC, *FTC Approves Final Settlement With Facebook*. The settlement required Facebook to give consumers clear and prominent notice and to obtain their express consent before sharing their information beyond their privacy settings; to maintain a comprehensive privacy program to protect consumers' information, and to obtain biennial privacy audits from an independent third party.

[215] See *FTC letter* dated 10 April 2014.

[216] European Commission, *Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union*, June 2011.

[217] ICO, *Global survey finds 85% of mobile apps fail to provide basic privacy information*, September 2014.

[218] See for instance: BBC News, *Not in front of the telly: Warning over 'listening' TV*, February 2015.

[219] See for instance: The Guardian, *Privacy fears over 'smart' Barbie that can listen to your kids*, March 2015.

- **wearable technology** – concerns have been raised about the extent to which wearers would be aware and able to control the use of their data.[220]

4.91 GOS (2014) noted how new technology could lead to more information being revealed than people might expect:

> '…As more and more data is aggregated it may reveal aspects of the individual, system or environment that may be unexpected or intended to remain private. For example, information extracted from a building's heating controls, lighting and sensors might reveal information about an individual, such as when they are in the building…'[221]

Unexpected or unapproved data sharing and use

4.92 Some studies have suggest that consumers have a general dislike of companies sharing their data – particularly where they might be identifiable. For instance:

- Boston Consulting Group (2012) found that 70% of survey respondents disapproved of organisations allowing third parties to use data that could be traced back to consumers, compared with 31% disapproving of organisations collecting data in order to deliver a product or service;[222]

- Deloitte (2013) reported that 10% of respondents were happy with organisations sharing personal data with another company. Only 22% of consumers were confident that companies did not sell their details to other companies without their knowledge; and 20% that companies always removed their identity when passing data to other organisations;[223] and

- Big Brother Watch (2015) reported that 15% of respondents considered it acceptable for firms to share anonymised online personal data with other companies.[224]

---

[220] See, for instance, *Article 29 Data Protection Working Party Opinion 8/2014 on the Recent Developments on the Internet of Things*, September 2014. This noted various concerns, including that users might be unable adequately to review data before its use; that data communications might take place automatically and without a user's awareness and that users may find it hard to control the subsequent use of the data, which could include detailed life and behavioural patterns. The Article 29 Data Protection Working Party was set up under the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. It has advisory status and acts independently.
[221] Government Office for Science, *The Internet of Things: making the most of the Second Digital Revolution - A report by the UK Government Chief Scientific Adviser*, December 2014.
[222] Boston Consulting Group, *The Value of our Digital Identity*, November 2012. Note that these findings were based on a survey in three European countries that did not include the UK (Netherlands, Germany and Poland).
[223] Deloitte, *Data Nation 2013 – Balancing growth and responsibility*, August 2013.
[224] Big Brother Watch, *UK Public Research - Online Privacy*, March 2015.

4.93 Much targeted advertising is supported by first parties sharing consumer data with third parties.[225] Consumers' apparent dislike of targeted advertising (**see paragraph 4.70**) may therefore relate to some extent to their concerns about data sharing between companies.

4.94 ICO (2015) also suggest that consumers' concerns about loss of control once they share their data are compounded by fear that inaccurate data is shared between firms and that it will be hard for them to resolve this.[226] The 2014 ICO Track found that 60% of respondents were concerned about organisations holding inaccurate or out-of-date data.[227]

4.95 However, consumers' concerns about how their data might be shared also appears to relate to fears that it might be misused. ESRC/ONS (2014) reported qualitative research that '…participants described receiving unwanted and annoying insurance and other marketing calls that they were convinced were the result of illegal data sharing or sales'.[228]

4.96 Recent press stories have claimed that sensitive pension information and medical details were available for sale[229] and have prompted ICO to launch an investigation.[230] This also illustrates how apparent activities can suddenly come to the fore, quickly raising awareness and concerns.

4.97 Likewise, recent ICO investigations have identified a number of examples of data being shared and traded in chains, raising potential concerns about how well they were protecting consumers' data. For example:

- in one investigation, ICO found that the firms involved had signed confidentiality agreements with data brokers that meant they were completely unaware that they were within a chain/cycle; and
- in another investigation a consumer credit lender was passing on details of applicants who did not meet their risk profile to other lenders via a lead generation firm. The contractual arrangement provided that 50% of net revenue from selling or marketing the data would be passed to the lender.

4.98 Multiple steps in the supply chain complicate the identification of sources, and raise compliance risks. They also make it hard for consumers to track how

---

[225] The data shared can be pseudonymous, to help with targeting consumers by their characteristics.
[226] ICO, *Data Protection Rights: What the public want and what the public want from Data Protection Authorities*, May 2015.
[227] ICO, *Annual Track*, September 2014.
[228] ESRC and ONS, *Dialogue on data: Exploring the public's views on using administrative data for research purposes*, March 2014.
[229] See for example: Daily Mail, *After Mail exposes trade in sensitive pension details...Now they are selling your health secrets*, March 2015.
[230] ICO, *ICO launches investigation into firms sharing sensitive data*, April 2015.

their information is being used. ICO, for instance, cited a case in which a complainant's data was traced back through a chain involving four companies.

4.99 Some respondents also identified a growth in sophisticated, real-time analytics occurring 'behind the scenes', about which they considered few consumers were likely to be aware. With advances in technology and storage, data has an increasingly long lifespan and some data is also available to some bodies instantaneously (such as browsing data).

4.100 Furthermore, some studies have suggested that even if data has been anonymised, it may be possible to link it to specific individuals by combining it with other available data. For example:

- in 2007, two researchers reported how they used combined anonymous movie ratings from 500,000 Netflix subscribers with data on the Internet Movie Database to identify the records of known users, including their apparent political preferences and other sensitive information;[231] and
- in 2013, researchers published their analysis of the data of 1.5 million mobile phone users in Belgium over 15 months. They found they could identify 95% of them using just four points of reference (eg Twitter posts mentioning location).[232]

Nuisance contacts

4.101 Another concern cited by CFI respondents and in consumer surveys is the potential misuse of consumer data to support the generation of unsolicited and unwanted calls, texts and emails. In practice, many such 'nuisance contacts' may not relate to unexpected data collection and sharing. But it is likely that at least some results from these activities.

4.102 There is clear evidence that a large number of people suffer annoyance as a result of nuisance contacts. For example:

- Which? reported research in 2013 that 85% of people received an unsolicited call every month,[233] and Ofcom research (2015) found that more than four in five (86%) of participating UK adults with a landline phone reported experiencing a nuisance call in a four week period;[234] and

[231] Arvind Narayanan, Vitaly Shmatikov, *How To Break Anonymity of the Netflix Prize Dataset*, Cornell University Library, February 2008.
[232] Yves-Alexandre de Montjoye, César A. Hidalgo, Michel Verleysen and Vincent D. Blondel, *Unique in the Crowd: The privacy bounds of human mobility*, March 2013.
[233] Which?, *Government must tackle nuisance calls and texts*, June 2013.
[234] Ofcom, *Landline Nuisance Calls Panel Wave 3 (January to February 2015)*, April 2015.

- ICO reports regularly on concerns people raise with it about nuisance calls and messages. At the time of writing, in the first four months of 2015, it had recorded 51,302 concerns about marketing calls and texts (with accident claims and PPI-related contacts accounting for about one-third in total).[235] The Nuisance Calls and Texts Task force noted that consumers' reported complaints were likely to represent a 'fraction of the number of unwanted calls and texts received'.[236]

4.103 While the Task Force reported a lack of hard evidence about the extent to which businesses were deliberately flouting the law,[237] or simply unclear about best practice, it believed that the companies making calls may often be lead generators who go on to sell any information they obtain.

4.104 Some nuisance contacts are, in fact, scams – intended to con people into handing over money or providing more personal details. We have not covered this specific issue in our report, although we note that it is a further potential source of detriment.

The potential for the discriminatory use of data

4.105 Another potential source of harm identified by some respondents was for firms to use consumers' data for discriminatory purposes. Two forms of discrimination were most mentioned – price discrimination and discrimination on the basis of consumers' profiles (in particular their potential vulnerability). We consider price discrimination in **Chapter 3**, and address briefly below the issue of profiling.

4.106 Some firms and trade bodies responding to our CFI suggested that better use of consumer data helped them to avoid targeting vulnerable groups – for instance, more granular data meant that they would not send adverts inappropriately to minors or vulnerable consumers.

4.107 However, some respondents also suggested that if firms are able to identify consumers' characteristics, they might be able to discriminate against them on the basis of their willingness to pay, but also for their gender, race and sexual orientation, or to target the most vulnerable consumers.

4.108 One CFI respondent noted a 2013 study in the US that examined a dataset of over 58,000 volunteers who provided their Facebook Likes, to develop a

---

[235] ICO, *Nuisance calls and messages*, accessed on 6 June 2015.
[236] The Nuisance Calls and Texts Task Force on Consent and Lead Generation, *Report of the Nuisance Calls and Texts Task Force on Consent and Lead Generation* (December 2014). The Task Force was convened by Which? at the request of the Department of Culture, Media and Sport (DCMS), following the publication of the DCMS Nuisance Calls Action Plan in March 2014.
[237] In this case, the relevant legislation is PECR.

model that predicted individuals' psycho-demographic profiles. This model correctly discriminated '…between homosexual and heterosexual men in 88% of cases, African Americans and Caucasian Americans in 95% of cases, and between Democrat and Republican in 85% of cases'.[238] The same respondent suggested that the use of big data analytics in the housing market might enable landlords to sift applicants.

4.109 We have not considered these issues in detail, but we note that there is again at least the potential for consumer trust to be eroded if there is a perception that data is used to discriminate in such ways.

The potential for detriment through loss of trust and self-exclusion

4.110 As we note above, it is difficult to be clear about the extent of harms that may arise from the manifestation of sources of concern such as data misuse. However, the most immediate effect may be in terms of negative impacts on consumer confidence and thus their willingness to share data.

4.111 As we noted in **paragraphs 4.46 to 4.47**, it seems that approximately 30% of consumers may be potentially unwilling to engage in sharing their data; and estimates of those only willing to do so on a case-by-case basis varied from 42% to 53%.

4.112 In **Chapter 2**, we set out some of the benefits for firms and consumers from the appropriate collection and use of consumers' data. Consumers (and firms) may effectively suffer detriment by missing out on these benefits if people decide to limit their information sharing, or not to share information at all because of a lack of trust in how their data is being collected and used.

Consumers' behaviour and the 'privacy paradox'

4.113 Despite their general concerns, it is clear from consumers' behaviour that many do in fact share their data with companies and this data is used for purposes such as service delivery and improvement, as well as targeted advertising. As ICO (2015) noted, '…Whilst in surveys and research the public generally state that they are concerned about how and why their personal data is being processed this is often in contrast to how the public actually behave in their daily lives'.[239]

---

[238] Michal Kosinskia, David Stillwella and Thore Graepelb, *Private traits and attributes are predictable from digital records of human behaviour*, February 2013.
[239] ICO, *Data Protection Rights: What the public want and what the public want from Data Protection Authorities*, May 2015.

4.114 This phenomenon has sometimes been called the 'privacy paradox' – that is, despite apparent high levels of concern about privacy risks, consumers often give up their privacy, sometimes for relatively low-level rewards.[240]

4.115 A number of reasons were suggested to us by respondents to our CFI, as well as in the literature, for this apparent inconsistency between attitudes and behaviour. These fell broadly into:

- research effects;
- behavioural responses to risk perceptions; and
- fatalism/acceptance that data sharing is inevitable.

Research effects

4.116 The 2014 Sciencewise report, drawing on work by Hallinan and Friedewald (2012),[241] noted how the discrepancy between consumers' attitudes and behaviour may reflect their lack of understanding of the data environment, making it hard to apply their concerns on a daily basis. Whilst they might therefore have general concerns, consumers were likely to put these to one side when faced with the specific and tangible nature of actual transactions.

4.117 Research itself could sometimes prompt responses from people that might not play out in real life. The Sciencewise report[242] pointed to analysis by Singleton and others (2007)[243] which highlighted how 'people will express concerns if questioned about 'concerns', but will readily trade these 'concerns' for health or other benefits, even altruistic ones. 'Real world' choices can be very different (and constrained) from those offered in opinion surveys where costs and trade-offs may not appear.'

4.118 There is some evidence that could support the suggestion that for many consumers, data concerns may not be at the forefront of their minds when transacting with companies. For example:

- qualitative research in 2013 for Ofcom found that consumers tended only to express concerns once prompted to think about the issues and 'overall

---

[240] See: The Nuisance Calls and Texts Task Force on Consent and Lead Generation, *Report of the Nuisance Calls and Texts Task Force on Consent and Lead Generation* (December 2014), for a more detailed explanation.
[241] Dara Hallinan and Michael Friedewald, Fraunhofer Institute for Systems and Innovation Research (ISI), *Public Perception of the Data Environment and Information Transactions: A Selected-Survey Analysis of the European Public's Views on the Data Environment and Data Transactions*, December 2012.
[242] Sciencewise, *Big Data - Public views on the collection, sharing and use of personal data by government and companies*, April 2014.
[243] Cambridge Health Informatics and General Medical Council, *Public and Professional attitudes to privacy of healthcare data - A Survey of the Literature*, November 2007.

there was little spontaneous thought or concern given to online data issues. Most of those who expressed concern did so only when their attention was drawn to it…';[244] and

- RSS (2014) reported that, when prompted with examples, 72% of respondents agreed that they would stop using a company that failed to keep their data safe or lost it (see **paragraph 4.73**). But when asked unprompted what would make them stop using a company, its 'data usage' was cited by only 7% – well behind other factors such as service (26%) and price (24%).[245]

4.119 This suggests that surveys may in some cases, by prompting respondents, be registering levels of concern that are otherwise latent and only come to the surface when consumers are asked directly to consider the issues.

Consumers' behavioural response to risk perceptions

4.120 As described above, CFI respondents identified a number of potential risks to consumers, including identity theft, data loss, misuse of data and discrimination. Survey evidence supports the contention that consumers perceive a range of specific risks – particularly data loss and information sharing without their agreement.

4.121 For this high-level CFI, we did not conduct a comprehensive trawl for all potential examples of consumer harm and it is, in any case, very difficult to reach a firm view on the real nature, extent and impact of detriment.

4.122 Given the low levels of consumer awareness and understanding of how their data is collected and used at an individual level, it is possible that some detriment goes unnoticed or unreported. It is clear from media reports and ICO investigations that there are examples of rogues, but also legitimate firms, collecting and using consumers' data in ways that may raise concerns.

4.123 However, to some extent the 'privacy paradox' may reflect a combination of factors. For example:

- low levels of individual awareness of how data is used but, for most people, comparatively rare instances where they themselves can discern

[244] Ofcom, *Being online: an investigation of people's habits and attitudes*, June 2013.
[245] Royal Statistical Society (RSS), *Public attitudes to the use and sharing of their data*, July 2014. Base: Split sample, 1,009 GB adults aged 16-75.

real harm from the sharing of information, when considered in the context of how much information they are sharing day-to-day;[246]

- awareness that data may be used to market products to them; and media stories and investigations concerning loss and misuse of data, which create a persistent underlying sense of unease about data sharing; and

- a sense on the part of some consumers that they need to address how their data is used, coupled with uncertainty about how to do so.

4.124 Consumer Futures (2014), reporting the views of focus group participants about smart meters, found that while some consumers had very few concerns about data privacy (for example, being more interested in reducing their energy bills), for most consumers '…there was an underlying feeling of unease about data privacy, with a sense that they should be paying more attention to it, but they don't know how; it is a complex area and they do not know who to trust'.[247]

4.125 For this high-level CFI, we have not conducted research into consumer perceptions and behaviour, and more evidence may be needed. However, it is possible that, where they are aware and given a choice, many consumers decide on a case-by-case basis that the clear and present benefits they derive from sharing their data to access services outweigh the potential risks that may arise from doing so. They may therefore share data despite an ongoing sense of disquiet.

4.126 A review of the literature on information privacy by the Behavioural Insights Team at Which? concluded that consumers' consideration was 'biased towards low benefits instead of high risks'.[248] They suggested this reflected a number of factors including the following:

- **Information asymmetries** – consumers have far less information than companies about how their information will be used and even if they had more information would struggle to process it. Consequently, they use shortcuts to make decisions about privacy risks. For example, they may:

  - discount as unlikely events they find hard to imagine;

[246] Although some harms may go unnoticed or may be hard for consumers to relate to the collection and use of their data.
[247] Consumer Futures, *Smart and clear - Customer attitudes to communicating rights and choices on energy data privacy and access*, January 2014.
[248] The Nuisance Calls and Texts Task Force on Consent and Lead Generation, *Report of the Nuisance Calls and Texts Task Force on Consent and Lead Generation*, December 2014.

- trust privacy policies that look professional, regardless of their content; and
- ignore complex information, such as privacy policies.

- **Behavioural biases** – consumers may also be subject to inherent biases that drive how they react. For example, they may:
  - discount large long-term risks for smaller short-term gains;
  - prefer avoiding complex decisions; and
  - be more willing to agree to provide information if options are presented ambiguously.

Fatalism' or 'acceptance' that data sharing is unavoidable

4.127 In 2011, the EC reported found that 82% of UK respondents saw disclosing personal information as an increasing part of modern life and 65% thought that there was no alternative to disclosing personal information if they wanted to receive products or services.[249]

4.128 Some respondents to our CFI described this attitude as 'fatalism', whilst others considered it was simply 'acceptance' on the part of consumers that they needed to share their data to be able to transact. UK studies have confirmed that many consumers see some form of personal data sharing as inevitable. For instance:

- DMA (2012) found that 80% of consumers in Britain accept that the disclosure of personal information was a part of modern life. Almost two-thirds of people expected to provide personal information when shopping online and this figure rose to 70% among those aged 16-24;[250] and
- RSS (2014) reported that 68% agreed it was impossible to live in the modern world without giving personal information to companies and government.[251]

4.129 ICO (2015) reported focus group research that while consumers might take precautionary actions when providing data online, '…convenience often

[249] European Commission, *Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union*, June 2011.
[250] DMA, *Data Privacy: What the consumer really thinks*, June 2012.
[251] RSS, *Public attitudes to the use and sharing of their data*, July 2014.

outweighs the perceived risks…[and]…the public will continue to use online services seeing the potential problems as being a "necessary evil".'[252]

Implications

4.130 Perceived trust and familiarity are key factors in driving consumers' attitudes and survey evidence suggests that some sectors may have more to do than others in addressing apparent shortfalls in trust (see **paragraphs 4.57 to 4.60**).

4.131 However, consumers' views on the collection and use of their data, and their willingness to share it varies from individual to individual and case-by-case – depending on factors such as the type of data involved, who is collecting it and why. This suggests that efforts to address consumers' concerns need to be tailored to the circumstances and address specific concerns. This includes activities to raise their awareness and understanding, so that they can make informed decisions about whether and how to engage with firms and provide challenge – which in turn may drive up standards by acting as a spur to firms to compete more on privacy protection.

4.132 In terms of the potential for consumer harm, the detrimental implications of a data loss or breach (including resolving any subsequent misuse of their data), may be substantial for the individuals involved. Likewise, unapproved sharing of data is clearly a source of consumer concern and nuisance contacts are a source of substantial annoyance.

4.133 However, it is hard to scale the extent of these and the harms resulting against the total volume of information flows. For firms, the most significant implications could instead relate to the threat these fears and concerns represent to consumer confidence. Some surveys suggest that consumers might refuse or cease to transact with firms that they perceive are failing to protect their interests. These apparent consumer responses, if they persist or become more widespread, could have important implications for firms – making it harder to build and maintain a customer base, or make strategic decisions.

4.134 As we note, despite their concerns, consumers are sharing data in increasing volumes (the 'privacy paradox'). However, there is a risk that this could generate a false sense of security in terms of whether consumers will continue to share data in the future.

---

[252] ICO, *Data Protection Rights: What the public want and what the public want from Data Protection Authorities*, May 2015.

4.135 In particular, a number of CFI respondents suggested that fast-evolving technologies could, over the next few years, see a rapid growth in seamless data collection across many aspects of peoples' daily lives. As we noted in **Chapter 2**, IoT will enable large numbers of previously unconnected devices to communicate and share data with one another, with potentially little or no human intervention.[253] Such developments could both accelerate the volume of data use, while aggravating the difficulties consumers face in their awareness, understanding and control over it.

4.136 Currently, consumers seem more aware of active than passive data collection and many appear uncomfortable about passive collection when they are aware of it. The growing profile of IoT, and developments such as the roll out of smart meters may raise consumer awareness of how their data is being collected and shared.

4.137 Consumer trust appears already to be fragile. If attitudes shift as a result of a rapid evolution in data collection and sharing, this could lead to behavioural changes that hinder consumers' willingness to engage with new developments and act as a potential barrier to investment and innovation. It may also prompt further calls for consumer empowerment. We consider the current position on consumer consent and control in the next section and some of the regulatory activities in this area in **Chapter 5**.

Section C: Consumer consent and control

4.138 It seems clear from the evidence reported above that many consumers lack awareness of how their data is used and have latent or overt concerns about sharing their data, although most still do so.

4.139 Some firms responding to our CFI suggested a range of factors incentivised them to protect consumers and that protections were in place. For instance:

- reputational risk meant it was in their best interests to ensure that consumers felt comfortable and confident sharing data with them;
- the contractual arrangements they had with third parties ensured these parties met all legal requirements and would protect consumers' data;
- the cookie warnings, Terms and Conditions and Privacy Notices presented to consumers – which some chose to opt out from; and

[253] Ofcom, *Promoting investment and innovation in the Internet of Things: Summary of responses and next steps*, January 2015.

- the information they gave consumers about how to protect their privacy.

4.140 However, many respondents raised concerns about consumers' ability to give informed consent, as well as the extent to which they can exercise control over first and third parties' use of their information. We address these issues in more detail below.

Consumer consent

4.141 Other than self-exclusion from data sharing activities altogether, consumers' primary means of controlling the use of their data is through their decision whether to consent to share their information when asked – for instance, whether to agree or not to:

- the Terms and Conditions (T&Cs) presented to them;
- companies' Privacy Statements;
- use of cookies, when asked by 'cookie notices' on websites they visit (although consumers' agreement is assumed if they continue to use the site without actively responding to these notices); and
- the data sharing options set out when installing or using apps on their mobile phones and tablets.

4.142 Many respondents to our CFI, representing both firms and consumers, were critical of the current arrangements for securing consent. Principal concerns raised by respondents, as well as in the literature, include that they:

- were designed to promote businesses' rather than consumers' best interests;
- were unclear about under what circumstances consumers' data would be shared and with whom (for instance referring simply to 'trusted third parties'), making it hard for consumers to know to what onward use of their data they were consenting;
- were too lengthy and complex and seldom read (especially on mobiles);
- lacked standardised formats – varying from firm-to-firm, making them harder quickly to consider;
- adopted inconsistent means of requiring consent – some requiring consumers to opt-in to some marketing processes but to opt-out of others;

- change over time – sometimes often, making it harder for consumers' to keep track of what they have agreed to; and

- typically provided consumers with just a binary, 'take it or leave it' option.

4.143 A number of respondents cited media stories that the terms and conditions of many companies exceeded famous literary works such as Hamlet and Macbeth.[254] Some cited stories about an internet site that included a clause in which the consumer agreed to hand over their soul, to which 88% of people had reportedly agreed.[255] Deloitte (2013) reported that on average it took 25 minutes to read a privacy policy and that if an internet user read the privacy policies of all new websites they visited in a year it would take 31 hours.[256]

4.144 Surveys and studies we saw broadly support the contention that few consumers read and understand terms and conditions or privacy statements.[257] For instance:

- in the 2011 EC survey, 58% of UK consumers said that they read sites' privacy statements. However, across the EU as whole, only 34% had read and understood them with the remainder (24%) not fully understanding them. Across the EU, respondents who did not read T&Cs said that this was because it was sufficient for them to see that websites had a privacy policy (41%); around a quarter believed the law would protect them in any case (27%), or conversely, that the websites would not honour the privacy statements anyway (24%);[258]

- Consumer Focus (2012) found that 32% of consumers claimed they always read the T&Cs carefully before proceeding, with 53% saying they rarely read them and 14% saying they never did so. Key reasons for not reading them included their length and clarity. Of those consumers who said they always read T&Cs, only 18% mentioned as a reason that they wanted to understand how their data and related information was used by the product/service provider;[259] and

- Deloitte (2014) reported that 47% of adult internet users in Britain said that they always or fairly often agreed to T&Cs and/or privacy polices of online services without reading them. Furthermore, only 22% of those who

---

[254] See for example: BBC News, *Is small print in online contracts enforceable?*, June 2013.
[255] See for example: The Telegraph, *Gamestation collects customers' souls in April Fools gag*, April 2010.
[256] Deloitte, *Data Nation 2013 – Balancing growth and responsibility*, August 2013.
[257] Survey evidence on this topic may be subject to response bias.
[258] European Commission, *Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union*, June 2011.
[259] Consumer Focus, *Consumer Focus Digital Behaviour Survey*, March 2012.

read them thought that privacy policies were clear about how companies intended to use their data.[260]

4.145 Consumers may be further hampered by incomplete application of the requirements by firms. In 2013 ICO, together with 19 other Data Protection Authorities, participated in a GPEN sweep of 2,186 privacy notices. This international sweep found that 23% of the sites had no privacy policy at all, and of those that did, a third were considered to be difficult to read, and many were not tailored to the website. Most UK sites had a privacy policy that was easy to find and gave a fairly clear indication of what personal data was being collected about customers and why they were using this information. However they generally were not clear on how long personal data would be retained for or if it would be transferred internationally.[261]

4.146 The use of different types of devices may also have implications for the ease with which consumers can give their consent. In particular, mobile devices present particular problems for providing clear advice to consumers. A 2014 global survey by GPEN reported by ICO, examined over 1,200 mobile apps and found that 43% 'failed to tailor privacy communications to the small screen, either by providing information in too small print, or by hiding the information in lengthy privacy policies that required scrolling or clicking through multiple pages'.[262]

4.147 Research suggests that consumers want more transparency and clearer explanations of how their data will be used before they consent to its collection. There is also some evidence that consumers might want different types of consent for different types of circumstances. For example:

- Consumer Focus (2012) presented consumers who were aware of online registration with possible alternative types of T&Cs, to find out which they thought might work better. They found that 47% wanted T&Cs to be in plain English and no longer than two pages; and 40% wanted a standard set of T&Cs developed for all consumers by an independent body;[263]

- Ofcom 2013 noted that '…Participants said that transparency was important: they wanted their consent to be sought before their details were sold to third parties, or at least to be informed of this. They felt that they ought to have ownership over their personal information...';[264] and

---

[260] Deloitte, *Data Nation 2014 – Putting customers first*, November 2014.
[261] ICO blog, *Global privacy study gives international view*, August 2013.
[262] ICO, *Global survey finds 85% of mobile apps fail to provide basic privacy information*, September 2014.
[263] Consumer Focus, *Consumer Focus Digital Behaviour Survey*, March 2012.
[264] Ofcom, B*eing online: an investigation of people's habits and attitudes*, June 2013.

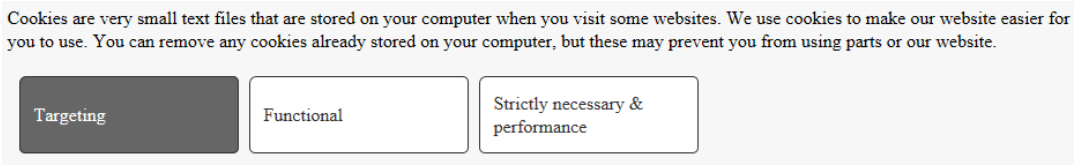
- Boston Consulting Group (2012) reported that for some less sensitive data, up to 69% of respondents considered opt-out, or even assumed consent, appropriate. But for more sensitive data such as credit card or financial information, 83% thought an opt-in mechanism should be required.[265]

4.148 Some respondents to our CFI were critical of the 'cookie law', which requires sites to explain to consumers how cookies are used and for consumers to give informed consent to store non-essential cookies. They considered that it had failed to improve consumers' awareness and control of their data use. Certainly, there was some survey evidence from Deloitte (2013) that most people (57%) either ignored cookie banners or had not noticed them.[266]

4.149 In terms of possible solutions, ICO has advocated the use of privacy by design principles, in combination with Privacy Impact Assessments, to ensure that privacy protections are 'built in' to business models.[267] A number of CFI respondents suggested that consent mechanisms needed to be more tailored to the context and the consumers' wishes. In doing so, some pointed to the diverse range of consumer perceptions and attitudes that we have also identified in this chapter. As we noted in **Box 2.6**, cookies vary in terms of their function and how necessary they are to the consumers' experience when accessing sites. Some examples of graduated cookie notices were presented as illustrative of how consumers might be given more flexibility (**Box 4.7**).

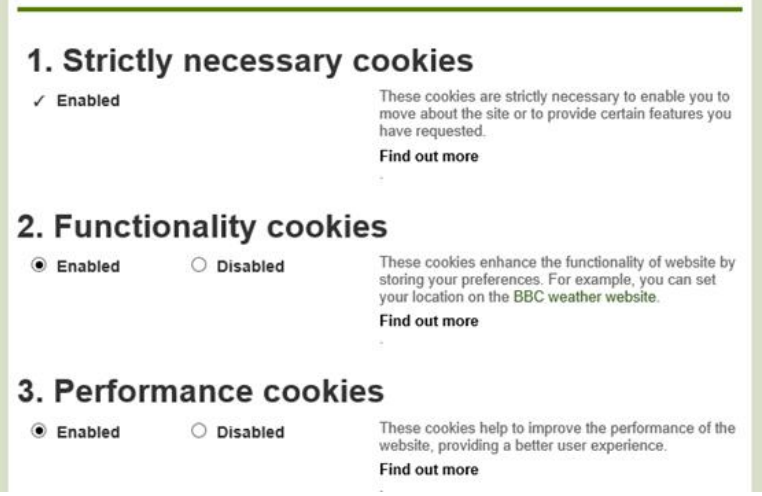
Box 4.7: Examples of graduated consent notices for cookies

BT for instance provides visitors to its site with three options for cookie settings ('targeting'; 'functional'; 'strictly necessary and performance'), along with a list and explanation of the cookies involved.



[265] Boston Consulting Group, *The Value of our Digital Identity*, November 2012. Note that these findings were based on a survey in three European countries that did not include the UK (Netherlands, Germany and Poland).
[266] Deloitte, *Data Nation 2013 – Balancing growth and responsibility*, August 2013.
[267] ICO, *Privacy by design*. See also paragraph 103ff of ICO, *Big data and data protection*, July 2014.

Similarly, the BBC offers visitors three settings: ‘strictly necessary’; ‘functionality’ and ‘performance’.



4.150 Mobile operating systems (OS) differ in how they present consent options to consumers when asking them to agree to the permissions required by an app. A device using Google’s Android OS presents permissions at the point of the download of an app as an all-inclusive ‘take it or leave it’ list – that is, users are not able to select or deselect items on the list. In contrast, a device using Apple’s operating system, iOS, asks users to give their permission at the point at which an app wants to access their personal data via just-in-time consent requests and gives users a choice to allow access to each of the different items requested individually.[268] Users can also manage their settings at the OS level (for instance in terms of whether location tracking is turned on or off).

4.151 Some respondents suggested that the principle of graduated consent might be extended more generally to requests to approve T&Cs and Privacy Statements. Consumers might, for instance, be offered different service options in return for differing levels of data sharing.

4.152 Others’ suggested improvements have included providing clear and simple explanations at the top of each request for consumers to agree, so that they can easily see what they are signing up to.

[268] Google has announced plans to change its Android software app permissions for data sharing reportedly to be closer to that of Apple’s OS. See: The Guardian, *Google unveils Android 'M' software with focus on security and battery life*, May 2015.

4.153 Improving consent mechanisms could have important implications for consumers' willingness to share data, with consequent beneficial impacts for firms. For example:

- Consumer Focus (2012) reported that 72% of its survey respondents agreed that they would be more willing to share their information if the recipient was clear how it would be used and if permission could subsequently be withdrawn;[269] and
- Deloitte (2013), reported that some individuals were content for organisations to share their data with other organisations, where otherwise they wouldn't have been, provided they were informed of how their data would be used for their or the public benefit.[270]

Consumer control

4.154 Survey evidence suggests that consumers consider that responsibility for ensuring the security of their data is shared between themselves and the companies they deal with. For instance:

- CCP (2011) reported that while 21% felt people should have sole responsibility for their own information, many felt that responsibility should be shared;[271]
- the 2011 EC Study found that 55% of UK social network site users thought they were responsible for ensuring their information was collected, stored and exchanged safely by social networking sites; and 34% thought the sites themselves were responsible;[272] and
- more recently, however, the 2015 TRUSTe privacy survey reported that 79% of respondents believed they were primarily responsible for protecting their privacy online.[273]

4.155 As well as adopting strategies such as limiting their use of the internet or providing only minimal information, consumers have various tools and options available to them to control their security and privacy, including what data they share, how their data is used as well as what communications and information they receive (**Box 4.8**).

---

[269] Consumer Focus, *Consumer Focus Digital Behaviour Survey*, March 2012.
[270] Deloitte, *Data Nation 2013 – Balancing growth and responsibility*, August 2013.
[271] CCP, *Online personal data: the consumer perspective*, May 2011.
[272] European Commission, *Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union*, June 2011.
[273] TRUSTe, *2015 TRUSTe UK Consumer Confidence Index*, January 2015.

Box 4.8: Tools to help consumers exercise control[274]

In terms of managing what information they share and its use, the options include:

- Changing browser settings (for instance for Microsoft Internet Explorer), which enable consumers to set their security and privacy preferences – including for cookies and pop-ups and tracking. This includes features such as Do Not Track (DNT), which asks web applications not to track users' movements.
- Using the dashboards of service providers such as Google and Facebook to decide what privacy settings they wish to apply by logging in to their accounts.
- Using tools that enable them to opt out of OBA (eg Your Online Choices, and by clicking on the AdChoices logo).
- Using online tracking services that can help consumers understand what companies are tracking them and allow them to decide which ones to allow and which to block (eg Ghostery, Disconnect).
- Using services that can help consumers manage their social media privacy settings (eg Privacyfix).
- Using services that are designed to collect no information from them (eg search engine DuckDuckGo) or that help consumers to encrypt their communications (eg Mailpile).
- Making subject access requests – consumers have the right to see a copy of the information an organisation holds about them as well as other rights of access.[275]

In terms of managing what communications they receive, the options consumers can use include:

- Services that enable consumers to filter out spam (unsolicited and undesired emails), such as Mailwasher.
- Services that enable ad-blocking, such as Adblock Plus.
- Services that enable consumers to record that they do not want to receive unsolicited sales or marketing calls (Telephone Preference Service, TPS), or direct mailing (Mailing Preference Service, MPS).

---

[274] This list and the examples provided are not intended to be comprehensive or to endorse particular services. There are many tools available, including mobile apps, intended to help consumers manage their security and privacy.

[275] Section 7 of the Data Protection Act 1998 allows individuals who make a written request and pay a fee to be told whether any personal data is being processed; given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people; be given a copy of the information comprising the data; and given details of the source of the data (where this is available). Individuals can also request information about the reasoning behind any automated decisions. See: ICO, *Subject access request*.

4.156 Although various options are available to help consumers take some control over the collection and use of their data, evidence differs on the extent to which they do so (**Box 4.9**). Broadly, however, it seems that consumers are aware of the most immediate controls available to them and do react when prompted – for instance, opting out of marketing. Many are also aware of and implement key self-protection techniques such as providing the minimum information when asked, checking that online transactions are protected and controlling unwanted emails (spam).

4.157 In aggregate, it seems that most consumers have taken at least some action to address their security and privacy. For instance, the TRUSTe consumer confidence index for 2015 suggests that 88% of consumers took some steps to protect their privacy in the last year – in particular, deleting cookies (58%) or changing privacy settings (48%).[276]

4.158 Citizens Advice (2015) suggested that consumers' awareness of tools could be growing and that this might in part reflect the 'Snowden effect', as well as software companies increasingly seeing privacy as a brand asset.[277]

4.159 In particular, the evidence suggests that a relatively high proportion of consumers know about and use privacy settings on social media. Social media may therefore be having an educative effect: raising consumers' awareness generally of the use of their data.

4.160 However, it also appears that consumers are less likely to adopt some of the more active options available to them – such as using sites' own 'dashboards' to control their privacy settings, or asking companies to explain what data they hold on them. A large proportion of consumers therefore do not take more active control of their data in terms of restricting its collection or use, or following up how it is used.

[276] TRUSTe, *2015 TRUSTe UK Consumer Confidence Index*, January 2015.
[277] Citizens Advice, *Personal data empowerment – Time for a Fairer Data Deal?*, April 2015.

Box 4.9: Consumers' use of controls

CCP (2011) suggested that consumers had high levels of awareness of many of the methods by which they might control use of their data (such as opting out of receiving marketing, and data sharing with partner companies) and that most who were aware of these techniques used them regularly. For instance, 85% of those with a social networking site profile were aware of the ability to change privacy settings and 82% of these said they did so regularly.[278]

The 2011 EC Study found that UK consumers used methods such as anti-spy software (63%), tools and strategies to limit unwanted emails (52%), deleting cookies (45%) and checking that the transaction was protected (44%). Less than one-in ten (9%) said they did none of the actions presented to them.[279]

Consumer Focus (2012) found that only 13% of consumers had used services' control panels or dashboards. Most were unaware that such tools existed (28%) or did not know how to use them (38%). A further fifth (21%) were aware but did not use them. Consumer Focus also asked consumers whether they had ever made a subject access right request to ask to see all the personal information an organisation held about them and if necessary, ask for it to be corrected or deleted. More than two-fifths (43%) were unaware they had this right and only 6% had ever made such a request.[280]

RSS (2014) reported that while 'easy' privacy precautions were fairly common, few respondents had been proactive or done something which involved a loss of service. For example, although 78% had opted out of receiving marketing from websites and 52% had signed up for the Telephone Preference Service, only 46% had changed the default settings on their computer to increase their privacy; and 15% had stopped using Facebook. Despite high public support for more transparency, only 5% had asked a government department, public service or private company what information they held about them.[281]

TRUSTe (2015) reported that while 58% of people had deleted cookies and 48% had changed their privacy settings, fewer (30%) had turned off location tracking and 13% had opted out of behavioural advertising.[282]

ICO (2015) reported that while focus group participants said they were aware of control settings on social media sites, these controls were seen as confusing and time consuming because sites often changed how they worked.[283]

---

[278] CCP, *Online personal data: the consumer perspective*, May 2011.
[279] European Commission, *Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union*, June 2011.
[280] Consumer Focus, *Consumer Focus Digital Behaviour Survey*, March 2012.
[281] Royal Statistical Society, *Public attitudes to the use and sharing of their data*, July 2014.
[282] TRUSTe, *2015 TRUSTe UK Consumer Confidence Index*, January 2015.
[283] ICO, *Data Protection Rights: What the public want and what the public want from Data Protection Authorities*, May 2015.

4.161 We noted in **Chapter 2** that some respondents to our CFI suggested that personal information management services (PIMS) represented a potentially significant development – enabling consumers to manage the storage and control of their data from one location.

4.162 There is some evidence that many consumers support the concept of managing their own data. For example, 85% of respondents to the 2012 DMA survey agreed that they would prefer to hold their own personal information and exchange it for services when they choose.[284] There is also evidence that some consumers may find the prospect of managing their data daunting: the 2014 RSS survey found that 40% agreed that it was too difficult for them to keep control of all their personal data and that it should be the government's job to prevent anyone misusing it.[285]

4.163 While we were told that the number of organisations offering PIM services is growing, consumers do not appear to have taken them up substantially to date. As we note above, some respondents suggested that new developments such as IoT and the roll out of smart meters could spur greater consumer awareness of these services and their take up.

4.164 Many CFI respondents suggested that consumers felt a lack control over the collection and use of their data. As we noted in **paragraph 4.66**, the survey evidence we have seen would appear to support this. Perhaps unsurprisingly, a high percentage of survey respondents apparently want more control. For instance:

- Consumer Focus (2012) reported that 84% of respondents agreed that they should be able to control what information organisations collected about them and what this information was used for;[286]
- DMA (2012) likewise found that almost 90% of consumers in the UK would like more control over the personal information they share with companies and how it is stored;[287]
- RSS (2014) found a high levels of public support for transparency, with most agreeing (72%) that they 'would really like to know what information private companies know about me' (only 5% disagreed);[288] and

[284] DMA, *Data Privacy: What the consumer really thinks*, June 2012.
[285] RSS, *Public attitudes to the use and sharing of their data*, July 2014.
[286] Consumer Focus, *Consumer Focus Digital Behaviour Survey*, March 2012.
[287] DMA, *Data Privacy: What the consumer really thinks*, June 2012.
[288] RSS, *Public attitudes to the use and sharing of their data*, July 2014.

- TRUSTe (2015) reported that ways to increase trust included giving consumers clear procedures for removing personal information (54%), easy opportunities to stop contacts by third parties (39%), and to give consumers information on how their personal information is being used (35%).[289]

4.165 A feeling of insufficient control over the use of their information and lack of understanding about its use may explain in part why some people choose not to share their data, to limit their data sharing with companies, or even to lie when providing information (see **paragraphs 4.73 to 4.74**).

4.166 As we note above, there are some tools that consumers can use to help manage how their data is used, although we have not considered the level of protection these tools provide individually or in aggregate, or their effectiveness.[290]

4.167 There also a number of new technological developments, including the Internet of Things (IoT), that could lead to a further and rapid increase in data gathering and sharing and where consumers may have limited or even no awareness that this is happening.

4.168 In some cases, there may even be no human-machine interface. Consumers already have limited engagement in terms of reading privacy policies and these developments could add a layer of complexity, further hindering consumers' engagement, informed consent and ongoing awareness of how their data is used. Some CFI respondents considered that this was part of an apparent power shift from consumers to firms collecting and using data without consumer knowledge/consent.

4.169 Some respondents to our CFI considered that consumer awareness, understanding and acceptance of the use of their data would grow as organisations become more transparent. They pointed to a range of activities to raise consumer awareness, including, the following:

- **Improvements to privacy notices**. For instance, Facebook and Skype were cited as examples of new privacy policies which used graphics and clearer language to explain how they use data. Also, many apps provide

[289] TRUSTe, *2015 TRUSTe UK Consumer Confidence Index*, January 2015.
[290] For example, we were told by the IAB that the 'opting out' of OBA using AdChoices is itself by means of a cookie. This seems likely to mean that consumers who regularly clear their cookies (for example to maintain privacy) are then opted back in. This could defeat the object of the opt-out, although we note that the site also offers a browser extension to provide persistency when a user exercises their choices.

contextual or just-in-time notices and reminders about data-sharing practices.

- **Websites with consumer education or transparency purposes**. Many companies are building websites to educate consumers about how their data is used, or have taken other actions intended to provide consumers with greater control over their data. For example:
  - Facebook's data policy website, explaining how data is collected, shared, and how users can manage or delete their data;
  - Microsoft's Your Privacy is Our Priority;
  - Google's recently updated privacy controls on My Account;
  - a large data broker, Acxiom, has enabled US consumers to see the data it held about them (aboutthedata.com); and
  - Barclays' Digital Driving Licence.

4.170 These developments are welcome, although some CFI respondents suggested that they were primarily for publicity purposes and more was needed. There have also been some industry developments that may increase how much consumer data can be collected, such as Microsoft's decision to no longer enable Do Not Track (DNT) as the default state in Windows Express Settings (although users can still turn the feature on).[291]

4.171 It is important that efforts to improve business transparency, consumer awareness, consent and control are not concentrated in particular areas or parts of sectors but are comprehensive across all levels.

4.172 To raise consumers' awareness about the use of their data, however, firms themselves need to know their own obligations. It is therefore concerning that ICO's most recent survey of public and private sector organisations found that:

- only 10% of all private sector organisations surveyed knew that personal information should be processed for limited purposes (with only 5% of small firms aware); and

[291] Microsoft, *An update on Microsoft's approach to Do Not Track*, April 2015.

- only 25% of all private sector organisations surveyed knew that personal information should not be kept for longer than necessary (with only 15% of small firms aware).[292]

4.173 This suggests that business awareness of obligations needs to be addressed, in the same way that consumers' awareness of how they might use tools to protect themselves.

4.174 Just as improving consent mechanisms for consumers could increase their willingness to share data, so there is evidence that they are likely to feel more comfortable sharing data if they consider that they have more control. For example:

- Boston Consulting Group (2012) reported that consumers who are able to manage and protect their privacy are up to 52% more willing to share information than those who are not;[293] and

- Deloitte (2014) reported that if organisations made it easier to manage personal data, 49% of consumers say they are likely to use the data to make better decisions and 59% would update personal data held by a company to keep it up to date.[294]

Implications

4.175 There appears to be widespread concern about the effectiveness of the current consent mechanisms available for consumers. The evidence also suggests that many consumers do not actively or effectively engage with these mechanisms and even if they do, they cannot always be sure what they are consenting to.

4.176 Overall, it appears that consumers want more transparency and control over the collection and use of their data. Improving consent and control mechanisms for consumers could increase their willingness to share data, with subsequent beneficial implications for firms. Consumers need simple solutions that enable them to make informed choices, including to decide not to share their information.

4.177 There have been some positive developments in terms of tools to help consumers take control and industry efforts to raise awareness. However, the

---

[292] ICO, *Annual Track 2013 Practitioners*, June 2013. Responses were unprompted.
[293] Boston Consulting Group, *The Value of our Digital Identity*, November 2012. Note that these findings were based on a survey in three European countries that did not include the UK (Netherlands, Germany and Poland).
[294] Deloitte, *Data Nation 2014 – Putting customers first*, November 2014.

number of players and tools suggests the need for greater alignment of communication and approaches across industry.

4.178 While there are some signs that privacy is becoming more of a competitive focus, it does not appear currently to be a major element of most firms' offer to consumers. An increasing drive to raise standards in B2C relations could help ensure standards and protect consumer interests in B2B relations where their data is being shared.

4.179 Furthermore, while most consumers take some form of action to protect their security and privacy, many have not taken up some of the more sophisticated market-led solutions. This suggests that more action might be needed to raise their profile and to make them user-friendly. Developments such as IoT may further complicate consumers' ability to agree to, monitor and control their data use.

4.180 Improvements in consumer awareness, understanding, attitudes, consent and control are most likely to happen where they are driven across all relevant sectors at all levels and within a supportive regulatory framework. We consider in **Chapter 5** the role of regulation, as well as industry's self-regulatory initiatives in addressing these challenges.

5. The Regulatory Environment

Introduction

5.1 In **Chapter 2**, we describe the way that the collection and use of consumer data is regulated, including a number of self-regulation initiatives relevant to consumer data. In **Chapters 3** and **4** we set out the main concerns and potential harms that were raised with us from a competition and consumer perspective.

5.2 In this chapter, we describe how policy makers and authorities are thinking about these concerns, including proposals to change the data protection framework. We describe the inputs we received in response to our questions about regulation and set out our emerging thinking about how the regulation of consumer data should be shaped.

5.3 Before addressing the position in the UK, we consider international developments. This context is particularly relevant to the use of consumer data given that its collection and use can be global in nature.

The international environment

Europe and the Digital Single Market (DSM)

5.4 In May 2015, the European Commission launched proposals to create a Digital Single Market (DSM) involving a number of inter-related works-streams. A number of elements of the DSM relate to the collection and use of consumer data (**Box 5.1**).

Box 5.1: Digital Single Market and consumer data

Elements of the DSM relating to the collection and use of consumer data include the following:

- **Reinforcing trust and security in digital services and in the handling of personal data** – the European Commission announced plans to establish a public-private partnership on cyber-security and solutions for online security. The objective is to ensure that networks and the information they hold are adequately protected from risks such as data interception, fraud and identity theft. Under the same theme, the Commission committed to introducing new rules on data protection by the end of 2015. See **paragraph 5.5** onwards in this chapter for a discussion of the General Data Protection Regulation (GDPR).

- **A fit-for-purpose regulatory environment for platforms and intermediaries** – the EC described the growing role of online platforms in economic life, based on the amount of data they collect and the algorithms that they use to exploit this data. It suggested that some platforms may be able to control both access to online markets and the way in which those markets operate. It announced plans to launch a comprehensive assessment of the role of platforms, including in the sharing economy, and of online intermediaries. One of the questions the assessment intends to address is the way platforms use the data they collect.
- **Building a data economy** – the Commission described the importance of data, in particular big data analysis and insights, to the future economy of the EU and described some of the barriers to its development including national requirements on data location and lack of clarity on the rights to process data. It announced plans to propose a free flow of data initiative in 2016 to break down these barriers.

Draft General Data Protection Regulation (GDPR)

5.5 The proposed new GDPR – which was first put forward by the Commission in January 2012[295] – is currently being negotiated by the European Parliament and the Council of the European Union.[296] Given the late stage of negotiation of the Regulation, we did not conduct our CFI with the intention of making recommendations about its final shape. However, we report here the comments made to us about its potential impact.

5.6 Instead of a single Directive, as currently,[297] it is intended to establish a new Regulation which applies directly across Europe.[298] The Commission's stated intention behind the new framework is to harmonise European laws in this area and to ensure that the regime adapts to the challenges brought about by globalisation and technological development (in particular, the scale and scope of data collection and use). There is no intention radically to change the objectives and principles underlying the existing regime but rather to harmonise and strengthen them to create legal and practical certainty for businesses and users and to build trust in the online environment as a driver

---

[295] European Commission, *Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, January 2012.
[296] On 15 June 2015, the Commission announced that the next phase of negotiations on the GDPR would start later in the month, with the final form of the text due to be agreed by the end of 2015. See: *Commission proposal on new data protection rules to boost EU Digital Single Market supported by Justice Ministers*, June 2015.
[297] A Regulation (unlike a Directive) would be directly binding on data controllers in all member states immediately upon adoption by the EU institutions, without the need for implementation at national level.
[298] It is proposed that there will be a corresponding Directive with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data.

of economic development. A key component is to put individuals in greater control of their own data, supported by strong enforcement.

5.7 There is considerable uncertainty about the final shape of the regulation, but it is clearly central to the development of markets which involve the commercial collection and use of consumer data. The most significant aspects of the original proposal are set out in **Box 5.2**.

Box 5.2: General Data Protection Regulation

Key aspects of the draft GDPR include:

- a **revised definition of personal data** which is broader than that currently used in the DPA;
- a **strengthening of the consent regime** when this is used as means to process personal data;
- a requirement for **transparent and easily accessible privacy policies** and to communicate information about processing of personal data in an intelligible form, using clear and plain language;
- a **wider territorial scope** to include the processing of personal data of EU subjects by a non-EU data controller;
- a right, with exceptions, **not be subject to automated personal profiling** (the creation of a 'profile' in order to take decisions about a person or analyse or predict personal preferences, behaviours and attitudes);
- a **right 'to be forgotten'**, namely a right of individuals to request that organisations delete personal data relating to them (for example social media businesses).
- a **right of data portability** enabling individuals to obtain a copy of the data held about them in a reusable, electronic format;
- a **requirement for data protection by design and by default** (data controllers must implement appropriate technical and organisational measures and procedures to comply with the Regulation); and
- **greater enforcement powers** including substantial fines.

5.8 Respondents agreed with the need for an effective, and well-enforced, data protection regime. It was put to us that that the new framework may have a positive or negative impact on competitive markets depending on its design. Advertising and marketing businesses, in particular, expressed concerns that, insofar as regulation may have the effect of limiting data collection, there is a

corresponding risk to innovation which ultimately harms consumers. This may be the case, we were told, if the regulatory framework is overly prescriptive in terms of its requirements or if its scope is too far reaching. For example, it was suggested that a too-broad definition of personal data combined with a requirement for explicit consent to process it would have a significant detrimental effect on the digital advertising industry. We heard that advertising funds much of the 'free' content online and that reduction in advertising funding may lead to reduced choice. We also heard that smaller businesses may find it difficult to implement some aspects of the new regime, potentially impacting their ability to compete with larger firms.

5.9 Some welcomed that the GDPR offers a harmonised approach to data protection and privacy issues which would ensure a level playing field across Europe and should, therefore, be swiftly adopted. One respondent thought that more research is needed on understanding social norms governing online privacy before making regulatory changes.

5.10 As noted above, the new regulation may address data portability. Article 15 of the original text stated that '…A user shall be able to request a copy of personal data being processed in a format usable by this person and be able to transmit it electronically to another processing system'. **Chapter 2** discusses existing moves in the UK to promote data portability, via the midata programme set up by the previous government.

5.11 Several respondents cited the role data portability could play in promoting competition between providers and increasing the ability of smaller and new providers to gain market share, especially in markets where brand reputation had been built up over time. Other respondents were concerned that a catch-all data portability provision might undermine incentives to invest in services related to the use and storage of consumer data.

European and international developments

5.12 There has been active debate by policy makers at a European level on the implications of increasing data collection. There has been discussion, initiated by the European Data Protection Supervisor (EDPS), about the need for privacy and competition authorities to work more closely in assessing the impacts of, for example, mergers that involve companies that collect and use consumer data.[299] We discuss competition issues and the relationship with

[299] See: *European Data Protection Supervisor – Preliminary Opinion – Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy*, March 2014.

privacy in **Chapter 3**. The Article 29 Data Protection Working Party[300] has also produced opinions on the data protection and privacy implications of the IoT, anonymisation and device fingerprinting.[301]

5.13 Enforcement activity undertaken against data loss/theft and misuse of data (including misleading business practices) has been described in **Chapter 4** (particularly **paragraphs 4.79-81, 4.87-88, 4.96-7**). International enforcement action has also been taken against businesses suspected of inadequate compliance with data protection law. Co-ordinated enforcement was taken by European Data Protection authorities in response to Google's decision to replace over 60 separate privacy policies into a single privacy policy.[302] Key criticisms were failure to obtain user consent, failure to specify how long data would be retained and combining all the data across all its services without a proper legal basis. Facebook has also been the target of enforcement authorities in relation to privacy policies.[303]

5.14 In December 2014, a number of privacy authorities signed an open letter to the operators of seven app marketplaces (Apple, Google, Samsung, Microsoft, Nokia, BlackBerry and Amazon.com) urging them to make links to privacy policies mandatory for apps that collect personal information.[304] The absence of privacy policies was a particular concern, together with the fact that a link to a privacy policy was not a mandatory requirement.

5.15 GPEN, of which ICO is a member, reported in May 2015 that it will assess how websites and mobile apps for children collect personal data and how they address the issue of parental consent to that data collection. Findings will be reported in the autumn of 2015.[305]

5.16 In the United States, the FTC has also taken an active interest in the collection and use of consumer data. The enforcement action it has taken in relation to deceptive business practices, notably against Brightest Flashlight and Snapchat has already been described (see **Chapter 4**). It has also undertaken an investigation into the role of data brokers, which, in May 2014, reported a fundamental lack of transparency about data broker industry

---

[300] The Article 29 Data Protection Working Party was set up under the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. It has advisory status and acts independently.
[301] EC, *Opinions and recommendations*.
[302] The Dutch Data Protection Authority found Google to be non-compliant with data protection law in November 2014 (but did not levy a fine). The Spanish Data Protection Authority fined Google €900,000 in December 2013 and the French Data Protection Authority fined Google €750,000 in January 2014. In January 2015, *Google signed a formal undertaking with the ICO* to improve the information it provides to people about how it collects personal data in the UK.
[303] For example, by the German consumer protection authority, the Verbraucherzentrale (VZBV), against Facebook in relation to alleged unfair terms, misleading advertising, and data-protection concerns.
[304] Office of the Privacy Commissioner of Canada, *Joint Open Letter to App Marketplaces*, 9 December 2014.
[305] Out-Law, *Children's websites and apps to be assessed by privacy watchdogs*, 12 May 2015.

practices. This has led to recommendations for legislative change in the USA to promote greater transparency and consumer access to data held by such brokers.[306] The Executive Office of the White House, in its report on Big Data and Privacy, has considered the policy implications of big data.[307] Noting both the considerable advantages big data may present, as well as privacy risks, among other recommendations, it advised that policy attention should focus more on the actual uses of big data and less on its collection and analysis – since the adverse harms to individuals materialise when the data is used rather than when it is collected.

Domestic regulatory activity

5.17 In **Chapter 2**, we set out the main UK regulations which may apply to businesses which make commercial use of consumer data. Many relevant authorities have some role in the oversight of consumer data use and have been active in recent years in responding to the growth and changes in consumer data collection and use. Here we describe the roles and responsibilities of these authorities and their key interests.

Relevant authorities

Information Commissioner's Office

5.18 ICO is the UK's independent authority responsible for promoting good practice and legal compliance in relation to data protection and the privacy of individuals. In this capacity, in addition to taking enforcement action, it has produced a large number of publications providing advice and guidance about the current application of the DPA and PECR. It has also looked forward to the challenges raised by business and technological advances, in particular mobile applications and big data.

5.19 Relevant ICO publications and guidance include:

- ICO Code of Practice and Guidance (July 2010), which explains how the DPA applies to the collection and use of personal data online and gives advice on good practice;[308]

[306] FTC, *Data Brokers*, May 2014. There have also been investigations launched by the Dutch data protection authority, and concerns by the Belgian data protection authority have been recorded.
[307] Executive Office of the President, President's Council of Advisors on Science and Technology, *Report to the President, Big data and Privacy: a technological perspective*, May 2014.
[308] ICO, *ICO Code of Practice and Guidance*, July 2010.

- Privacy notices code of practice (December 2010), intended to help businesses collect and use information appropriately by drafting clear and informative privacy notices;[309]

- Guidance on the use of cookies and similar technologies (May 2012), which focuses principally on the information and consent requirements under PECR; [310]

- Privacy in mobile apps (December 2013), which addresses the challenges presented by the collection and use of data in the mobile environment;[311] and

- Big data guidance and data protection (July 2014), which considers a number of scenarios where data protection issues may arise in big data analytics.[312]

5.20 In terms of enforcement, ICO takes action against breaches of the DPA and PECR. It has powers to take criminal prosecutions, issue fines up to £500,000 and seek enforcement notices, subject to resources and prioritisation.

5.21 Insofar as personal data has been misused for the purpose of cold-calling or spam text, it also takes the lead in tackling unsolicited live marketing calls, recorded marketing calls and marketing texts using its enforcement powers under PECR, and has issued a number of enforcement notices and fines.[313] It is a member of the London Action Plan (to which the CMA also belongs), an international initiative involving 27 countries, which is also focused on co-operative enforcement action against spam.[314] In addition Ofcom has a joint action plan with ICO to tackle nuisance calls and messages.[315] Examples of its enforcement activity in this area have been set out above and in **Chapter 4.**

Ofcom

5.22 Ofcom is the independent regulator and competition authority for the UK communications industries. Its principal duties are to further the interests of citizens in relation to communications matters and to further the interests of

---

[309] ICO, *Privacy notices code of practice*, December 2010.
[310] ICO, *Guidance on the rules of cookies and similar technologies*, May 2012.
[311] ICO, *Privacy in mobile apps*, December 2013. The guidance can also be applied to other devices using similar app technology, for instance living-room devices such as smart TVs or games consoles.
[312] ICO, *Big data and data protection*, July 2014.
[313] ICO publishes details of all the enforcement cases it has undertaken.
[314] See the London Action Plan website.
[315] See published update (December 2014). Section A of the update sets out details of respective enforcement activities in this area.

consumers in relevant markets, where appropriate by promoting competition.[316]

5.23 Ofcom has commissioned a number of reports relating to market developments in this area such as the adoption of digital technology, under its general responsibility to encourage investment and innovation in relevant markets. These include research on:

- the online data economy;[317]
- living room connected devices;[318]
- consumers' online experience;[319] and
- the app environment.[320]

5.24 In particular, Ofcom recently consulted on potential barriers to investment and innovation in the IoT and published its response in January 2015, see **Box 5.3**.[321]

Box 5.3: Ofcom common framework for data privacy (IoT)

Following a consultation on how to promote investment and innovation in the IoT,[322] Ofcom noted that some IoT applications may have the potential to expose the limitations of traditional approaches to data privacy. It concluded that, while the collection and use of personal data will continue to be regulated by ICO '…a common framework that allows consumers easily and transparently to authorise the conditions under which data collected by their devices is used and shared by others will be critical to future development of the IoT sector.'

Ofcom proposes to work with ICO, government, other regulators and industry to facilitate progress on this issue nationally and internationally.

---

[316] Section 3(1) Communications Act 2003. Ofcom also operates under a number of different pieces of legislation.
[317] Analysys Mason, *Report for Ofcom – Online data economy value chain*, February 2014.
[318] Ofcom, *Internet connected living room devices*, 2014.
[319] Ofcom, *Being online: an investigation of people's habits and attitudes*, June 2013.
[320] Ofcom, *Apps environment*, March 2014.
[321] Ofcom, *Promoting investment and innovation in the Internet of Things*, January 2015.
[322] Summary of responses and next steps following consultation on the IoT: Ofcom, *Promoting investment and innovation in the Internet of Things*, January 2015.

Financial Conduct Authority (FCA)

5.25 The FCA is the UK regulator for financial services, with objectives established in the Financial Services Act 2012.[323] It has an overarching mission to ensure that financial markets work well, including by securing an appropriate degree of protection for consumers, protecting and enhancing the integrity of the UK financial system, and promoting competition in the interest of consumers.

5.26 The interest and work of the FCA in relation to firms' use of consumer information is wide-ranging and multi-faceted. For instance, when authorising and supervising firms, the FCA considers whether IT infrastructure, data protection and/or data usage policies raise concerns in terms of consumer protection or market dynamics.[324] Its interest in how consumer data is collected and used permeates a number of sectoral activities, including market reviews and studies where it consider issues, including market features, that might disrupt markets working to the benefit of consumers, including those relating or intrinsically linked to how consumer information is collected and used (for example the FCA's thematic review of PCWs in the general insurance sector referred to in **paragraph 2.44** above).

5.27 The FCA work and interest encompasses not only current business models but also emerging models, for example online financial intermediaries (which can range from price comparison websites to those relying on more detailed personal data and/or credentials). This work ranges from horizon-scanning and analysis of potential impact, to interventions in specific sectors. It also includes thought leadership pieces on issues such as behavioural economics, which consider how consumers make decisions and, in turn, how information about consumers might be used to influence market outcomes.

5.28 The FCA has a number of pieces of work planned that relate to consumer data. In its 2015/16 Business Plan, the FCA notes its plans for a market study into big data and Insurance:

> '…to investigate how insurance firms use Big Data, such as web analytics and behavioural data tools (including the increasing use of social media) as well as other unconventional data sources. We will identify potential risks and benefits for consumers, including whether the use of Big Data creates barriers to access products or services. We will also examine the

[323] FCA, *What we do*.
[324] See for instance: FCA, *FSA factsheet: Your responsibilities for customer data security*, 2011 (data protection); or the handbook (lead generators).

regulatory regime to ensure that it does not unduly constrain beneficial innovation in this area'.[325]

5.29 In addition, the FCA's business plan notes that it is:

> '…planning to consult on proposals in relation to cold-calling, as unsolicited marketing may be causing significant distress to consumers. We also want to look at the use of quotation searches, which will enable consumers to shop around for credit without their credit record becoming unduly impaired'.[326]

Competition and Markets Authority

5.30 The CMA seeks to promote competition both within and outside the UK for the benefit of consumers. The CMA has a number of different legal powers related to its various responsibilities, which are:

- investigating mergers that could restrict competition;
- conducting market studies and investigations in markets where there may be competition and consumer problems;
- investigating where there may be breaches of UK or EU prohibitions against anti-competitive agreements and abuses of dominant positions;
- bringing criminal proceedings against individuals who commit the cartel offence;
- enforcing consumer protection legislation;
- co-operating with sector regulators and encouraging them to use their competition powers; and
- considering regulatory references and appeals.

[325] FCA, *FCA Business Plan 2015/16*.
[326] FCA, *FCA Business Plan 2015/16*.

5.31 The CMA may use its consumer protection powers in relation to breaches of CPRs,[327] UTCCRs[328] (and forthcoming CRA) and CCRs[329] to address market-wide problems.

5.32 The CMA belongs to the Consumer Protection Partnership (CPP) which includes the CMA and FCA, the National Trading Standards Board and Citizen's Advice and aims to improve consumer protection, co-ordinate enforcement and reduce consumer detriment.[330] CPP's priorities for 2015 include the use of personal data in online markets. Its outputs for 2015 include both this CFI and research by Citizens Advice into the disadvantages and detriments caused to consumers by a lack of transparency about how the personal data market works, and lack of control over how their data is captured and used, and by whom.[331]

5.33 The CMA shares its consumer protection powers with a number of partner organisations. In using those powers, it will prioritise projects where there are systemic market problems or where consumers are unable to exercise choice, or where we can expect to achieve wider impact, for example, by developing the law or by having a deterrent effect. This role complements and reinforces the effects of our other work to improve markets and to support economic growth, by addressing problems where competition enforcement alone does not, or cannot, make a market work well for consumers.

5.34 The CMA is also part of a pan-European network of public consumer protection bodies which provide mutual assistance and co-operation under the CPC Regulation.[332]

---

[327] TSS and, in Northern Ireland, the Department of Enterprise, Trade and Investment (DETINI) have an enforcement duty but the CMA also has power to enforce the CPRs (which is exercised to tackle undesirable market wide practices as outlined above). See Regulation 19 of the CPRs.
[328] In relation to the UTCCRs, the CMA and Trading Standards Services (TSS) have joint responsibility for enforcement, although the CMA is the lead authority and primary source of expertise and guidance.
[329] The CMA is not an 'enforcement authority' under the CCRs but may take enforcement action under Part 8 of the Enterprise Act 2002. See Enterprise Act 2002 (Part 8 EU Infringements) Order 2014/2908 Schedule 1.
[330] The Consumer Protection Partnership (CPP) was formed in April 2012 as part of the Government's institutional reform of the consumer landscape. The CPP includes the National Trading Standards Board (NTSB), Trading Standards Scotland (TSS), the Department for Enterprise, Trade and Investment Northern Ireland (DETI), the Competition and Markets Authority (CMA), the Financial Conduct Authority (FCA), the Trading Standards Institute (TSI), Consumer Council for Northern Ireland (CCNI), Citizens Advice (CitA), and Citizens Advice Scotland (CAS)
[331] Citizens Advice, *Personal data empowerment - Time for a fairer deal*, April 2015. This CMA CFI itself is identified as part of the CPP work-plan.
[332] Regulation 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (the CPC Regulation). For further details, see 4.18ff. of CMA7.

Application of consumer protection legislation

CPRs

5.35 We set out in **Table 5.1** below illustrative examples of potentially unfair commercial practices under the CPRs by businesses which may collect and/or use consumer data.[333] We stress that these are for illustration and indicative purposes only. Any assessment would need to be made on an individual basis on the basis of prioritisation principles.

Table 5.1: Illustrative examples of potential breaches of CPRs

Breach	*Potential application*
General prohibition	• Failure to observe the 'cookie law' and/or to process personal data fairly in accordance with the DPA.[334]
Misleading actions or omissions	• Offering 'free' services in exchange for consumer data without explaining the commercial motives – which is material information the consumer needs. • Misrepresenting the privacy, security, or confidentiality of users' information –which could still be deceptive, even if the privacy policy or other small print is factually correct (for example, the consumer is told that data is collected in order to complete a purchase. That may be factually correct but would be misleading if the data were also used to put the consumer on a 'sucker' list'). • Failing to explain relevant digital content functionality such as geo-location tracking for marketing purposes (Insofar as this example may also involve breaches of the DPA, PECR and CCRs in relation to the pre-contract information regarding functionality, the general prohibition may also be engaged). • Failing to adhere to the standards set out in a code which the trader has publicly affirmed they are a member of – for instance the IAB code.

Source: CMA.

UTCCRs/CRA

5.36 We set out in **Table 5.2** below illustrative examples of terms which may be unfair on the basis of the grey list in the UTCCRs. Similar provisions apply under the forthcoming CRA, as set out in **Chapter 2**.

[333] Other legislation may also apply, for example the CCRs. The regulations which may apply are set out in **Chapter 2**.

[334] An example of where CMA may have concerns in relation to the collection and use of data is the ICO undertaking sought in relation to an UCAS application form which required the unticking of boxes to opt out of receiving adverts about mobile phones, energy drinks etc. The unticking of those boxes also resulted, however, in students not receiving other education-related information that they needed. Consequently they were, in effect, forced to allow the processing to take place, and so their ability to take an informed decision was significantly impaired.

Table 5.2: Illustrative examples of potential breaches of UTCCRs

Grey list term: terms may be unfair if they have the object or effect of:	***Objection as described in Guidance***	***Potential application***
Irrevocably binding the consumer to terms with which he had no real opportunity of becoming acquainted before the conclusion of the contract.	Consumers should have an opportunity to read and understand terms before becoming bound by them. (Guidance, 9.1) It is not 'hidden terms' themselves that are indicated to be unfair, but any term which binds the consumer to accept or comply with them – or, in legal jargon, 'incorporates' them 'by reference'. (Guidance, 9.2) If terms require consumers to accept that they are bound by the terms of other linked contracts, they should be given an appropriate chance to read them (Guidance, 9.3) The overriding requirement is that consumers are effectively alerted – before committing themselves – to all contractual provisions that could significantly affect their legitimate interests. (Guidance 9.4)	Potential application to terms requiring consumers to accept terms of third party privacy policies / terms and conditions.
Enabling the seller or supplier to alter the terms of the contract unilaterally without a valid reason which is specified in the contract.	A right for one party to alter the terms of the contract after it has been agreed, regardless of the consent of the other party, is under strong suspicion of unfairness. A contract can be considered balanced only if both parties are bound by their obligations as agreed (Guidance, 10.1)	May potentially apply where privacy policies or terms are unilaterally varied after the contract has been entered into, for example where already collected data is put to a different use to that for which it was originally collected.
Giving the seller or supplier the possibility of transferring his rights and obligations under the contract, where this may serve to reduce the guarantees for the consumer, without the latter's agreement.	A term is unlikely to be fair if it allows the supplier to sell on its business to someone else who offers a poorer service (Guidance 16.1). An assignment clause may be considered fair if it allows the supplier to assign only in circumstances which ensure that the consumer's rights under the contract will not be prejudiced (Guidance, 16.2)	May potentially apply to an assignment of business which has consumer data, in particular where the assignee changes the use to which the data is being put, or has a materially worse privacy policy.
Other potentially unfair terms	***Objection***	***Potential application***
'Have read and understood' terms and conditions declarations.	Such declarations may require consumers to say the terms and conditions have been met, whether they have or not which may defeat the purpose of the Directive that terms must be clear and intelligible (Guidance, 18.5.5).	May potentially apply to privacy policies, terms and conditions and/or end user licence agreements.
Reservations of special rights	A term or statement which could be understood as permitting the supplier to pass on information about the consumer more freely or widely than would otherwise be allowed under the Data Protection Act is likely to be open to challenge (Guidance, 18.6.2)	May potentially apply to privacy policies, terms and conditions and/or end user licence agreements.
Terms which may breach requirement for plain English and intelligible language	The requirement of the underlying Directive is that 'consumers should actually be given an opportunity to examine all the terms' (Recital 20). Objections may be raised to small print, legal jargon or technical terms, long sentences etc. Fairness requires that consumers have a real chance to learn, by the time the contract becomes binding, about terms whose effect might otherwise come as an unpleasant surprise (Guidance, 19.9)[335]	May potentially apply to long, jargonised, or difficult to read, privacy policies, terms and conditions and/or end user licence agreements.

Source: CMA.

[335] The CJEU has explained that the requirement of plainness and intelligibility means that the term should not only make grammatical sense to the consumer but must put the consumer into the position of being able 'to

Self-regulation

5.37 Alongside regulation, self-regulation, where effective, can be a means of raising standards and building trust as new technologies can enable even greater collection and sharing of data. A number of self-regulatory initiatives (summarised in **Chapter 2**) supplement the applicable laws. There are also new initiatives in train.

5.38 We support effective and proportionate self-regulation for the reasons set out in the OFT's policy statement, which also sets out a number of factors which may contribute to a successful self-regulatory scheme, as set out in **Box 5.4** below.[336]

Box 5.4: Factors that may contribute to the success of self-regulation

In 2009, the OFT published its Policy statement on the role of self-regulation in the OFT's consumer protection work. This document was produced when OFT operated the consumer codes scheme and was prepared in that context. Nonetheless we consider the principles continue to apply more broadly. The factors identified by the OFT in 2009 were:

- there are clear policy objectives to show how quality problems will be addressed;
- private interests are aligned with public interest;
- there are suitable governance arrangements within a dedicated structure;
- there is a genuine commitment to the initiative from strong industry leadership;
- independent non-industry stakeholders are involved and have the opportunity to influence;
- adequate and sustainable resources are allocated to the regime;
- the scheme has wide coverage which ensures an influence on the market as a whole;
- there are clear rules that, at a minimum, ensure compliance with the law and do not restrict competition;
- setting of rules utilises industry knowledge;

---

evaluate, on the basis of clear, intelligible criteria, the economic consequences for him which derive from it [the term]'. See C-26/13 *Arpad Kasler, Hajnalka Kaslerne Rabai v OTP Jelzalogbank Zrt*, at paragraph 75.

[336] OFT1115, *Policy statement - The role of self-regulation in the OFT's consumer protection work*, September 2009.

- there is public awareness of the scheme and consumer-focused provision of information and publicity;
- the systems, processes and outcomes must be readily understood and transparent;
- there are clear procedures for complaints;
- there is an effective redress system;
- there are well designed effective sanctions;
- businesses are offered assistance to achieve compliance;
- the scheme conducts proactive monitoring;
- sanctions are actively enforced; and
- the initiative is supported by appropriate government action.

5.39 We have not conducted a detailed assessment of the initiatives referred to in **Chapter 2** against all these factors – focusing instead at a high level on awareness of and enforcement within those we looked at. However, we consider these factors provide a useful set of principles against which these and other schemes could self-assess the impact of their activities.

5.40 We undertook a brief review of the complaints received which is set out in **Box 5.5** below. Whilst not a measure of awareness, the extent to which the bodies receive contacts and complaints from the public provide some information on their profile and usage. In this respect, the numbers were typically small when considered against the volume of data being collected and shared. We believe it is important for the organisations that run these initiatives to continue to promote them to consumers.

Box 5.5: Awareness and use of self-regulation initiatives

IAB/ASA

The ASA receives a total of approximately 35,000 complaints annually about breaches of the CAP Code. Since it began administering the new Online Behavioural Advertising (OBA) rules in February 2013, it had received a total of 206 OBA-related complaints to May 2015.[337]

[337] The majority of complaints focused on problems consumers experienced when trying to opt-out of receiving OBA. Some complainants had attempted to opt-out of OBA, but believed their opt-out had failed because they

A 2014 TRUSTe- and EDAA-commissioned survey found that 26% of adults in Great Britain had seen the AdChoices icon accompanied by the 'AdChoices' text (a reported increase from 13% in 2012). Of the respondents who recognised the icon, 28% had clicked on it.[338] Various consumer campaigns have been deployed to raise awareness of the icon in the UK, Ireland, Germany, France, Greece, Finland, Sweden and Portugal.[339]

DMA/DMC

Over a 15-month period from April 2013 to June 2014, the Direct Marketing Commission (DMC) – an independent body that investigates complaints against DMA members – received 360 complaints, of which 103 consumer complaints and 12 business-to-business complaints involved DMA members.[340]

MRS

The MRS operates 'Codeline' – a confidential query service which provides advice on the MRS Code of conduct. In 2013-14, this received 568 queries, of which 39% related to data protection.[341]

5.41 Self-regulatory initiatives have various powers to investigate alleged breaches of the code and multiple redress mechanisms. Typical procedures are summarised in **Box 5.6**.

Box 5.6: How self-regulators handle complaints

Upon receiving a complaint, self-regulators tend to investigate further and decide whether the complaint requires a substantive investigation and formal adjudication or whether the matter can be resolved informally.

Where there has been a minor breach the matter may be closed, often with a formal reminder of the party's obligations under the Code. If the matter is to be resolved formally, it will typically be referred to an independent body for adjudication.

If the complaint is upheld at adjudication, the various sanctions that can be applied include: a formal undertaking from the party to comply with the Code; a formal undertaking to carry out changes to the party's processes or procedures; the issue of a warning; suspension or cancellation of membership; or the matter may be referred to relevant law enforcement and consumer protection bodies where necessary.

---

continued to see advertisements which they thought had been served by OBA or which carried the 'AdChoices' icon. Other complainants had experienced difficulties in using the opt-out mechanism and found that their choices had been reset shortly after opting-out.

[338] EDAA and TRUSTe, *The European Advertising Consumer Research Index 2014*, December 2014.

[339] For more about the UK campaign see: IAB, *Consumers gain greater control over targeted online ads*, June 2013.

[340] DMC, *Annual Report 2013/2014*, January 2015.

[341] MRS, *Annual Review 2013/14*, August 2014.

The DMC, the MRS and the ASA also publish any formal adjudication on their respective websites.

In addition to its standard redress mechanisms, where the party is certified and displays a compliance seal or icon, many self-regulatory initiatives have the power to strip them of that icon. For example, for third party signatories of the IAB Framework for OBA, the ASA has the power to remove the trading seal that a business will receive in complying with the EU best practice recommendation as well as the removal of the EU Licence for the 'AdChoices' icon.

5.42 Information on the extent to which complaints lead to enforcement action suggest that application of the more severe sanctions is relatively rare, see **Box 5.7** below. Low numbers may reflect many factors – including general levels of compliance, the nature of the complaints raised and the use of informal action to remedy the problems.

Box 5.7: Self-regulation and enforcement

ASA

In the year to March 2015, 736 of the 35,000 complaints received by the ASA in relation to the whole of the CAP Code led to an adjudication on a potential breach.[342] None of the adjudications related to the OBA rules or Section 10 of the CAP Code.

In relation to OBA, the vast majority of complaints received were resolved after initial assessment within the complaints team.

In terms of database cases (section 10) the ASA resolved 234 cases (about obtaining, processing, management and use of personal information for the purposes of marketing products and services through targeted and personalised direct marketing). Of these 47 were withdrawn, suggesting that 187 were 'problem' cases. The ASA notes that they largely resolve database complaints to the satisfaction of complainant without the need for formal investigation.

DMA/DMC

Over a fifteen month period to June 2014, the DMC found five companies in breach of the DMA Code. In two of those five adjudications the companies were subsequently expelled from DMA membership.

[342] ASA, *Adjudications: Advanced Search*.

When assessing how to deal with a complaint, the DMC told us it looks at how they can best help and encourage companies to reduce complaints and improve their compliance prior to an adjudication. This is evident in one of the DMC's latest adjudications. The DMC held that there had been a breach of the DMA Code in relation to the clarity of a member's information when consent is secured online. The member had made a number of changes to reduce complaints and co-operated fully with the investigation. In light of this, the DMC reprimanded the member and reminded it of its obligations under the Code.[343]

MRS

In the year 2013/14, the MRS investigated 77 complaints, 11 of which became disciplinary cases. Of the 11 disciplinary cases, one of the complaints was upheld, leaving eight complaints not upheld and two complaints outstanding as at 31 March 2014.[344]

5.43 We consider that, in a situation where fragile consumer trust is a potential concern, the appropriate use and publicity of sanctions enforced could help demonstrate the value of self-regulatory initiatives more broadly in that they and their members take seriously the need to protect consumers and that poor practice will be visibly punished.

New developments

5.44 ICO is developing plans for a Privacy Seal scheme to drive up privacy standards. In part this is a recognition of the value of adopting more co-regulatory and self-regulatory approaches given the growing collection and use of consumer data collection. It may also recognise the difficulties of notice and consent mechanisms in an era of Big Data/IoT. This scheme is outlined in **Box 5.8** below.

Box 5.8: ICO Privacy Seals

In autumn 2014, ICO consulted on the framework criteria for an ICO-endorsed 'privacy seal'.[345] As ICO explained in the consultation document, a privacy seal scheme acts as a 'stamp of approval' highlighting an organisation's commitment to maintaining good privacy standards. ICO has proposed to endorse at least one privacy seal scheme, operated by an independent third party in the UK, with a view to launching the first round of endorsed schemes in 2016. The scheme operator(s) will be accredited by the UK Accreditation Service (UKAS).

[343] DMC, *DLG (t/a Consumer Lifestyles) – complaints about consumer marketing*, May 2014.
[344] MRS, Annual Review 2013/14, August 2014, page 11.
[345] ICO, *Privacy seals: draft framework criteria*, October 2014.

ICO has explained that:

> '…the aim of the initiative is to raise awareness of privacy concerns, encourage transparency by organisations and build consumer trust and choice. The presence of a seal will highlight those organisations that go the extra mile to look after people's information and potentially provide them with a competitive advantage. A privacy seal will raise the bar for privacy standards across the UK and will help protect personal information'.[346]

5.45 BIS and DCMS have also been working with the Digital Economy Council (DEC) in an initiative led by the Digital Catapult to develop a data sharing and trust framework and potential platform for data sharing, see **Box 5.9** below.

Box 5.9: Digital Catapult Trust Framework initiative

The Digital Catapult Centre is leading a Personal Data and Trust programme to find innovative, non-regulatory ways to unlock greater economic and societal value from consumer and commercial data. One strand of the programme is the development of a data sharing and trust framework that aims to give consumers greater control of how their data is used and shared, and by whom and that generates value by increasing the flow of data sharing between organisations

Work on the Framework is in its early stages but Digital Catapult aim to have an initial version of the Framework ready for launch by the second quarter of 2016. It is envisaged that organisations from all sectors will pay to join the framework and agree to adhere to a voluntary set of rules and practices on consumer data. They will then have potential access to customer data held by other members, subject to consumer permissions.

The Digital Catapult centre is also working with the British Standards Institution and ICO to consider how consumer facing Kitemarks might feature in the Framework.

5.46 These initiatives could help to drive up standards and address some of the concerns we identified in our CFI. They also need to be visible to consumers with clear and well understood identifiers of membership that signal higher quality, allowing consumers to reward compliant firms.

Views on the regulatory regime

5.47 In some markets, the competitive process does not function well and can fail to generate efficient market outcomes for both consumers and firms, due to

[346] ICO, *Data protection rights: What the public want and what the public want from Data Protection Authorities*, May 2015.

one or more factors, often referred to as market failures.[347] Regulation, when correctly designed and enforced, can correct market failures and encourage competition and choice. In the case of data, it also ensures respect for values and fundamental rights of consumers, including privacy.

5.48 However, disproportionate or over-prescriptive regulation could have unintended consequences that negatively impact on efficient and competitive markets, causing detriment to consumers and firms. It may also restrict the possibilities for innovation and limit economic growth.

5.49 Non-compliance with regulation may also have implications for competition. If some businesses comply while some do not, this can affect the costs firms incur and may distort competition. It is important, therefore, to create an effective regulatory environment where businesses are incentivised to respect the regulations, which are proportionate and appropriately enforced.

5.50 In this section, we set out some of the information we have received on the existing regulatory regime and what changes might help to ensure or enhance the benefits for consumers and firms from the commercial use of consumer data.

5.51 A view held by a number of respondents representing both business and consumer perspectives was that the balance of power over the collection and use of data had moved from consumers towards businesses. We were told by one large business that big data collectors collect information consumers are not aware of, do things with it that they were not asked about, and don't allow them to opt out or exercise choices about it. We were also told by a business consultancy that, as a result of increasing digitisation, there has been a shift from a primary focus on volunteered information (such as consumers completing forms) to 'passive' data collection. Another response from an industry body referred to the 'information asymmetry' in favour of suppliers and against consumers. Reasons given for this alleged shift in power included technological changes, business practices and lack of effective enforcement of the current regime.

5.52 We received various suggestions on how the regime could be improved. It was suggested by some respondents that consumers should have to opt in to data collection as the default and not opt out. Another suggestion was that,

[347] Market failures can include the presence of public goods, monopoly power, benefits or costs to society that are not considered in decisions that consumers and firms make, decision made by consumers that are made on behalf of others or that impact on other people, asymmetric information, and inconsistencies of decisions made at different points in time.

whenever businesses contact individuals, they should be required to be clear about how and where information about the consumer was obtained.

5.53 We set out below in more detail particular issues raised regarding consumer awareness, consent and control, and enforcement.

Consumer awareness, consent and control

5.54 As discussed in **Chapter 4**, when given a fully informed choice, consumers appear willing to share certain data for certain purposes when they are confident that this represents their best interests. If not, they may withhold data, or seek to disguise it, or disengage.

5.55 A number of respondents criticised the current operation of privacy notices and (where applicable) terms and conditions. Although there was a recognition of the tension between, on the one hand, the need for legal compliance in a technically difficult area and, on the other, consumers' desire for a seamless experience when using digital media, a number of responses indicated that, in practice, they fail to perform their intended task of generating understanding and ensuring the fair collection and use of personal data. Views put forward included that privacy policies are more designed to protect the firm rather than inform the consumer and are drafted by corporate lawyers to maximise the company's room to manoeuvre (for example by monetising the data) and reduce consumers rights to challenge.

5.56 These criticisms are not new. For instance, in its report, in its 2014 report, on 'Responsible use of data'[348] the House of Commons Science and Technology Committee noted that online terms and conditions are too long and complicated to obtain informed consent about use of data. In its response, the government agreed with the Committee and referred to the protections under the CRA that such terms are assessable for fairness.[349]

5.57 ICO and others have noted the inherent difficulties in the 'notice and consent' model in the context of big data/the IoT. The White House report[350] cited notice and consent mechanisms in privacy notices as a form of market failure since they creates a non-level playing field where users cannot properly evaluate the choice offered to them.

---

[348] House of Commons Science and Technology Committee, *Responsible Use of Data Fourth Report of Session 2014*, HC 245, November 2014.
[349] House of Commons Science and Technology Committee, *Responsible Use of Data: Government Response to the Committee's Fourth Report of Session 2014–15*, March 2015.
[350] Executive Office of the President, President's Council of Advisors on Science and Technology, *Report to the President, Big data and Privacy: a technological perspective*, May 2014.

5.58 This is a cause for concern. The concept of fair dealing which underpins consumer protection legislation requires businesses not to take advantage of consumers' circumstances to their detriment. The CMA is concerned by situations where consumers do not fully understand privacy policies or terms and conditions (including EULAs) which set out the basis on which data is collected and/or used or which seeks their consent.

Cookies

5.59 The implementation of the cookie law was cited by some respondents as a regulation which increased transparency that data was being collected but did not necessarily give an indication of how much data was collected or by whom or for what purposes.

5.60 As we noted in **Chapter 2**, some cookies are necessary to supply products and services. However, there were a number of concerns in relation to non-essential cookies, including that:

- cookies and similar technology can collect a large amount of data which are not necessary for the provision of the service requested;
- the acceptance of non-essential cookies is bundled with the acceptance of essential cookies which is an unfair condition of access; and
- some websites will not work properly if cookies are disabled.

5.61 Many websites load multiple third-party cookies serving differing purposes onto a user's computer each time they visit. In 2014, ICO led an international study looking at the use of cookies on 478 websites, which found that:

- UK websites placed the highest number of cookies, averaging 44 cookies during a person's first visit. Ten of the 84 UK sites examined set more than 100 cookies (with one setting 225 cookies);
- 70% were third party cookies; and
- 86% were persistent cookies.[351]

5.62 ICO has recognised that, in practical terms, obtaining informed consent for third party cookies on a publisher website is a particularly challenging area because the third party (which sets the cookie) has no direct interface with the user (since the cookie, which may be set when the user visits the publisher

[351] ICO, *Article 29 Cookie Sweep Results*, February 2015.

website, may not be visible on the screen).[352] Consumers may also give implied consent to the setting of cookies since the information collected may be innocuous as far as the consumer is concerned. However, based on the evidence set out in **Chapter 4** about consumer attitudes, different consumers are likely to have different views. The information obtained in the CFI suggests that there are a number of concerns about the way that such notices currently operate, particularly as regards the bundling of essential and non-essential cookies. While regulation of the 'cookie law' falls primarily to ICO, the implications of the operation of cookie notices may also fall within the consumer protection and markets role of the CMA.

5.63 Based on this evidence, in relation to both privacy notices/terms and cookie notices (and generally), we consider that businesses could helpfully do more to explain the data they are collecting from consumers, what they will use it for, and give consumers more control over the data provided.

Enforcement of the existing regime

5.64 Some respondents argued for more enforcement activity. They argued that, to build trust, more enforcement action should be taken so that those who breach the law will know that they will be punished. Some argued that, while the law was fit for purpose, it was not robustly enforced and that reassurance was needed, for example to ensure that businesses comply with personal data minimisation principles, store it securely and keep it no longer than is necessary. One respondent said that a prime cause of problems in the personal data market was regulators' lax interpretation and enforcement of consent mechanisms and privacy notices.

5.65 It was also argued, in many cases referring to the work of the EDPS in this area, that to ensure cohesiveness between authorities currently responsible for different 'enforcement silos', there needs to be greater co-ordination and cooperation, for example between CMA, Ofcom and ICO to reflect the convergence of issues between data protection, consumer protection and competition. Others argued for higher fines, for more effective individual or collective redress mechanisms or that criminal sanctions should be applied.

5.66 We also note a potentially evolving role for private enforcement action in relation to breaches of privacy. For example there is an ongoing private action before the High Court in which the claimants are pursuing Google for

[352] ICO takes the view that the key point is that informed consent is obtained rather than which party obtains it. ICO also states that the appropriate compliance mechanism, and level of information to be provided, is likely to be governed by the intrusiveness of the data collected. The use of cookies to create detailed profiles of an individual's browsing activity may be quite intrusive. As such, more priority should be given to getting meaningful consent than is the case for less intrusive cookies, for example those which record unique page views.

damages for breach of privacy rights on the grounds of reasonable expectation of privacy when using the Safari browser in circumstances when, for a limited time, Google, contrary to the privacy settings on the Safari browser in Apple devices, tracked and personalised adverts based on browsing history.[353] Private actions may have important implications, as shown for example with the 'right to be forgotten' CJEU judgment.[354]

Conclusions

5.67 Regulation can play an important role in ensuring markets work well. For data, regulation can also ensure essential privacy rights are respected. This has been a short, high level review of a wide-ranging activity, so we have not tried to reach a definitive view on how well markets are working, including the way they are regulated. However we have identified some elements of how firms' collection and use of consumer data could support well-functioning markets:

- Consumers should know when and how their data is being collected and used and be able to decide whether and how to participate; and they should have access to information from firms about how they are collecting, storing and using data, so that they can select the firm which best meets their preferences.

- Firms should compete on all issues that matter to consumers, including the provision of clear and useable controls that enable consumers to manage data-sharing.

- Consumers and firms should share the benefits of using consumer data. Consumers may get a new or better service or lower prices because firms are becoming more efficient, or even trade their data for a direct financial reward. Firms may gain more sales or market share or become more profitable.

- The regulation of the collection and use of data should ensure the protection of essential rights such as privacy. The market can help achieve this goal where regulations encourage competition and choice, allowing a 'race to the top' by firms to offer consumers better services.

---

[353] Vidal-Hall and others v Google Inc [2014] EWHC 13 (QB).
[354] Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González, Case C-131/12, Judgment 13 May 2014 (the 'right to be forgotten' case). The court held that, '…although the processing of personal data is permitted where it is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, this is not the case where such interests are overridden by the interests or fundamental rights and freedoms of the data subject — in particular his right to privacy'.

- Non-compliance with regulation should be tackled proportionately and effectively, so that firms and consumers can feel confident that the rules are being applied fairly.

Enforcement

5.68 The CMA is one of a number of authorities with a role in consumer protection and enforcement relevant to the collection and use of consumer data. We will play an active role in the enforcement of regulation on consumer data, working with other regulators to ensure an integrated approach to enforcement and regulation, assessing which tools are most appropriate to tackle specific problems.

5.69 The growth in the collection and use of data, and the complexity of data markets make the role of regulators increasingly challenging. It is therefore important to find ways to make markets work well as far as possible, so that regulators can focus on areas of most serious concern such as breaches and persistent poor practice. Consequently, it is important that we work together with other authorities effectively, liaising and potentially working together to ensure we adopt a consistent and joined-up approach to enforcement in this area. This will build on existing arrangements: the CMA already has in place memoranda of understanding with ICO,[355] Ofcom[356] and the FCA.[357] Ofcom has also signed a letter of understanding with ICO setting out the basis for collaboration in areas of common enforcement responsibility.[358]

5.70 We recognise the growing challenges of enforcement in these developing markets and the different types of regulation that may be applicable in different circumstances. We will therefore work with other regulators to share information on new developments (eg technological, new types of products) and on complaints. We aim to create a robust, consistent and proportionate approach to tackling breaches of regulation in order to create confidence in the market.

Regulation

5.71 During the course of our project we have heard many concerns that current regulations are inadequate. The European data protection framework is already under revision which will have an impact on businesses which collect

---

[355] CMA, *CMA and ICO memorandum of understanding*, May 2015 (consumer protection).
[356] CMA, *CMA and Ofcom memorandum of understanding*, February 2015 (consumer protection), and CMA, *CMA and Ofcom memorandum of understanding*, June 2014 (competition).
[357] CMA, *CMA and FCA memorandum of understanding*, July 2014 (competition and consumer protection).
[358] Ofcom, *Letter of Understanding between the Office of Communications and the Information Commissioner's Office*.

and use consumer data. We stand ready to advise on any proposed changes. We will use the information, assessments and findings we have reached in this CFI to inform the approaches of relevant domestic and international partners to these issues.

5.72 We live in a global economy and many businesses operate across international boundaries. It is important that the framework for standards and regulation develops in a coordinated way internationally, eg using the OECD as a forum to develop new approaches. We will similarly contribute to the development of international policy in this area, using the knowledge we have gathered in this project.