Appendix L: summary of research on consumers' attitudes and behaviour

Introduction

1. The issues of data privacy and the processing of user data have attracted a considerable amount of interest and research from a wide range of different perspectives, including consumer protection, legal, behavioural economics, information processing and psychology.

2. In order to have a comprehensive understanding of the research about data privacy and data processing, we have carried out a review of the publicly available consumer survey data and the relevant academic research. The purpose of the review is to establish an evidence base to inform our understanding of these issues.

3. We recognise that the consumer survey evidence is based on stated preferences rather than actual observed behaviour and that, in surveys, respondents might be stating a preference about privacy without having to consider what a relevant counterfactual might be. However, the purpose of this review is to build up a picture of consumers' attitudes in general and identify broad themes in terms of issues and concerns. We use this material alongside our review of academic research (which does analyse actual consumer decision-making in experimental settings and field experiments) to inform our evidence base.[1]

4. Following GDPR article 4(2), we use the general term 'data processing' to describe any action operation or set of operations which is performed on personal data.[2] This includes, but is not limited to, the collection, storage, use and deletion of data. Where relevant, we will indicate where we are discussing specific elements of data processing, such as data collection or data sharing to avoid confusion.

5. Since the publication of the interim report in December 2019, this appendix has been updated to include:

---

[1] In Chapter 4 we further develop our evidence base by combining the material set out in this appendix with data from firms about how consumers behave in practice eg in terms of the proportion of users engaging with Privacy Policies and privacy controls and settings.

[2] GDPR article 4(2) defines data processing as: 'any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use disclosure by transmission, dissemination or otherwise making available, alignment of combination, restriction, erasure or destruction'.

- A high-level comparison of our current findings with the findings on consumer attitudes at the time of the CMA's 2015 report Commercial Use of Consumer Data.

- Survey material on consumer attitudes and behaviour that has been published since the Interim Report.

- Additional academic research that is relevant to consumer attitudes and behaviours.

- An expanded discussion of the factors that could explain the reported discontinuity between consumers' stated preferences and actual behaviour in regard to privacy (the so-called 'privacy paradox').

- The section of this report detailing consumer attitudes has been expanded with a detailed description of consumers' perception of the benefits and the harms associated with data processing in relation to personalised advertising.

6. However, in line with the previous iteration of this appendix that accompanied our interim report, we have retained the focus on three main topics in relation to data privacy and data processing. In order to structure our research and analysis, we have considered a series of high-level questions for each of the topics. We have then broken those high-level questions down into a series of sub-questions which enables us better to explore the wide range of issues that are dealt with in the consumer survey and academic research. The topics and initial high-level questions that we considered against each topic are:

- <u>Topic 1: Consumers' knowledge and understanding of data processing</u>

  (i) How much do consumers know, or think they know, about data processing?

  (ii) Are consumers engaging effectively with terms and conditions and privacy policies?

- <u>Topic 2: Consumers' control over their data</u>

  (i) Do consumers feel in control of their data and to what extent do they engage with controls over their data?

  (ii) What influence do behavioural biases and choice architecture have on the decisions that consumers make regarding privacy choices?

- <u>Topic 3: Attitudes towards data processing and personalised advertising</u>

(i) What are consumer attitudes towards data processing?

(ii) What are consumer attitudes towards personalised advertising?

(iii) What do consumers perceive the benefits and harms of data processing in relation to personalised advertising to be?

7. We then discuss some of the potential implications of the consumer survey and academic research for remedies. For example, how issues to do with choice architecture and behavioural biases could be relevant and whether consumers want more control over their data.

8. Finally, we set out the methodology used to assemble the consumer survey research in a separate annex. This appendix includes a list of the sources and academic research referenced in this report.

Comparison with the CMA's 2015 report "The commercial use of consumer data"

9. In 2015 the CMA carried out a report into the commercial use of consumer data to understand how consumer data is being collected and used commercially. As part of this report the CMA investigated consumers' awareness and understanding of, attitudes towards and control over data processing. This section highlights the key findings and how it compares with our current research.

10. The CMA found that most consumers were aware that companies collect their data, although this did vary by age and social grade. However, few consumers understood what data is collected about them in addition to what they have provided. Awareness of how data is used was similarly low.

11. Responses to the CMA's Call for Inputs identified a number of benefits for consumer 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. At the same time, most consumers believed that businesses benefited the most from data processing. Consumers also believed that firms provided insufficient information about what information they gathered and why.

12. The CMA reported that studies had identified a spectrum of public attitudes to how people perceive their personal data and their level of comfort in sharing it, although it was possible to make some broad classifications. Attitudes were also heavily influenced by the context in which data processing took place.

For example, many consumers were less willing to share data with commercial firms or where there was no clear benefit to sharing data. Overall, the CMA found that consumers had substantial reservations about sharing their data and how it might be used.

13. That being said, many consumers still shared their data despite the high reported levels of concern. The CMA found this was partially the result of biases that influence consumers towards low benefits instead of high risks. Such biases included information asymmetries, consumers' tendency to discount future harms and benefits, and the perception that data sharing was unavoidable.

14. Consumers perceived their main method to control their data was to choose whether or not to consent to data sharing when asked. However, few consumers read or understood privacy policies, spurred in part by the large amount of time required to read these documents. Consumers wanted more transparency and clearer explanations of how their data would be used and shared.

15. As for other tools and settings available to them, consumers were aware of the most immediate settings available to them and especially so with privacy settings on social media platforms. Consumers were less likely to adopt active settings and controls, such as sites' 'dashboards.' The CMA noted that many consumers felt a distinct lack of control over the collection and use of their data and a similar number expressed a desire for more control.

16. In comparing these findings with our current research, we note that little appears to have changed for consumers over the past five years. For instance, the finding that consumers feel they lack control over the collection and use of their data still holds true. In addition, consumers still desire more transparency and clearer explanations of how their data will be used. This is despite the introduction of the GDPR in 2018 which was designed to grant more control and transparency to consumers.

17. One difference between the two reports lay in how consumers utilised social networking privacy settings. The 2015 report found that consumers regularly used privacy settings on social networking sites while also reporting that participants often struggled to find and use privacy settings on other popular online services. However, the 2015 report also found that consumers mostly utilised 'easy' controls and reacted to settings when prompted instead of taking proactive approaches, such as using sites' own "dashboards" to control privacy settings. The high levels of engagement reported in 2015 thus appear to be related to prompts, such as restricting who can see a social media post,

and that few consumers interacted with the less visible privacy settings, such as restricting targeted advertising.

18. The fact that consumers' current knowledge of and control over data processing appears not to have changed significantly over the last five years would tend to suggest that it may not change substantially in coming years without some sort of external impetus.

19. In the next section we summarise our main findings for each of the 3 main topics set out above using a high-level questions and sub-questions structure. We then move into the main part of the report, starting with a short discussion of some key issues relating to the economics of privacy. In particular, we set out a discussion of the factors which are relevant to considering what has been termed the 'privacy paradox' and which is important in terms of influencing much of the discussion of consumer behaviour in an on-line setting.

Summary findings

Consumers' knowledge and understanding of data processing

How much do consumers know, or think they know, about data processing?

20. There is evidence consumers understand that personal data is valuable to platforms and most all agree that companies benefit the most from data processing. Perhaps as a part of this, consumers also tend to believe that companies primarily collect data for their own benefit. [3,4]

21. Most consumers are not sure what information online platforms hold about them, but there is a higher recognition for information consumers actively enter compared to information that is passively collected.[5,6,7] There is a common perception that platforms collect a large amount of data, although few consumers are aware of the true volume of the data that is or can be collected.[8]

---

[3] Data and Marketing Association and Acxiom (2018). GDPR: A consumer perspective.
[4] Ipsos MORI (2016a). Digital footprints: Consumer concerns about privacy and security.
[5] An example of information that a consumer might actively enter is their age when filling in registration forms. An example of passively collected information might be a user's IP address.
[6] Miller, C., Coldicutt, R., & Kitcher, H. (2018) for Doteveryone. People, Power and Technology: The 2018 Digital Understanding Report.
[7] Harris Interactive (2019) for the ICO. Adtech – Market research report.
[8] Ipsos MORI (2016a). Digital footprints: Consumer concerns about privacy and security.

22. There is a consensus in both the academic research and the consumer survey evidence that most consumers only have a basic understanding of data processing. Specifically:

- There is a higher recognition of 'active' methods of data collection over 'passive' methods, although most consumers are aware of cookies.[9,10]
- Consumers are more likely to recognise easily visible uses of data (eg personalised advertising and recommendations) over more hidden uses (eg price discrimination).[11]
- Few consumers are aware of the extent to which data sharing occurs or that data can be combined to form profiles before being shared.[12]
- Men and consumers who described themselves as confident internet users are more likely to report a greater awareness of how data is collected, used and shared.[13,14]
- There is also some evidence that awareness of how data is collected, used and shared is increasing over time.[15]

23. At the same time, there is also evidence that consumers may overestimate their knowledge of data processing and research by Harris Interactive for the ICO, Which? and the CDEI has also found that consumers' attitudes towards data processing change as they learn more.[16,17,18]

24. Evidence from the academic research indicates that it is difficult for consumers to anticipate how their data will be used. For example, advances in data mining and computing power can create unforeseen uses for data.[19] The Stigler Center has also argued that the knowledge deficit between consumers and firms can be compounded because firms do not face strong incentives to differentiate themselves on a basis of privacy.

---

[9] An active method of data collection can be asking a user to register their details on a website. A passive method can include apps collecting location data when not in use.
[10] Ofcom (2019). Adults Media Use and Attitudes report - data tables. Table 97.
[11] Miller, C., Coldicutt, R., & Kitcher, H. (2018) for Doteveryone. People, Power and Technology: The 2018 Digital Understanding Report.
[12] Which? (2018). Control, Alt or Delete? Consumer research on attitudes to data collection and use.
[13] Ipsos MORI (2016a). Digital footprints: Consumer concerns about privacy and security.
[14] Information Commissioner's Office (2019). Information Rights Strategic Plan: Trust and Confidence.
[15] Information Commissioner's Office (2019). Information Rights Strategic Plan: Trust and Confidence.
[16] Harris Interactive (2019) for the ICO. Adtech – Market research report.
[17] Which? (2018). Control, Alt or Delete? Consumer research on attitudes to data collection and use.
[18] The Centre for Data Ethics and Innovation (2019). Interim report: Review into online targeting.
[19] Stigler Center (2019). Stigler Center committee on digital platforms – Market structure and antitrust subcommittee.

25. In addition to this, only a small minority of consumers report that they always read privacy policies or terms and conditions.[20] Academic research shows strong evidence that the number of consumers who read online policies in practice is likely to be significantly lower than that reported in consumer surveys.

26. A key reason for this lack of engagement is the length of time required to read and understand privacy policies. For example, research in 2007 estimated that a user would have to spend several weeks per year to read the privacy policies on every website they visited.[21,22] As consumers now visit more websites and the word count of the twenty most popular mobile apps' privacy policies are on average 50% longer than those studied in 2007, the amount of reading time required in 2020 is likely to be even higher than in 2007.[23]

27. Both studies and data provided by Google to the Australian Competition and Consumer Commission ('ACCC') show that even if consumers do attempt to read online policies, the average amount of time spend looking at those policies is very low – well below two minutes.[24] This suggests that consumers cannot be engaging with these policies in a meaningful way. A number of studies also argue that the online environment and the interfaces – or choice architecture – that users are presented with actually facilitates a lack of engagement with online policies on the part of consumers.[25]

28. Approximately half of consumers say they do not understand online policies when they read them.[26] Again, the academic research indicates that the actual number who do not understand online policies in practice is likely to be higher than that reported in the consumer surveys.[27] Consumers point to 'legalistic jargon' and 'blanket statements' when explaining the reading difficulty and studies have found that understanding online policies requires a high level of reading competence.[28] There is a common perception that

---

[20] Information Commissioner's Office (2019). Information Rights Strategic Plan: Trust and Confidence.
[21] European Commission (2019). Special Eurobarometer 487a: The General Data Protection Regulation.
[22] MacDonald, A. and Cranor L.F. (2008). The Cost of Reading Privacy Policies.
[23] Reading privacy policies of the 20 most used mobile apps takes 6h40
[24] Obar, J. & Oeldorf-Hirsch, A. (2016). The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services.
[25] Norwegian Consumer Council (2018). Deceived by Design; Norwegian Consumer Council (2018). Every Step You Take
[26] Harris Interactive (2019) for the ICO. Adtech – Market research report.
[27] Whitley, E. & Pujadas, R. (2018) Report on a study of how consumers currently consent to share their financial data with a third party.
[28] Cardogan, R.A. (2004). An Imbalance of Power: The Readability of Internet Privacy Policies. Journal of Business and Economic Research.

platforms purposefully make their online policies overly long and complex to the disadvantage of the consumer.[29]

29. Finally, the term 'privacy policy' can itself be misleading as some consumers incorrectly infer that a privacy policy means that the firm will not share their data with third parties.[30]

Consumers' control over their data

Do consumers feel in control of their data and to what extent do they engage with controls over their data?

30. It is clear that few consumers feel they have complete control of their data.[31, 32] While it appears that some consumers believe they can manage some aspects of data processing, such as choosing whether or not to enter information or visit a website in the first place, these same consumers feel that they have little meaningful control over how their data is used or shared once they have signed up to a platform.[33] Furthermore, as consumers learn more about data processing they begin to feel less in control and less confident in their ability to manage some aspects of data processing.[34]

31. Consumers also report that it is hard to effectively engage with companies who collect and use their data because they feel:[35,36,37]

- disempowered by their lack of knowledge and transparency about how companies collect, use and share their data;
- it is hard to access and change the personal information held by businesses;
- reliant on data-driven services which they do not believe they can give up; and,

---

[29] Which? (2018). Control, Alt or Delete? Consumer research on attitudes to data collection and use.
[30] Turow, J., Hoofnagle, C.J.,Mulligan, D.K., Good, N., and Grossklags, J. (2007). The Federal Trade Commission and Consumer Privacy in the Coming Decade.
[31] European Commission (2019). Special Eurobarometer 487a: The General Data Protection Regulation.
[32] Ipsos MORI (2016a). Digital footprints: Consumer concerns about privacy and security.
[33] Ipsos MORI (2016a). Digital footprints: Consumer concerns about privacy and security.
[34] Which? (2018). Control, Alt or Delete? Consumer research on attitudes to data collection and use.
[35] Which? (2018). Control, Alt or Delete? Consumer research on attitudes to data collection and use.
[36] Information Commissioner's Office (2019). Information rights strategic plan: Trust and confidence
[37] Miller, C., Coldicutt, R., & Kitcher, H. (2018) for Doteveryone. People, Power and Technology: The 2018 Digital Understanding Report.

- there is a perceived lack of alternatives if they want to stop using specific companies whose collection of data they are concerned about.

32. There are discrepancies regarding consumers' confidence in their ability to set and control the privacy features on their browser and social media accounts. Typically survey participants will report that they are confident in their ability to set and control privacy features but when tasked to do so in a workshop environment, many consumers struggled to accomplish this.[38,39] The participants who reported a problem commonly noted that the privacy settings were often complicated to find and use.

33. It is unclear how often UK consumers change their privacy settings although we note that a majority of UK consumers report that they have made a change at least once to the privacy settings on their browser or social media account.[40,41] However, few consumers report that they find it easy to access and change the personal information held by a business or find out how their data is collected, stored, used and shared.[42] Perhaps due to this, most consumers agree that default settings should stop their information from being shared.[43,44]

34. With regard to the General Data Protection Regulation ('GDPR'), the majority of consumers have heard of it although only half have some understanding of what GDPR entails. Overall:[45]

- the most well-known right was the right to access a user's own data;
- the most exercised right was the right to object to receiving direct marketing; and
- the least well-known and exercised right was the right to have a say when decisions are automated.

---

[38] Ipsos MORI (2016a). Digital footprints: Consumer concerns about privacy and security.
[39] The Centre for Data Ethics and Innovation (2020). Review of online targeting: Final report and recommendations
[40] European Commission (2016b). Flash Eurobarometer 443: e-Privacy
[41] European Commission (2019). Special Eurobarometer 487a: The General Data Protection Regulation.
[42] Information Commissioner's Office (2018). Information Rights Strategic Plan: Trust and Confidence.
[43] European Commission (2016b). Flash Eurobarometer 443: e-Privacy
[44] Illuminas for Citizens Advice (2016). Consumer expectations for personal data management in the digital world.
[45] European Commission (2019). Special Eurobarometer 487a: The General Data Protection Regulation.

What is the influence of behavioural biases and choice architecture on privacy decisions?

35. This is an area where there is more in the way of academic research compared to consumer survey material.

36. Making decisions about privacy and security settings in the online world is likely to be subject to the same sorts of behavioural biases as are present in the offline environment. However, the online environment may exacerbate the impact of behavioural biases because consumers have to deal with more information and face more decisions.

37. The academic literature tends to focus on a specific set of consumer biases which are ones that tend to be the most researched and best evidenced. These include:

    - status quo bias: users tend to stick with the default settings they are presented with;
    - framing or presentation effects: the way in which choices about control over the disclosure of personal information is framed can have a significant impact on what information is disclosed;
    - anchoring effects: when making a decision, users often make use of information that may not be directly relevant as a reference point;
    - loss aversion / endowment effects: users report that they would need to be paid more to give up control over their personal data than they would be prepared to pay to regain control over their personal data;
    - myopia / hyperbolic discounting: consumers place greater weight on near future outcomes and under-weight longer term effects; and,
    - 'Hot' decision-making: where an individual's decision-making can be influenced by their emotional state.

38. These biases can have a significant impact on consumers' perceptions of control and their willingness to disclose personal data. For instance, a number of studies indicate that consumers tend to accept default settings and where consumers perceive that they have control over their data (as a result of framing effects), they then tend to disclose a greater amount of personal information. A number of researchers have argued that the presence of such

biases calls into question whether the standard 'Notice and Consent' approach is sufficient on its own to protect consumers.[46]

39. We note that the literature does not discuss how these biases might interact or which are most significant in any given situation. However, a number of studies have focused on Google and Facebook, their default settings and the privacy controls that they offer. These studies find that these firms have designed their user interfaces to make the privacy-intrusive settings the default options and – in some cases – may present misleading or unbalanced information to the user.[47]

40. There is evidence from both academic research and consumer surveys that consumers expect (and indeed would prefer) default settings to be privacy focused.[48,49]

41. Studies also point out that if consumers' choices can be influenced by the choice architecture and behavioural biases, then those same factors can also be harnessed in the design of remedies to address some of the concerns identified in relation to user engagement - for instance, to improve user engagement with privacy policies or to make consumers more aware of the consequences of choosing certain privacy settings. This is considered in more detail below as part of our discussion of the implications for remedies.

Attitudes to data processing and personalised ads

What are consumer attitudes towards data processing?

42. It is clear from the surveys and academic research that consumers report that privacy is important to them, but it is hard to determine exactly how much consumers value their privacy.

Privacy Paradox

43. Research has also reported what has been termed the 'privacy paradox'. That is, consumers say privacy is very important to them, but their actions and behaviours indicate otherwise.

---

[46] Athey, S., Catalini, C., & Tucker, C. (2017) The digital privacy paradox: Small money, small costs, small talk.
[47] Norwegian Consumer Council reports: Deceived by Design (2018) and Every Step You Take (2018)
[48] Stigler Center (2019). Stigler Center committee on digital platforms – Market structure and antitrust subcommittee.
[49] European Commission (2016b). Flash Eurobarometer 443: e-Privacy

44. There is some discussion in the academic research as to whether this is in fact a genuine 'paradox'.

45. One argument is that consumers may be behaving rationally in the face of the scale of the transaction costs associated with fully evaluating the costs and benefits associated with signing up to the use of an online service provider. That is, when it comes to not reading privacy policies, consumers may be making the rational calculation that the cost of reading the policy (in terms of the time it would take to read it) exceeds the benefit of doing so, and so just choose to accept the terms and conditions without reading the privacy policy to avoid incurring that cost.

46. Another argument is that there are a range of factors which make it difficult for consumers to make effective choices. The research indicates that decisions about privacy and the disclosure of personal information are heavily context-specific and depend on the nature of the data being disclosed. As a result, general statements about privacy preferences may be of limited significance when it comes to trying to predict privacy decisions in specific circumstances.[50]

47. Another important factor which will make it difficult for consumers to make properly informed decisions relating to privacy trade-offs is that consumers struggle to anticipate what the long-term implications might be of sharing their data with platforms and so they are having to make decisions based on imperfect or asymmetric information. The large amount of information available online can make it difficult for consumers to identify information that is most relevant to them and, in particular, the way in which online services curate information may not be fully transparent. In addition, behavioural biases and cognitive limitations can also impact on consumers' decision-making.

48. The factors set out above would mean that making decisions involving privacy considerations is challenging at the best of times. However, the same factors also mean that consumers can be influenced in the decisions they make about what data they share and how much information they disclose on an on-going basis. How platforms choose to make use of default settings, how the choice of privacy setting is presented to consumers and what language is used to describe the privacy settings (the 'choice architecture') will all have an influence on consumer choices. Small incentives, navigation costs and

---

[50] Martin, K. & Shilton, K. (2016). Putting mobile application privacy in context: An empirical study of user privacy expectations for mobile devices.

irrelevant but reassuring information can influence consumers to disclose more information than they otherwise would.[51]

49. There is also an argument that consumers may simply not be making any assessment of the risks involved in sharing their data. For instance, a consumer may feel that they have no agency or control and have little choice but to accept terms that are presented on a 'take it or leave it' basis. This will be a particular issue where platforms have become 'must haves' for many users and have substantial market power.

50. In the case of decisions about privacy in an online setting, it is difficult a priori to determine which of these explanations is most relevant. All three explanations (ie consumers acting rationally; consumers' rationality being impeded; and consumers not being in a position to make active choices) are likely to be relevant to explaining user behaviour with respect to privacy in an online environment. As a result, solutions which attempt to address concerns about the collection of user data will need to take into account these different cognitive styles rather than adopting a single solution.

Attitudes to Data Processing

51. Most consumers now see data processing as a fact of modern life and that it will only become more prevalent. Despite this, there is evidence that consumers do not fully understand the role of data processing: only the most informed consumers understand that data processing is the 'price' they pay for accessing free online products or services.[52]Qualitative surveys have also found that data processing may not be a top of mind concern for most consumers when using the internet.[53,54]

52. This does not mean that consumers are comfortable with data processing. Instead, there is evidence that the majority of consumers are either uncomfortable with data processing or concerned for their privacy.[55,56] The majority of consumers also have at least one concern about data processing.[57,58] For example, most consumers are worried about their data

---

[51] Irrelevant but reassuring information could be the safety features of a similar but unrelated technology. In the paper by Athey et al (2017) it was information about encryption.
[52] Which? (2018). Control, Alt or Delete? Consumer research on attitudes to data collection and use.
[53] Which? (2018). Control, Alt or Delete? Consumer research on attitudes to data collection and use.
[54] Miller, C., Coldicutt, R., & Kitcher, H. (2018) for Doteveryone. People, Power and Technology: The 2018 Digital Understanding Report.
[55] The European Commission (2016c). Special Eurobarometer 447: Online platforms
[56] Ipsos MORI (2016a). Digital footprints: Consumer concerns about privacy and security.
[57] European Commission (2018). Special Eurobarometer 480: European attitudes towards Internet security
[58] European Commission (2019). Special Eurobarometer 487a: The General Data Protection Regulation.

being shared and this concern is magnified when the data sharing is perceived to be happening without the consumer's consent.[59] There is also evidence that the more consumers learn about data processing the more concerned they become.[60,61] That being said, the degree to which consumers are uncomfortable or concerned with data processing varies widely across the population.

53. Surveys suggest that consumers are more comfortable and accepting of data processing when:

- the data feels relevant (eg location data in maps) and is not considered sensitive (eg age versus household income);[62]
- the data is anonymised and aggregated;[63]
- there is a clear benefit to using the data for the consumer or society;[64] and,
- the NHS or other government bodies process their data instead of commercial third parties.[65]

54. Only a minority of consumers trust online platforms with their data and among these, social media platforms are the least trusted.[66,67] Research by Ofcom has found that out of Twitter, Snapchat, Instagram, YouTube and Facebook, Facebook is the least trusted platform amongst adults.[68] Some consumers also believe that platforms will do what they want with their data regardless of what the consumer agrees to.[69] This is important considering that most consumers report trust as being one of the most important considerations for them when making decisions in the online environment.[70]

What are consumer attitudes towards personalised advertising?

---

[59] Ipsos MORI (2016a). Digital footprints: Consumer concerns about privacy and security.
[60] Which? (2019). Data dozen segmentation update.
[61] Harris Interactive (2019) for the ICO. Adtech – Market research report
[62] Data and Marketing Association and Acxiom (2018). Data privacy: What the consumer really thinks.
[63] Royal Statistical Society (2014). Royal Statistical Society research on trust in data and attitudes towards data use / data sharing.
[64] Royal Statistical Society (2017). Data governance: public engagement review.
[65] Data and Marketing Association and Acxiom (2018). GDPR: A consumer perspective.
[66] Information Commissioner's Office (2018). Information Rights Strategic Plan: Trust and Confidence.
[67] Ipsos MORI (2016a). Digital footprints: Consumer concerns about privacy and security.
[68] Ofcom and Information Commissioner's Office (2019). Internet users' concern and experience of potential online harms. Page 69-70
[69] Miller, C., Coldicutt, R., & Kitcher, H. (2018) for Doteveryone. People, Power and Technology: The 2018 Digital Understanding Report.
[70] Open Data Institute (2018). Attitudes towards data sharing.

55. Not all consumers are aware that the ads they receive online can be personalised.[71] For consumers who do not mind or enjoy advertising, they would prefer to see adverts that are relevant to them instead of seemingly random ads.[72] That being said, only a minority of consumers are happy to share their data to receive ads that a relevant to them.[73,74]

56. There is also evidence that the more consumers learn about personalised advertising, the more uncomfortable they become with it and the less desirable it becomes.[75] One potential explanation for this is that most consumers believe personalised advertising operates on relatively broad or generic categories, such as gender or age and so become uncomfortable when they realise the categories are more granular.[76]

57. Consumers generally find it difficult to avoid online tracking, and only a minority of consumers feel in control of the ads they see online.[77] Where consumers do take steps to avoid adverts, the two most common reported methods are to opt-out of receiving marketing information or to use adblockers.[78] Research has also shown that some consumers will simply ignore ads if they cannot avoid them.[79]

Consumer perceptions of the benefits and harms of data processing and behaviourally based targeted advertising

58. Few surveys examine what UK consumers perceive the specific benefits or harms of data processing and targeted advertising to be. Instead, consumer surveys tend to focus on the high-level benefits and harms resulting from all forms of online targeting. Where possible we report surveys that address attitudes to personalised advertising.

59. Overall, it appears that consumers struggle to perceive any benefits of data processing unless they are provided with specific examples. In the case of personalised advertising, consumers recognise that it increases the relevance of what they are shown.[80] Some consumers also voice frustration when ads

---

[71] Ofcom (2019). Adults Media Use and Attitudes report - data tables. Table 98.
[72] Harris Interactive (2019) for the ICO. Adtech – Market research report
[73] Ofcom (2019). Adults Media Use and Attitudes report - data tables. Table 97.
[74] Oxford Internet Institute (2019). Perceived threats to privacy online: The internet in Britain.
[75] Harris Interactive (2019) for the ICO. Adtech – Market research report.
[76] Which? (2018). Control, Alt or Delete? Consumer research on attitudes to data collection and use.
[77] Harris Interactive (2019) for the ICO. Adtech – Market research report.
[78] Ofcom (2019). Adults Media Use and Attitudes report - data tables. Table 95
[79] Drèze and Hussherr (2003) Internet advertising: Is anybody watching?
[80] Which? (2018). Control, Alt or Delete? Consumer research on attitudes to data collection and use.

are not related to their interests. However, there is also evidence that very few consumers are willing to share their data in return for these benefits.

- In 2018 Ofcom found that only 15% of respondents were happy for online companies to collect and use their data in return for a personalised service. [81]

- In 2016 Ipsos MORI found that only 5% of respondents felt that companies using their personal information to send more personalised adverts and marketing materials to try and sell more goods and services benefited them greatly. [82]

60. On the other hand, consumers struggle to pinpoint specific examples of harms as a result of data processing or behaviourally based targeted advertising. However, there were a series of general concerns which did emerge from those surveys, including:

- loss of privacy;

- the use of inaccurate or personal data in automated decisions;

- loss of control over both data and ads;

- breaches to data security; and

- a lack of trust in the organisations that enable data processing and targeted advertising.

61. One of the reasons that consumers may struggle to articulate either the benefits or the harms from personalised advertising is the fact that – as indicated above - few consumers understand what, how and why data is collected and shared, or how behaviourally-based targeted advertising operates. Combined with the inherent opaqueness in data processing and online targeting, and psychological biases, this indicates that consumers' ability to anticipate potential harms and benefits is likely to be substantially constrained.

62. Recent qualitative research from Which? examined methods used to collect data for personalised advertising. Although Which? found that a majority of participants had a preference to receive targeted, rather than generic, adverts,

---

[81] Ofcom (2019). Adults Media Use and Attitudes report - data tables. Table 98
[82] Ipsos MORI (2016a). Digital footprints: Consumer concerns about privacy and security.

participants also had a clear preference that they should have to opt-in to data collection for targeted advertising, rather than opt-out.[83]

Implications for remedies

How can issues with choice architecture and behavioural biases be addressed?

63. As indicated above, a number of studies have identified that an awareness of consumer biases and the potential for the manipulation of user interfaces can itself be harnessed to assist users to make better choices about their privacy.

64. In terms of information-based remedies, there is evidence that simplifying privacy policies could improve consumer engagement rates.[84] Other options such as adding quality cues or estimated reading times have also been shown to improve engagement rates in experimental settings.[85] A significant majority of consumers also express a desire for online policies to be simplified.[86]

65. There is also scope for the choices available to consumers to be adapted to 'nudge' them towards better choices. 'Nudging' interventions are ones which are designed to address issues arising from cognitive or behavioural biases. A key aspect of a nudge intervention is that it should change the choice architecture to nudge consumers to make decisions that are better aligned with their privacy objectives but does not actually restrict the user's set of choices.

66. Studies have pointed to the importance of a number of behavioural influences which can assist in making 'nudges' more effective:

- *Feedback:* for example, providing consumers with information as to who can see their personal data and how much information is collected about them can be important in exposing them to the implications of their privacy decisions.

- *Framing:* how privacy decisions are presented to consumers (eg whether data is sensitive or not) can influence the amount of data that is revealed.

---

[83] Which? (2020). Are you following me? Consumer attitudes towards data collection methods for targeted advertising
[84] European Commission (2016a). Study on consumers' attitudes towards online terms and conditions.
[85] European Commission (2016a). Study on consumers' attitudes towards online terms and conditions.; The Behavioural Insights Team (2019) The behavioural science of online harm and manipulation, and what to do about it.
[86] Ipsos MORI (2016a). Digital footprints: Consumer concerns about privacy and security.

- *Timing / Saliency:* the point at which information is provided to consumers can have a significant impact on how deeply they engage in thinking about privacy decisions.

67. More specifically, the Behavioural Insights Team carried out a series of experiments which were intended to identify those approaches which were effective in improving consumers' understanding and, as importantly, identifying those measures where the evidence was more mixed or indeed suggested that certain approaches were not effective.[87] Techniques which were found to be effective included: displaying key terms as frequently asked questions; using icons to illustrate key terms; and, providing information in short chunks at the right time. Techniques where the evidence was mixed or indicated that techniques were not effective included: presenting key points in a summary table; adding examples and icons to the full terms; and, making summaries expandable, allowing customers to click each summary point for more information.

68. Other research indicates that seemingly small implementation decisions can have a significant impact on whether and how consumers people interact with consent notices. For instance, how data privacy options are displayed in a screen vertically (ie whether one option is positioning higher than the other) may influence the proportion of users that will choose a given option.[88]

69. For instance, one study found that consumers were more likely to interact with a consent notice placed in the lower part of the screen compared to other positions. It was suggested that if consumers used their thumbs to navigate websites on a smartphone, then it would be easier to tap elements on the bottom part of the screen than those at the top[89]. These findings point to the need to consider issues such as the ergonomics of design features as well as the content and way in which choices are presented to consumers. These findings also point to the need to trial different approaches.

70. An important message from the academic research is that different nudge approaches should be regarded as complements rather than substitutes: there is not a single 'silver bullet' which would address all the concerns

---

[87] Behavioural Insights Team (2019). 'Best practice guide. Improving consumer understanding of contractual terms and privacy policies: evidence-based actions for businesses.'
[88] Acquisti, A., John, L.K. and Loewenstein, G. (2013) 'What is Privacy Worth?' The Journal of Legal Studies, Vol. 42, No. 2, 249-274.
[89] Utz, C., Degeling, M., Fahl, S., Schaub, F., and Holz, T. (2019) (Un)informed Consent: Studying GDPR Consent Notices in the Field.

identified in relation to the way consumers make decisions about their privacy.[90]

Do consumers want more control over their data? If so, is that level of control practical?

71. There is evidence that control over one's own data is very important for consumers and that a significant majority of consumers want more control over the data they provide to platforms. [91,92] However, Which? has argued that it might not be practical to give consumers themselves more control over their data.[93] Instead, they argue that consumers would be better served by improved control and regulation within the data ecosystem. This could include clearer accountability when data is treated improperly or if a data breach occurs.

72. There is strong evidence that consumers also want more regulation for online platforms and data processing. Research has also shown that government regulation is perceived to help reduce online privacy concerns.[94] It appears this finding may be underlined by the fact that most consumers perceive online media to be less regulated than traditional media.[95]

73. The Stigler Center (2019) has outlined a number of reasons why government regulation is necessary for consumers' best interests:[96]

- the harms of privacy and security breaches are not internalised by firms;
- it is costly for consumers to monitor the consequences of privacy and security breaches;
- a great deal of information is held by firms with which consumers have no direct contact and little influence over; and
- consumers are often left to bear the burden of privacy and security breaches themselves despite rarely knowing what actions they can take.

---

[90] WIK-Consult (2015) Personal data and privacy. A report for Ofcom.
[91] Miller, C., Coldicutt, R., & Kitcher, H. (2018) for Doteveryone. People, Power and Technology: The 2018 Digital Understanding Report.
[92] Data and Marketing Association and Acxiom (2018). Data privacy: What the consumer really thinks.
[93] Which? (2018). Control, Alt or Delete? Consumer research on attitudes to data collection and use.
[94] Škrinjarić, B., Budak, J. & Rajh, E. (2018). Perceived quality of privacy protection regulations and online privacy concern.
[95] Ofcom and Information Commissioner's Office (2019). Internet users' concerns about and experiences of potential online harms. Page 68
[96] Stigler Center (2019). Stigler Center committee on digital platforms – Market structure and antitrust subcommittee.

74. In the presence of tracking technologies that allow merchants to infer consumers' preferences and engage in price discrimination, the usefulness of privacy regulatory protection will depend on consumers' level of sophistication. Regulation would be necessary if consumers were not aware of how merchants were using their data (to price discriminate) and could not adapt their purchasing habits accordingly.

Analytical Framework: The Economics of Privacy

75. There are a variety of factors which are relevant to the analysis of data privacy issues from an economic point of view.

76. Decisions about sharing personal information typically involve a trade-off for the consumer. In order to access a service or to benefit from a price discount etc, the consumer has to disclose some data about themselves to the firm. For instance, disclosure of some personal data can help to inform the targeting of the advertising that a user is presented with so that they only see adverts which are relevant to them. It can also result in improved services and potentially mean that consumers are offered cheaper prices if firms choose to price discriminate or to offer promotions to certain customer groups. Disclosure of personal data by consumers also benefits firms in terms reducing the costs of targeting and enabling efficiency gains leading to increased revenues.

77. At the same time, disclosure of personal data exposes consumers to a series of information asymmetries and risks which can be difficult for them to assess and quantify: consumers' personal data can be shared with third parties without the users' knowledge or permission; data can be collected on an on-going basis; firms holding personal data can be subject to security breaches; consumers can be exposed to identity theft etc.

78. It is therefore up to the consumer to decide how much they value a service and whether those benefits outweigh the costs that arise from that loss of privacy. All other things being equal, we might expect that the more valuable the service, the greater the privacy ‘cost’ a consumer would be willing to accept and the more data they would be prepared to share.

79. These issues are not limited to an online environment - similar considerations will apply to the disclosure of personal information in an offline setting. What makes these issues more complex in an online environment, however, is that these information asymmetries are compounded. For instance, relative to the firms collecting data about uses, users do not know the scale and frequency with which firms are collecting data about them or how that data will be used.

In addition, there is an absence of anyone to point the user to the important parts of the terms and conditions or privacy policies; there is no physical signature involved, which could present a stronger barrier than a simple click of a button; and consumer often have to rely on rules of thumb (or heuristics) to help simplify their decision-making choices (WIK-Consult, 2015).

80. These factors make it difficult for users to weigh up the costs and benefits of disclosing personal data. In many cases, markets can help deal with these issues by bringing together buyers and sellers and setting a market price. However, there is an absence of markets for personal data which would help users to put an economic value or price on their data.

81. Indeed, what elevates the significance of data privacy in an online world is that the collection of personal data is at the core of many online firm's business models. That is many platforms are free or provide free services to consumers in return for collecting their personal data on an on-going basis. This means that the incentives on firms may be skewed towards the collection of as much data as possible (in the absence of legal constraints).

Privacy Paradox

82. Before getting into the main report proper, we note that the academic research (eg Brown (2001), Acquisti (2004), Barnes (2006), Acquisti et al (2016), Kokolakis (2017), Barth and de Jong (2017)) has discussed the existence of a so-called 'privacy paradox' in relation to the collection of data from users in an online environment. That is, in surveys consumers will say that they are very concerned about their privacy, but they then behave in a way that contradicts this clearly stated preference eg by not taking advantage of privacy controls that are available to them. The apparent contradiction in the behaviour is an issue which runs through much of the research on privacy and privacy behaviour.

83. There has been some debate about whether this is in fact a true paradox. One argument is that consumers may be behaving rationally in the face of the scale of the transaction costs associated with fully evaluating the costs and benefits associated with signing up to use an online service provider. That is, when it comes to not reading privacy policies, consumers may be making the rational calculation that the cost of reading the policy (in terms of the time it would take to read it) exceeds the benefit of doing so and so choose not to accept the terms and conditions without reading the privacy policy to avoid incurring that cost.

84. Another argument is that there are a range of factors which make it difficult for consumers to make effective choices.

85. The research indicates that decisions about privacy and the disclosure of personal information are heavily context-specific and depend on the nature of the data being disclosed. As a result, general statements about privacy preferences may be of limited significance when it comes to trying to predict privacy decisions in specific circumstances.

86. There are also other factors which will make it difficult for consumers to make properly informed decisions relating to privacy trade-offs. One key factor is that it is difficult for consumers to anticipate what the long-term implications might be of sharing their data with platforms and so they are having to make decisions based on imperfect or asymmetric information. The large amount of information available online can make it difficult for consumers to identify information that is most relevant to them and, in particular, the way in which online services curate information may not be fully transparent. People will often be unaware of the information they are sharing and not be aware of how that information can be used.

87. In addition, behavioural biases and cognitive limitations can also impact on consumers' decision-making. Acquisti et al (2015) have argued that uncertainty and context dependency mean that people may not be able to navigate the complex trade-offs involving privacy in a self-interested fashion.

88. The factors set out above would mean that making decisions involving privacy considerations is challenging at the best of times. However, the same factors also mean that consumers can be influenced in the decisions they make about what data they share and how much information they disclose on an on-going basis. How platforms choose to make use of default settings, how the choice of privacy setting is presented to consumers and what language is used to describe the privacy settings (the 'choice architecture') will all have an influence on consumer choices.

89. Thaler et al (2014) have pointed out that choice architects will not always have the best interests of the people they are influencing in mind and that 'wily but malevolent' architects can have devastating effects on the people who are influenced by them. This concern can also be extended where choice architecture can be employed to shift consumers towards behaviours that primarily benefit data collection organizations (Acquisti et al, 2015).

90. Research suggests that consumers with privacy concerns can be reluctant to take the necessary steps to become more informed, even when the information to protect their privacy is made readily available (Acquisti and

Grossklags, 2005). Other research has also found that where securing privacy requires additional effort or comes at cost of a less smooth user experience, consumers were quick to abandon technology that would offer them greater protection (Athey et al, 2017).

91. There is also research which indicates that some consumers believe that a privacy policy means that their privacy is protected as the default (Turow et al, 2007, Martin 2015). That is, a majority of consumers believed that the term 'privacy policy' described a baseline level of information practices that protected their privacy.[97] When consumers saw the term 'privacy policy, 'they believed that their personal information would be protected and, in particular, they assumed the website would not share their personal information.

92. As a result, not only are actual privacy decisions heterogeneous and highly context specific (as opposed to broad statements about attitudes to privacy) but there can also be a range of factors which prevent consumers from expressing their true privacy preferences and biases can have a significant impact on consumer decision making.

93. Users could be attempting to carry out a rational assessment of the costs and benefits but behavioural biases such as the use of 'rules of thumb' and optimism bias, together with information asymmetries and cognitive limitations, means that they reach the wrong conclusions. Experimental work carried out by Adjerid et al (2017) has identified the possibility that – comparing hypothetical to actual choice contexts – consumers may overestimate their response to standard factors and underestimate that response to behavioural factors.

94. There is also an argument that consumers may simply not be making any assessment of the risks involved in sharing their data. For instance, a consumer may feel that they have no agency or control and have little choice but to accept terms that are presented on a 'take it or leave it' basis. This will be a particular issue where platforms have become 'must haves' for many users and have substantial market power.

95. In the case of decisions about privacy in an online setting, it is difficult a priori to determine which of these explanations is most relevant. Barth and de Jong (2017) suggests that all three explanations (ie consumers acting rationally; consumers' rationality being impeded; and consumers not being in a position to make active choices) are likely to be relevant to explaining user behaviour with respect to privacy in an online environment. As a result, solutions which

attempt to address concerns about the collection of user data will need to take into account these different cognitive styles rather than adopting a single solution.

Structure of the Review

96. Our review of both the academic research on privacy issues and consumer surveys on the collection of user data seeks to assess and summarise these issues in a structured way. It should be noted that not we have not necessarily been able to attribute both academic and consumer survey research to each of the specific sub-questions that we have used to structure the review.

97. Where relevant we seek to present areas where there appears to be a general agreement in terms of the available evidence about the significance of the various factors listed above. In other areas we simply try to set out the parameters of the academic debate or identify where further consumer research may be required.

98. We should stress that our review of the consumer and academic research is not intended to be a systematic review in a formal, academic sense. Rather we are seeking to bring together the most relevant academic literature and consumer survey material to establish what the available evidence is on the three topics set out above and to inform the analysis set out in the main report. We are also looking to identify where there might be gaps in the evidence base and where further research would be useful.

TOPIC 1

How much do consumers know or think they know about data processing?

99. In this section we refer to both awareness and knowledge according to the nature of the research, but we recognise that the two can have different implications for consumer behaviour. Awareness describes perception and cognitive reaction but does not necessarily imply understanding. That is, awareness is a more ‘passive’ position than knowledge and understanding: the fact that consumers are aware of an issue does not imply that they will then act on that awareness.

What do consumers know about the value of data to platforms?

Consumer Research

100. There is some evidence that consumers understand that personal data is valuable to online platforms. Most consumers also agree that companies benefit the most from data collection. and consumers also tend to believe that companies collect data for their own benefit. Ipsos MORI asked respondents what they believed were the main reason companies collect personal information and found that:[98]

- 41% believed it was to send customers more marketing;
- 39% believed it was to sell data to other companies; and
- 14% believed it was primarily collected to create new products or services.

101. In qualitative interviews by Which? and Doteveryone, respondents were more likely to say that data was collected for business purposes, such as sending marketing emails than other reasons.[99,100]

Are consumers aware of what data is or can be collected by platforms?

Consumer research

102. Overall, most consumers are unsure of the information online platforms hold about them. As Ipsos MORI found, 83% of UK respondents did not know what personal information companies hold about them.[101]

103. Most consumers recognise that information they actively enter online is collected by platforms:

- Research for Doteveryone in 2020 found that 85% of respondents understood that organisations collect information by tracking what they do online.[102]

---

[98] Ipsos MORI (2016a). Digital footprints: Consumer concerns about privacy and security.
[99] Which? (2018). Control, Alt or Delete? Consumer research on attitudes to data collection and use.
[100] Miller, C., Coldicutt, R., & Kitcher, H. (2018) for Doteveryone. People, Power and Technology: The 2018 Digital Understanding Report.
[101] Ipsos MORI (2016b). Awareness of personal information held by companies.
[102] Miller, C., Kitcher, H., Perera, K. & Abiola, A., (2020) for Doteveryone. People, Power and Technology: The 2020 Digital Attitudes Report

- Harris Interactive research for the ICO found that 76% of respondents were aware that browsing history was collected, 76% were aware that search history was collected and 69% were aware that purchase history was collected.[103]

- The CDEI found that focus group participants tended to be aware that browsing history and location data could be used to personalise adverts.[104]

104. In contrast, there is less awareness of information that consumers do not actively volunteer, such as an IP address:

- Harris Interactive research for the ICO found that only 47% of respondents knew that device identifiers can be collected.[105]

- In 2018 Doteveryone found that only 38% of respondents thought data about their internet connection was collected and only 17% believed that information others share about them was collected.[106]

- The CDEI found that only 7% of participants believed that information about who people interact with online could be used in online targeting.[107]

105. Consumers' awareness of what data is collected also depends on the context in which it takes place. For example, consumers are more likely to believe that a map app collects location information than a crossword app.

106. Most consumers struggle to estimate how much data companies have about them but there is a common perception that companies collect a large amount of data. The Royal Statistical Society review found that consumers believed organisations collected too much data about them.[108] In 2016 Ipsos MORI found that 42% of respondents believed that companies collected a great deal of data about them.[109] A further 45% felt that companies had a fair amount of data on them.

107. Despite this perception, most consumers are unaware of the wide range and volume of data that is or can be collected about them. Which? gave focus

---

[103] Harris Interactive (2019) for the ICO. Adtech – Market research report
[104] The Centre for Data Ethics (2020). Review of online targeting: Final report and recommendations.
[105] Device identifiers are characteristics of the device being used, such as phone model or the operating system.
[106] Miller, C., Coldicutt, R., & Kitcher, H. (2018) for Doteveryone. People, Power and Technology: The 2018 Digital Understanding Report.
[107] The Centre for Data Ethics (2020). Review of online targeting: Final report and recommendations.
[108] This review examined consumer surveys towards data processing and privacy from 2009 to 2017. Royal Statistical Society (2017). Data governance: public engagement review.
[109] Ipsos MORI (2016a). Digital footprints: Consumer concerns about privacy and security.

group participants the privacy policies of major online companies such as Google and Facebook and despite most respondents believing that companies collected a significant amount of data about them, all but the most informed participants were unaware of the actual volume of data that was being collected.[110] These consumers were also unaware that entire data profiles could be constructed about them as well.

Academic Research

108. There appears to be little academic research which focuses specifically on whether consumers know how much data is collected about them or what that data might relate to. Instead research has tended to focus on the scale of data collection and how that content is collected in the first instance.

109. Digital Content Next (2018) monitored an Android phone with a single Chrome browser operating in the background. Over a 24-hour period and without any user interaction, the phone communicated approximately 900 data samples to a variety of Google endpoint servers. Of these data samples, approximately 35% were location related.

110. The Norwegian Consumer Council ('NCC') (2018) looked at how Google continuously tracks the location of its users through a number of different technologies. This tracking is implemented and enabled through the features 'Location History' and 'Web & App Activity'. The NCC argued that since the Web & App Activity setting was enabled by default, users that did not click 'More options' would not be aware that this data collection was happening.

111. It is unlikely that consumers are aware that so much data is potentially being collected about them and it is unlikely that they are aware of the type of data is being collected.

Are consumers aware of how data is or can be collected?

Consumer Research

112. Most consumers only have a basic understanding of how their data can be collected. For example, Ofcom presented respondents with four methods of data collection – through cookies, social media accounts, registration forms

[110] Which? (2018). Control, Alt or Delete? Consumer research on attitudes to data collection and use.

and smartphone apps.[111] While 82% of consumers were aware of at least one of these methods, only 37% were aware of all four methods.

113. Most consumers recognise active forms of data-collection but are generally less aware of passive methods of data collection:[112]

- In 2018 Ofcom found that 57% of respondents were aware that platforms collected information by asking customers to register with a website or app but only 49% were aware that apps on smartphones collected data on users' locations or what products and services interest them.[113]

- In its 2016 survey Ipsos MORI found that 66% of respondents recognised that companies collected data by asking consumers to register details but only 52% were aware that mobile phone applications collected location information and what products they are interested in to provide personalised advertising.[114]

114. One exception to the above is that most consumers are aware of cookies. In its 2016 survey Ipsos MORI found that 64% of respondents reported an awareness of cookies.[115] Similarly, in 2018 Ofcom found that 71% of respondents claimed they were aware that cookies were used to collect data.[116] However it is not clear if consumers understand how cookies operate as the surveys only asked respondents about general awareness.

115. A small minority of consumers falsely believe that incredibly invasive data collection takes place. Such misconceptions included the belief that any conversations made near or on internet-connected devices were being secretly recorded.[117]

116. There is some evidence that consumers are becoming more likely to report that they are aware of how data is collected over time:

- Ofcom found that the percentage of people who were aware that mobile apps collected location data increased from 45% in 2017 to 49% in 2018.[118]

---

[111] Ofcom (2019). Adults Media Use and Attitudes report - data tables. Table 97
[112] An example of active data collection is the use of registration forms. An example of a passive form of data collection are apps collecting location data when they're not in use.
[113] Ofcom (2019). Adults Media Use and Attitudes report - data tables. Table 97
[114] Ipsos MORI (2016a). Digital footprints: Consumer concerns about privacy and security.
[115] Ipsos MORI (2016a). Digital footprints: Consumer concerns about privacy and security.
[116] Ofcom (2019). Adults Media Use and Attitudes report - data tables. Table 97
[117] Which? (2018). Control, Alt or Delete? Consumer research on attitudes to data collection and use.
[118] Ofcom (2019). Adults Media Use and Attitudes report – chart pack. Page 98

- In 2017 the DMA found that 67% of respondents agreed that they felt more aware of how their data is used and collected than in the past.[119]

Academic research

117. Digital Content Next (2018) found that two-thirds of the information collected or inferred by Google through an Android phone and the Chrome browser was done through 'passive' methods, that is where an application is set up to gather information while it is running, possibly without the user's knowledge. The report defined Google's passive data gathering methods in terms of data from platforms: (eg Android and Chrome); applications (eg Search, YouTube, Maps) publisher tools (eg Google Analytics, AdSense); and, advertiser tools (eg AdMob, AdWords).

118. The report found that even when a user avoids interacting with prominent Google applications, Google was still able to collect a significant amount of information through its advertiser and publisher products.

Are consumers aware of how data is or can be used?

Consumer Research

119. Most consumers report that they have some awareness of how their personal data is used but very few feel fully informed. For example, the Information Commissioner's Office ('ICO') found that 73% of respondents felt that they had at least a familiar understanding of how personal data is used.[120] However, only 16% of respondents felt that they had a good understanding of how personal data is used.

120. Consumers' awareness of how data is used is largely related to what they can see, such as recommendations or personalised advertising. For example:

- In 2020 Doteveryone found that 79% of respondents recognised that personal information is used to target advertising while 75% recognised that it is used to tailor information to the individuals[121]. At the same time, they also reported that this understanding remained 'shallow'.

[119] Data and Marketing Association and Acxiom (2018). Data privacy: What the consumer really thinks.
[120] Information Commissioner's Office (2019). Information Rights Strategic Plan: Trust and Confidence.
[121] Miller, C., Kitcher, H., Perera, K. & Abiola, A., (2020) for Doteveryone. People, Power and Technology: The 2020 Digital Attitudes Report

- In 2018 Which? found that respondents focused on how data is used to personalise services and were surprised that data could be used to determine prices.[122]

- Research for the Economic and Social Research Council ('ESRC') found that some focus group participants recognised that their data can be used to improve the service or product they are receiving.[123]

121. When evaluating consumers' understanding of data processing, the Stigler Center (2019) explained that it is fundamentally difficult for consumers to anticipate all the ways in which their data can be used. For example, advances in computing power and data mining can create new uses of old data that is unforeseeable to consumers.

122. There is some evidence that consumers' understanding of how data can be used is increasing. The ICO found that the percentage of respondents who felt like they had at least a familiar understanding of how their personal data is used increased by 11 percentage points between 2017 and 2019.[124] Doteveryone found that the number of respondents who understood that platforms collect information to target advertising and tailor information increased by 9 and 15 percentage points respectively. [125, 126]

Are consumers aware of how their data is or can be shared?

Consumer Research

123. On the whole consumers are aware that their data is shared although only a minority of consumers claim they have a good understanding of how their data is shared. For example, the ICO found that only 15% of respondents felt that they had a good understanding of how their personal data is made available to third parties and the public by companies and organisations in the UK.[127]

124. Which? similarly found that most respondents had some awareness of data sharing but there was a common misconception that data sharing is

---

[122] Which? (2018). Control, Alt or Delete? Consumer research on attitudes to data collection and use.
[123] Hopkins Van Mil (2015). Big Data: Public views on the use of private sector data for social research.
[124] Information Commissioner's Office (2018). Information Rights Strategic Plan: Trust and Confidence; Information Commissioner's Office (2019). Information Rights Strategic Plan: Trust and Confidence
[125] Miller, C., Coldicutt, R., & Kitcher, H. (2018) for Doteveryone. People, Power and Technology: The 2018 Digital Understanding Report.
[126] Miller, C., Kitcher, H., Perera, K. & Abiola, A., (2020) for Doteveryone. People, Power and Technology: The 2020 Digital Attitudes Report
[127] Information Commissioner's Office (2019). Information Rights Strategic Plan: Trust and Confidence

'bounded'.[128] The idea that data can be combined, aggregated and shared was described as 'an important penny-drop' moment for consumers. Respondents were also unaware of the extent to which data sharing occurs and that an entire industry of data brokers focused on sharing and selling consumer data existed. [129]

125. We note that surveys from other countries also demonstrate that most consumers are aware that data can be shared. Deloitte found that 78% of American respondents believe that personal data is shared with third parties.[130] Similarly, the ACCC found that 80% of Australian respondents agreed that organisations exchange data about them with third parties.[131]

Academic research

126. Research indicates that it can be easy for consumers' data to be shared and combined without their knowledge. In examining the actual cost of internet services which have a zero monetary price, Hoofnagle and Whittington (2013) demonstrated that a user's profile can end up on a firm's servers even if they have no direct contact with service provider.[132] They argued that information-intensive companies misuse the term 'free' to promote products and services that actually involve non-monetary costs for the user and in doing so ignore consumer preferences for privacy.

127. The Stigler Center (2019) also argued that a consumer can come into direct and indirect contact with hundreds of companies and it was highly unlikely that they would have the capacity to understand the implications of sharing data with each company.

Are there any differences between consumer groups?

Consumer Research

128. For the most part men and those who describe themselves as confident internet users are more likely to report a greater awareness of data processing. For example:

---

[128] This is the belief that individual pieces of data are given to an organisation in order to receive a specific product or service.
[129] Which? (2018). Control, Alt or Delete? Consumer research on attitudes to data collection and use.
[130] Deloitte (2017). 2017 Global mobile consumer survey: US edition.
[131] Roy Morgan – prepared for Australian Competition and Consumer Commission (2018). Consumer views and Behaviours on Digital Platforms.
[132] Hoofnagle, C., & Whittington, J. (2013). Free: accounting for the costs of the internet's most popular price.

- In 2019 the ICO found that 19% of male respondents felt like they had a good understanding of how their personal data is used compared to 13% of females.[133]

- In 2018 Ofcom found that 41% of male respondents were aware of all four methods of data collection (cookies, social media accounts etc) compared to 33% of female respondents.[134]

- In 2016 Ipsos MORI found that 42% of users who described themselves as confident internet users were aware that companies sold personal data to other companies compared with 25% of those who described themselves as having low confidence.[135]

- Ipsos MORI also found that 23% of respondents who had low confidence could not describe any reason why companies collect personal data as opposed to 3% of those who described themselves as confident.

Are there any discrepancies between what consumers think they know and what they actually know?

Academic Research

129. There is consensus in academic literature that consumers do not have a comprehensive understanding of data processing. For example:

    - In a study of American internet users, Turow et al, (2005) found that users were aware that their internet activity was being tracked but were not aware of the extent to which their data was being shared.

    - Winegar and Sunstein (2019) also found that consumers typically have highly imperfect information about whether their data was collected, what data was collected and how their data was used by online advertisers.

    - Whitley & Pujadas (2018) found that consumers do not fully understand how data can be used or combined to make money.

130. The Stigler Center (2019) suggested that firms often did not face strong incentives to differentiate themselves on the basis of privacy as privacy is not a top-of-mind concern when a consumer is considering a good or service.

---

[133] Information Commissioner's Office (2019). Information Rights Strategic Plan: Trust and Confidence.
[134] Ofcom (2019). Adults Media Use and Attitudes report - data tables. Table 97
[135] Ipsos MORI (2016a). Digital footprints: Consumer concerns about privacy and security.

Furthermore, a firm that wanted to emphasise its privacy strengths had to be careful to do so without scaring consumers away from their products entirely.

131. Finally, Acquisti et al (2016) explained that consumers do not understand the consequences of the processing of their personal data. Information asymmetries mean that consumers are not usually in a position to understand when their data is collected, for what purposes, and with what consequences.

Consumer research

132. It is not possible to conclusively say from the consumer survey research whether or not any discrepancies exist. However, there is some evidence that consumers may overestimate their knowledge of data processing. For example, Which? found that even though consumers believed online platforms collected significant amounts of data they were still surprised at the amount of data requested in privacy policies of major online platforms.[136] Similarly, the CDEI found that all the participants in a series of focus groups reported being shocked at the prevalence and sophistication of online targeting systems. Common unknowns included: the prevalence of the use of online targeting practices across the internet; the range of different data being used; the sophistication of digital profiles; and, the inferences that can be made about user characteristics and preferences[137]

Are consumers engaging effectively with terms and conditions and privacy policies?

133. In this section we set out our findings from consumer surveys and academic research. In Chapter 4 we also set out data we gathered directly from platforms about the extent of users' engagement with privacy settings in practice, including data on the proportion of users that engage with Privacy Policies and different privacy controls and settings.

To what extent do consumers read these policies?

Academic Research

134. Academic research is clear that consumers do not read terms and conditions or privacy policies (Good et al (2006), Bakos et al (2014)). However, this is not a new phenomenon. Before the rise of online services, it was generally assumed that consumers did not read the fine print of terms and conditions

[136] Which? (2018). Control, Alt or Delete? Consumer research on attitudes to data collection and use.
[137] The Centre for Data Ethics and Innovation (2020). Review of online targeting: Final report and recommendations

(Becher & Unger-Aviram (2010)). 'Clicking without reading' can thus be seen as a modern-day extension of the 'signing without reading' phenomenon that had already been identified.

135. The research indicates that the context or subject matter of a contract is still an important factor in determining engagement with terms and conditions. Becher and Unger-Aviram (2010) found that more mundane topics (eg opening a bank account) might attract a low level of readership whereas an activity affecting a child (eg signing a contract for a nursery) would attract a high level of readership.

136. However, WIK-Consult (2015) has shown that the 'signing without reading' phenomenon can be exacerbated in the online environment as such an environment supports a reduction in the level of engagement:

- there is no one to point out the important parts of the terms and conditions; no physical signature is required;
- the default setting is typically 'I Agree'; and
- the consumer is deemed to have agreed to the terms and conditions just by continuing to use the website.

137. Consumers are also exposed to many more privacy policies online even though for most consumers, over half of all website visits last less than 15 seconds (WIK-Consult, 2015). It has also been estimated that around 20% of mobile apps that are downloaded are then only used once.[138]

138. Research has consistently demonstrated that very few consumers access privacy policies:

- Bakos et al (2014) examined consumers' actual behaviour and found that only 0.05% of agreements were accessed by consumers before they consented to them.[139]
- In experiments involving privacy policies, The European Commission (2016a) found that only 9.4% of participants accessed the terms and conditions when it was optional.

[138] Localytics (2014): App Retention improves – Apps Used Only Once Declines to 20%, http://info.localytics.com/blog/app-retention-improves.
[139] The study involved tracking the internet browsing behaviour of 48,154 monthly visitors to the web sites of 90 online software companies to study the extent to which potential buyers access the end-user license agreement.

- Obar & Oeldorf-Hirsch (2018) conducted an experimental survey and found that 74% of respondents did not open the privacy policy.

139. Even when consumers do access a privacy policy it does not mean they are fully engaged:

- Bakos et al (2014) found that the users that accessed an End User Licensing Agreement ('EULA') spent just an average of just over 60 seconds on that page (with a median time of just over 30 seconds).
- Obar & Oeldorf-Hirsch (2018) found the average reading time for a privacy policy in an experimental setting of 73 seconds.
- In submissions to the ACCC by Google, the average time spent by Australian users viewing the Google Privacy Policy web page was less than two minutes and only 0.03% spent more than 10 minutes on the Privacy Policy web page.[140]

140. Academic research has identified time as the predominant reason for consumers' disengagement with terms and conditions. McDonald and Cranor (2008) drew on empirical evidence and found that, on average, a user would have to spend several weeks per year to read the privacy policies on each website they visited. As this research was carried out in 2007 it is likely to underestimate the reading time as internet use and the number of websites visited has increased significantly since then.

McDonald and Cranor calculated the time to read privacy policies using a list of the 75 most popular websites [from AOL search data in October 2005] and assumed an average reading rate of 250 words per minute to find an average reading time of 10 minutes per policy. They then used data from Nielsen/Net Ratings to estimate the number of unique websites the average US Internet user visited annually, with a lower bound of 119 sites. They estimated that reading privacy policies would amount to approximately 201 hours a year.

Consumer surveys

141. Only a minority of consumers claim to always read the policies provided by online platforms:

- In 2020 Ofcom research found that only 15% of respondents strongly disagreed with the statement that they 'always agreed to terms and

[140] Australian Competition and Consumer Commission (2019). Digital platforms inquiry – final report.

conditions without reading them so that they could access the service or content.' [141]

- In 2018 Ofcom also found that only 12% of respondents strongly disagreed with the statement that they usually accept website or apps terms and conditions without reading them.[142]

- In 2019 the European Commission found that only 13% of respondents claimed they fully read privacy policies online.[143]

- In 2016 Ipsos MORI found that only 14% of respondents reported always reading privacy statements or terms and conditions to inform their decision about whether or not to use a site or service.[144]

142. There is some variation in the surveys about the proportion of consumers who do not normally read the policies provided by online platforms:

- In 2020, Ofcom found that 53% of respondents agreed that they always agree to terms and conditions without reading them so they can access a service or content.[145]

- In 2018 Ofcom found that 69% of respondents agreed that they usually accept website or apps terms and conditions without reading them.[146]

- In 2019 the European Commission found that 85% of respondents claimed they either read privacy policies partially or not at all.[147]

- In 2016 Ipsos MORI found that that 57% of respondents claimed they rarely or never read privacy policies to inform their decision about using an online service or site.[148]

- In both focus groups for Which? and research for the ESRC, most participants admitted that they do not normally read privacy policies.[149,150]

143. International surveys have indicated even higher levels of non-engagement. A Deloitte survey found that 91% of American respondents agreed that they

---

[141] Ofcom (2020). Internet users' experience of harm online – data tables. Table 265
[142] Ofcom (2019). Adults Media Use and Attitudes report - data tables. Table 81
[143] Ipsos MORI (2016a). Digital footprints: Consumer concerns about privacy and security.
[144] Ipsos MORI (2016a). Digital footprints: Consumer concerns about privacy and security.
[145] Ofcom (2020). Internet users' experience of harm online – data tables. Table 265
[146] Ofcom (2019). Adults Media Use and Attitudes report - data tables. Table 81
[147] European Commission (2019). Special Eurobarometer 487a: The General Data Protection Regulation.
[148] Ipsos MORI (2016a). Digital footprints: Consumer concerns about privacy and security.
[149] Which? (2018). Control, Alt or Delete? Consumer research on attitudes to data collection and use.
[150] Hopkins Van Mil (2015). Big Data: Public views on the use of private sector data for social research.

normally accept terms and conditions without reading them.[151] The ACCC found that only 5% of Australian respondents claimed they read privacy policies every time.[152]

144. One of the most common reason for not reading a policy was the length of time necessary to do so. For example:

- The European Commission found that of those who do not always read privacy policies, 75% stated that the length of the policy was the main reason they did not read a privacy policy.
- Ipsos MORI found that participants felt like online policies were lengthy and difficult to understand.
- Which? found that respondents believed the 'cost' of reading and trying to understand terms and conditions was too high.

145. Additionally, many consumers feel they have no "real" alternatives to major platforms and thus have no choice but to accept terms and conditions of platforms such as Google or Facebook. Doteveryone found that just under half (47%) of respondents felt that they had no choice but to sign up to services despite concerns.[153]

To what extent do consumers understand these policies?

Academic Research

146. There is evidence that consumers do not understand online policies when they do read them. In an experimental setting Whitley & Pujadas (2018) found that 77% of participants said that they did not feel informed when reading terms and conditions. Furthermore, when asked specific questions about the terms and conditions, only a small number of participants were able to answer correctly even after reviewing the policy.

147. The same experiment also found that assessing the quality and usefulness of privacy policies is complicated because of individuals' tendency to present themselves in socially acceptable ways (ie to give what they think would be considered to be the 'right' answer in a particular context). As result, some

[151] Deloitte (2017). 2017 Global mobile consumer survey: US edition
[152] Roy Morgan – prepared for Australian Competition and Consumer Commission (2018). Consumer views and Behaviours on Digital Platforms.
[153] Miller, C., Kitcher, H., Perera, K. & Abiola, A., (2020) for Doteveryone. People, Power and Technology: The 2020 Digital Attitudes Report

consumers may claim to be well informed or that they have read the privacy policy when in reality they may not have read or understood that policy at all.

148. Academic research has found that online policies can be very complex and difficult to understand. For example:

- Cardogan (2004) found that a high level of reading competence was required to engage with privacy policies. Other studies also suggest that even if read, privacy policies can only be understood by those with college–level reading skills (Schaub et al. 2017).

- Hoofnagle and King (2007) found that even some law students had problems understanding privacy policies.

- In the experiment by Whitley & Pujadas (2018), participants explained that a combination of ‘legal jargon’ and ‘blanket statements’ lay behind the difficult in understanding the terms and conditions.

149. Some studies have found that consumers do not understand the concept of a privacy policy in the first place. For instance, Turow et al (2005) found that 59% of Internet users in the US were under the impression that the existence of a privacy policy meant that the website would not share personal data with 3rd parties. One consequence of this was that in the presence of privacy policy, consumers were willing to disclose more personal information. Xu et al. (2012) have also suggested that providing consumers control through disclosure settings can reduce privacy concerns, even when that control is illusory.

150. Other studies also suggest that users believe that a privacy policy means that their privacy is protected as the default (Turow et al, 2007, Martin 2015). That is, a large majority of consumers believe that the term ‘privacy policy’ describes a baseline level of information practices that protected their privacy. When consumers saw the term ‘privacy policy,’ they believed that their personal information would be protected and, in particular, they assumed the website would not share their personal information. This suggests that the term privacy policy itself has the capacity to be misleading in that consumers infer that there is a policy in place to protect their privacy.

151. This finding is echoed in research carried out by Hoofnagle and King (2008) which found that the presence of privacy policies on websites led users to think that the websites protected their information. They argued that this result meant that website operators had little incentive to correct this misunderstanding and limited the ability of the market to produce outcomes consistent with consumers' expectations.

Consumer research

152. There is some evidence that approximately half of consumers struggle to understand online policies:

- In 2019, Harris Interactive research for the ICO found that only 59% of respondents felt like they understood the explanation on how adverts were personalised.[154]
- In 2018 Doteveryone found that 45% of consumers agreed that they often sign up to services online without understanding the terms and conditions.[155]

153. Ipsos MORI found that even those with advanced technical abilities sometimes struggle reading terms and conditions they find online.[156]

154. International surveys have found that some respondents believe that a privacy policy indicates an organisation will not share their data with third parties. For example, the ACCC found that 43% of respondents believed this to be true.[157] There is some evidence this may also be true for consumers in the UK. The European Commission found 12% of UK consumers who did not always read a privacy policy said this was because it was enough to see that the organisation had a privacy policy.[158]

155. There is also a common perception among respondents in qualitative interviews that organisation's purposefully make their privacy policies overly long and complex to disadvantage the consumer.[159,160] Which? found that this feeling was strongly related to a consumer's first experience of signing up and their exposure to terms and conditions.

[154] Harris Interactive (2019) for the ICO. Adtech – Market research report
[155] Miller, C., Kitcher, H., Perera, K. & Abiola, A., (2020) for Doteveryone. People, Power and Technology: The 2020 Digital Attitudes Report.
[156] Ipsos MORI (2016a). Digital footprints: Consumer concerns about privacy and security.
[157] Roy Morgan – prepared for Australian Competition and Consumer Commission (2018). Consumer views and Behaviours on Digital Platforms.
[158] European Commission (2019). Special Eurobarometer 487a: The General Data Protection Regulation.
[159] Ipsos MORI (2016a). Digital footprints: Consumer concerns about privacy and security.
[160] Which? (2018). Control, Alt or Delete? Consumer research on attitudes to data collection and use.

TOPIC 2

Do consumers feel in control of their data and to what extent do they engage with controls over their data?

156. We note that there can be a difference between consumers 'feeling' in control of their data and actually being in control. We note that in most of the consumer survey evidence we have reviewed, questions to consumers are phrased in terms of whether or not they 'feel' in control.

To what extent do consumers feel in control of their data?

Academic Research

157. The academic research in this area has explored two issues in relation to consumers' control over their data:

- What interpretation consumers draw from the presence of a privacy policy; and,
- The usability of tools which allow for greater control over how personal data is used online.

158. As indicated above, research suggests that the fact that a website offers a privacy policy can be taken by a significant number of users to indicate that the website will protect the user's privacy and will not share the users' data with third parties (Turow et al (2005)). In addition, other research indicates that the provision of more perceived control over personal data can have the paradoxical effect of leading users to take more risks with their personal data eg increasing their willingness to share sensitive data with other parties (Brandimarte et al (2012)).

159. In terms of usability, a study by Leon et al (2012) used a laboratory-based experiment to assess how well participants were able to use a number of different tools which were intended to give the user more control over their exposure to online behavioural advertising. The tools investigated covered a range of different approaches including:

- blocking access to advertising websites;
- setting cookies to indicate a user's preference to opt out of online behavioural advertising; and
- tools that were built directly into web browsers.

160. The study found serious usability flaws in all the nine tools that were examined. For instance, users found online opt-out tools to be challenging to understand and configure while they struggled to install and configure blocking lists to make effective use of blocking tools.

Consumer research

161. It is clear that very few consumers feel like they have complete control:

- In 2020 the CDEI found that only 36% of respondents believed that they have meaningful control over online targeting systems.[161]
- In 2019 the European Commission found that only 14% of UK respondents felt that they had complete control over their online data compared to 84% who felt they had little or no control over their data. [162]
- In 2017 the DMA found that 86% of respondents wanted more control of the personal information they give to companies and the way in which it is stored.[163]
- In 2016 Ipsos MORI found that only 6% of consumers felt like they had a great deal of control over their online data compared to 69% who felt they had little or no control over their data.[164]

162. It is the case that consumers believe they can manage certain aspects of data processing:

- In 2018 Ofcom found that 74% of respondents felt confident in knowing how to manage who has access to their personal data online.[165]
- In 2018 Which? found that before being informed about data collection methods and uses, 67% of respondents felt confident in knowing how to control what data they share.[166]

163. However, we note that these same consumers still feel that their scope to meaningfully control how their data is used and shared is very limited. For example, Ipsos MORI found that some respondents felt like they only had control over choosing whether or not to enter a website. Once their data had

---

[161] The Centre for Data Ethics and Innovation (2020). Review of online targeting: Final report and recommendations
[162] European Commission (2019). Special Eurobarometer 487a: The General Data Protection Regulation.
[163] Data and Marketing Association and Acxiom (2018). Data privacy: What the consumer really thinks
[164] Ipsos MORI (2016a). Digital footprints: Consumer concerns about privacy and security.
[165] Ofcom (2019). Adults Media Use and Attitudes report - data tables. Table 39
[166] Which? (2018). Control, Alt or Delete? Consumer research on attitudes to data collection and use.

been handed over, these same respondents felt they had lost control over who had access to their data.[167]

164. There is some evidence that as consumers learn more about data processing, they begin to feel less in control and less confident in their ability to manage some aspects of data processing: Which? found that as participants learned about how data is collected, shared and combined, they began to feel less in control of their data overall.[168] They also felt less confident in knowing how to manage who has access to their personal data.

- When Harris Interactive research for the ICO described the automated processes by which digital advertising is bought and sold to participants, the proportion who did not feel in control of the ads they saw rose from 42% to 59%.[169]

165. This loss of control is likely to reduce the levels of user engagement. Consumers report that it is hard to effectively engage with companies who collect and use their data because they feel:[170,171,172]

- disempowered by their lack of knowledge and transparency about how companies collect, use and share their data;
- it is hard to access and change the personal information held by businesses;
- reliant on data-driven services which they do not believe they can give up; and
- there is a perceived lack of alternatives if they want to stop using specific companies whose data collection they are concerned by.

166. Which? has argued that due to this, consumers have become rationally disengaged as the cost of trying to engage with data processing is significantly higher than any benefits a consumer would receive from engaging.[173]

---

[167] Ipsos MORI (2016a). Digital footprints: Consumer concerns about privacy and security.
[168] Which? (2018). Control, Alt or Delete? Consumer research on attitudes to data collection and use.
[169] Harris Interactive (2019) for the ICO. Adtech – Market research report
[170] Which? (2018). Control, Alt or Delete? Consumer research on attitudes to data collection and use.
[171] Information Commissioner's Office (2019). Information rights strategic plan: Trust and confidence
[172] Miller, C., Coldicutt, R., & Kitcher, H. (2018) for Doteveryone. People, Power and Technology: The 2018 Digital Understanding Report.
[173] Which? (2018). Control, Alt or Delete? Consumer research on attitudes to data collection and use.

167. Nevertheless, there is evidence that younger consumers are more likely to report feeling in control of their data than elderly consumers. For example, in Ofcom's survey 48% of those aged 16-24 felt very confident in managing their data as opposed to 24% of those over 55 years old.[174]

168. It appears that feelings of control are related to:[175,176,177]

- *Frequency of internet use:* Consumers who spend more time online or are frequent users of social media platforms are more likely to report feeling in control.
- *Knowledge:* Consumers who feel knowledgeable about data processing are more likely to report feeling in control.
- *Use of settings:* Consumers who pro-actively use privacy and data settings are more likely to report feeling in control.

169. There is mixed evidence on how consumers' feelings are changing over time:

- The European Commission found that the proportion of consumers who feel they have no control and those who feel they have full control both decreased while the proportion of consumer who feel like they have partial control increased by 10 percentage points between 2015 and 2019.[178,179]
- Ofcom found that the proportion of consumers who felt confident in knowing how to manage access to their personal data slightly increased from 72% to 75% between 2016 to 2018.[180]
- The DMA found that the proportion of consumers who reported feeling like they had little to no control over companies collecting or sharing info both increased by 9 percentage points between 2015 and 2017.[181]

[174] Ofcom (2019). Adults Media Use and Attitudes report - data tables. Table 39
[175] Ofcom (2019). Adults Media Use and Attitudes report - data tables. Table 39
[176] European Commission (2019). Special Eurobarometer 487a: The General Data Protection Regulation.
[177] Which? (2018). Control, Alt or Delete? Consumer research on attitudes to data collection and use.
[178] European Commission (2019). Special Eurobarometer 487a: The General Data Protection Regulation.
[179] European Commission (2016a). Flash Eurobarometer 443: e-Privacy
[180] Ofcom (2019). Adults Media Use and Attitudes report - data tables. Table 39
[181] Data and Marketing Association and Acxiom (2018). Data privacy: What the consumer really thinks

To what extent do consumers engage with controls over their data?[182]

Academic Research

170. The research indicates that consumers struggle to engage with controls over their data. Even users with privacy concerns can prove reluctant to take the necessary actions to become informed, even when the information to protect their privacy is made readily available (Acquisti and Grossklags, 2005). This finding has been echoed in more recent work by Athey et al (2017) which found that whenever privacy required additional effort or came at a cost of a less smooth user experience, participants in an experiment were quick to abandon technology that would offer them greater protection.

171. There is evidence that consumers want settings to be privacy enhancing by default. The Stigler Center (2019) conducted a series of experiments and found that consumers will often prefer and expect default provisions that enhance their privacy and security.[183]

172. At the same time, there is evidence that users do not understand how much protection privacy controls actually provide. In research by Habib et al (2017) on consumers use of private browsing, they found that two thirds of participants overestimated the privacy protections offered by privacy browsing.[184] A separate investigation found that the private browsing descriptions offered by major platforms did not help to clear up common misconceptions (Wu et al (2018)).

Consumer research

173. There are discrepancies regarding consumers' confidence in their ability to set and control the privacy features on their browser and social media accounts. For example, Ipsos MORI found:[185]

- 66% of respondents were confident in their skills and ability to set and control privacy features on a web browser on a PC or laptop;
- 62% of respondents were confident in their skills and ability to set and control privacy features on a web browser on a mobile phone;

[182] As indicated earlier, in Chapter 4 we set out data from platforms about the extent of user engagement with privacy controls and settings in practice.
[183] Stigler Center (2019). Stigler Center committee on digital platforms – Market structure and antitrust subcommittee.
[184] Private browsing is a feature offered by most major web browsers, in which browsers clear data associated with the user's activities once they close the private browsing window.
[185] Ipsos MORI (2016a). Digital footprints: Consumer concerns about privacy and security.

- 67% of respondents were confident in their skills and ability to delete web browser cookies.

174. The European Commission also found that that 85% of UK respondents reported that it was easy to change the privacy settings on their personal profiles.[186]

175. However, the CDEI found that when asked to change their settings on major online platforms, most focus group participants found the settings difficult to find and use.[187] These participants reported that user controls are complicated in their layout, overly burdensome to navigate and positive in their language in favour of online targeting. Doteveryone similarly asked participants to change the settings on their device. Within their group, many participants reported confusion over the design and architecture of products and services which in turn made changing their settings time-consuming.[188]

176. This year Doteveryone also found that although 89% of respondents thought it was very important to find out information regarding whether they can control how much data they choose to share with the company, only 25% of these respondents were able to find this information. [189]

177. Other studies have also found that only a few consumers appear to use or understand specific privacy tools available to them. For example, Ofcom found that 35% of respondents have deleted cookies from a web browser and 12% have used a virtual private network to hide their location online.[190] DuckDuckGo has also found that roughly half of American respondents overestimated the privacy benefits that private browsing offers.[191]

178. Based on the current survey evidence it is unclear how often UK consumers change the privacy settings on their browser or social media account. Most consumers report having changed a privacy setting at least once, however:

---

[186] European Commission (2019). Special Eurobarometer 487a: The General Data Protection Regulation.
[187] The Centre for Data Ethics and Innovation (2020). Review of online targeting: Final report and recommendations
[188] Miller, C. (2019) for Doteveryone. Engaging the public with responsible technology.
[189] Miller, C., Kitcher, H., Perera, K. & Abiola, A., (2020) for Doteveryone People, Power and Technology: The 2020 Digital Attitudes Report.
[190] Ofcom (2019). Adults Media Use and Attitudes report - data tables. Table 74
[191] DuckDuckGo (2017). A study on privacy browsing: Consumer usage, knowledge, and thoughts.

- In 2020 Doteveryone found that while 73% of respondents have checked their privacy settings on online accounts to restrict what information they share online, only 31% of respondents do this most or all of the time.[192]

- Doteveryone also found that 47% of respondents have used incognito or private browsing to stop organisations collection information about what they did online but only 13% do this most or all of the time.

- In 2019 the European Commission found that 74% of UK respondents reported that they had tried at least once to change the privacy settings from the default on a social network.[193]

- In 2016 the European Commission found that 64% of UK respondents reported that they had changed the privacy settings on their web browser at least once.[194]

- In 2016 Ipsos MORI found that 56% of participants reported often changing the privacy settings on social networking sites.[195]

179. Regardless, there were three common reasons for not changing privacy settings:

- *The respondent trusted the website to set the appropriate settings:* In 2019 the European Commission found that 37% of UK respondents who had not changed their settings felt this, up 23% from 2015.[196]

- *The respondent did not know how to change their settings:* In 2019 the European Commission found that 26% of UK respondents who had not changed their settings responded because they did not know how to. However, focus groups by Which? found that participants felt it was easy to change settings when they were shown how to do so.[197]

- *The respondent felt like there was no guarantee that the website wouldn't find a way to collect their data anyway:* This was reflected in qualitative surveys for the ESRC, Ipsos MORI and Which?[198,199]

---

[192] Miller, C., Kitcher, H., Perera, K. & Abiola, A., (2020) for Doteveryone. People, Power and Technology: The 2020 Digital Attitudes Report.
[193] European Commission (2019). Special Eurobarometer 487a: The General Data Protection Regulation.
[194] European Commission (2016b). Flash Eurobarometer 443: e-Privacy
[195] Ipsos MORI (2016a). Digital footprints: Consumer concerns about privacy and security.
[196] European Commission (2019). Special Eurobarometer 487a: The General Data Protection Regulation.
[197] Which? (2018). Control, Alt or Delete? Consumer research on attitudes to data collection and use.
[198] Ipsos MORI (2016a). Digital footprints: Consumer concerns about privacy and security.
[199] Hopkins Van Mil (2015). Big Data: Public views on the use of private sector data for social research.

180. Looking beyond platform or browser specific controls, most consumers report that they do not find it easy to access or change the personal information held by businesses about them or to find out how businesses collect, share and use their data. Table L.1 below sets out the ICO's findings from their 2019 survey.

Table L.1 Respondents' agreement or disagreement to statements about control over data

Q5. Do you agree or disagree with the following statements about the use of personal information in the UK?

	2018			2019		
	NET Agree	NET Disagree	Don't know	NET Agree	NET Disagree	Don't know
It is easy to access and change my personal information held by businesses/organisations	29%	59%	12%	31%	56%	13%
Current laws and regulations provide sufficient protection of personal information	33%	57%	10%	33%	58%	9%
Businesses/ organisations are open and transparent about how they collect and use personal information	26%	66%	8%	26%	65%	9%
It is easy to find out how my personal information is stored and used by businesses/ organisations	23%	64%	13%	23%	64%	13%
It is easy to find out whether my personal information is being made available to third parties	23%	63%	14%	23%	63%	14%

Base: All Adults: 2018 (2131) / 2019 (2259)

Information Commissioner's Office (2019). Information Rights Strategic Plan: Trust and Confidence.

181. In addition to this:

- This year the CDEI found that only 33% of respondents believed that companies will do what users request through their settings and preferences.[200]
- In 2018 the DMA found that 64% of respondents felt like they had little to no control over compelling a company to delete any information about them.[201]

[200] The Centre for Data Ethics and Innovation (2020). Review of online targeting: Final report and recommendations
[201] Data and Marketing Association and Acxiom (2018). Data privacy: What the consumer really thinks

- The DMA also found that 62% felt like they had little to no control over ensuring brands use their data for the purpose the consumer initially agreed to.

182. There is evidence that consumers agree that default settings should stop their information from being shared:

- In 2016 the European Commission found that 91% of UK respondents agreed that the default setting should be one which prevents their information from being shared.[202]

- In 2016 Ipsos MORI found that when discussing health data, participants imagined that the default option should mean that individual-level data is not shared.[203]

- In 2016 Citizens Advice found that respondents wanted information they felt was sensitive to not be collected by default.[204]

183. There is less agreement on how often online platforms should ask for permission to process consumer's data. The European Commission asked UK respondents when they think a website should ask for permission to access information or store tools to monitor online activities on devices and found that:[205]

- 54% felt that it should be the first time a user enters the website, with the option to change one's mind later;

- 39% felt they it should be asked each time the user enters the website; and

- 5% spontaneously answered 'never', as they did not want to share personal information.

184. There is evidence that younger consumers, those who use the internet frequently and those who describe themselves as confident internet users are more likely to change their settings or take actions to protect their privacy. For example:

---

[202] European Commission (2016b). Flash Eurobarometer 443: e-Privacy
[304] Ipsos MORI (2016c). The one-way mirror: Public attitudes to commercial access to health data.
[204] Illuminas for Citizens Advice (2016). Consumer expectations for personal data management in the digital world.
[205] European Commission (2016b). Flash Eurobarometer 443: e-Privacy

- Ipsos MORI found that older respondents were less likely to change their cookie settings than younger groups.[206]

- The European Commission found that 70% of 15-24-year olds had changed their privacy settings as opposed to 44% of those over 55 years old.[207]

- The European Commission also found that those who report using the internet more frequently are more likely to have changed the privacy settings on their browsers at least once.

- Which? found that those who go online for more than five hours a day are 1.7 times more likely overall to take actions to protect their privacy.[208]

- Which? also found that respondents who described themselves as confident in knowing what data they share were 1.6 times more likely overall to take actions to protect their privacy.

Are consumers aware of their rights under the GDPR? How often do they exercise these rights?

Consumer Research

185. The majority of consumers have heard about GDPR and roughly half have some understanding of what it entails. The ICO's 2018 annual tracker survey found that 84% of respondents had heard about GDPR but only 55% knew what it was.[209] In 2019 the European Commission found that 71% of UK respondents had heard about GDPR and 47% knew what it was.[210]

186. In line with this, most consumers have heard about some of the rights guaranteed by GDPR but only a few have exercised them. For example, the European Commission found: [211]

    - the most well-known right was the right to access your data with 64% of UK respondents reporting an awareness of this right;

    - the most exercised right was the right to object to receiving direct marketing with 33% of UK respondents having exercised this right; and

[206] Ipsos MORI (2016a). Digital footprints: Consumer concerns about privacy and security.
[207] European Commission (2016b). Flash Eurobarometer 443: e-Privacy
[208] Which? (2018). Control, Alt or Delete? Consumer research on attitudes to data collection and use.
[209] Information Commissioner's Office (2018). Information Rights Strategic Plan: Trust and Confidence.
[210] European Commission (2019). Special Eurobarometer 487a: The General Data Protection Regulation.
[211] European Commission (2019). Special Eurobarometer 487a: The General Data Protection Regulation.

- the least well-known and exercised right was the right to have a say when decisions are automated with 38% of UK respondents having heard about it and only 15% having exercised this right.

187. There was a consensus among some consumers that the rights guaranteed by GDPR were important. Another study found that 62% of respondents felt more confident in sharing their data when hearing about the rights guaranteed by GDPR.[212]

What influence do behavioural biases and choice architecture have on decisions that consumers make regarding privacy choices?

188. The literature recognises that consumers do not necessarily adopt a rational, utility-maximising approach to decision about privacy in an online environment. Other approaches which explicitly take into account factors such as incomplete and asymmetric information as well as biases due to cognitive limitations and contextual factors can also contribute to the analysis of the economics of privacy decisions and better reflect what is observed in the real world.

189. Cognitive patterns of information processing are sophisticated patterns that are functional and effective in filtering and processing information. However, it is possible that errors and biases occur in processing the information and in drawing conclusions on the processed information. Biases are not exceptional but rather they reflect the general ways in which people process information and therefore need to be taken into account when analysing how consumers actually behave.

Biases due to cognitive limitations

190. People's cognitive abilities to process information are limited and insufficient to process all information available at a given point of time. As an evolutionary adaptation, the human brain has developed heuristics which are mental shortcuts that assist with filtering information and reaching decisions in a timely manner based on incomplete information eg that a more expensive product will be higher quality. However, sometimes these shortcuts can lead to erroneous conclusions which makes them a major source of cognitive biases.

[212] Data and Marketing Association and Acxiom (2018). GDPR: A consumer perspective.

Context dependent biases

191. Although biases can lead people to reach irrational conclusions in the sense that the conclusions are unrealistic or do not reflect the facts, some biases exist because they lead to beneficial outcomes in specific contexts. For example, a variety of 'self-serving biases' causes people to interpret information regarding their own abilities overly optimistically with the highly functional result that they are encouraged to act more assertive, starting a self-fulfilling prophecy. Another example is people's biases due to myopia; people's general tendency to more heavily focus on direct outcomes and neglect future consequences. This tendency is functional in that the future is more uncertain and engaging in future outcomes might be a sunk cost. However, in the light of many decision-making contexts this tendency can lead to less-then optimal decisions.

What behavioural biases can influence users' privacy decisions?

Academic Research

192. The academic literature discusses a number of different behavioural biases that could be present in different contexts. We focus on a specific set of biases which appear to be the most relevant to privacy decisions and the most well researched. These biases and their potential impact on a consumer's decision-making in an online context are set out below.

193. **Status Quo bias:** consumers have a preference for things staying as they are or that the current state of affairs remains the same and any change from the status quo is perceived as a loss. This leads them to have an affinity for default settings. For example, being presented with an 'I Agree' button as the default choice in relation to Terms of Use / cookie policies when registering with a service/visiting a website. Firms may exploit the default effect in choice architecture to have 'privacy intrusive' settings as the default or make it difficult for users to make decisions in line with their stated preferences.

194. Goldstein et al (2008) argue that choice architects can exert influence over the choices consumers make through the use of default-settings. They argue that defaults can be perceived as the manufacturer's recommendations, and in many cases, users would be happy to accept those recommendations. They argue that many companies will try to set defaults in ways that align with customers' preferences. For example, the paper refers to companies such as Audi and Daimler pre-selecting the most popular colour as the default in on-line car configurators. The authors did, however, recognise that defaults could have a malign effect as well, referring to court cases in both the US and in

Europe about default settings leading to violations of privacy. The authors make a distinction between ‘mass defaults’, in which everyone gets the same default, and ‘personalized defaults’ which are tuned to the consumer’s needs. They argue that personalized defaults require some information about the consumer, and they should therefore be created in a way that respects the consumer’s privacy.

195. In a basic online setting, Lai and Hui (2006) considered the impact of the difference between ‘opt-in’ and ‘opt-out’ settings to receive newsletters from websites, as well as the role played by default settings. They found that participants were more likely to choose the default option. They did note a mitigating effect in that users who already had ‘high’ privacy concerns were less likely to be swayed by the default setting.

196. Users may assume that default settings are configured to protect them and so do not review the actual settings. Leon et al (2012) used a lab experiment to study how well users were able to make use of tools to control data sharing. As part of that study they found that a number of participants assumed that the default configurations of those tools were designed to protect them without reviewing the settings.

197. A number of studies have focused specifically on Facebook and its approach to default settings. For instance, Acquisti and Gross (2006) reviewed the privacy settings for Facebook and found that – at the time of their study - although the default settings allowed profile information to be publicly searchable, the majority of users that were surveyed had not changed these settings.

198. Stutzman et al (2012) used profile data from a longitudinal panel of 5,076 Facebook users to understand how their privacy and disclosure behaviour had changed between 2005-2011. Their research indicated the users in their panel exhibited increasingly privacy-seeking behaviour over time eg progressively reducing the amount of personal data shared publicly with unconnected profiles on the same university Facebook network.[213] However, they also found that changes implemented by Facebook between 2009-2010 stopped or in some cases reversed that trend. In addition, they noted that the amount and scope of personal information that users shared with people they did know actually increased. They considered that this was consistent with

[213] The authors of the study recognised that a limitation of their study was that it could not create a random sample of current Facebook users. As a result, they suggested that extrapolations to the general Facebook population should be considered ‘with caution’.

other experimental evidence that access to increasingly granular settings could increase feelings of control and promote sharing of information.

199. **Framing or Presentation effects:** The way in which control over the disclosure of personal information is presented to users can affect their decisions about disclosure, even when there is no difference in the privacy risk.

200. The way in which privacy controls are framed can mean that users may actually disclose more personal information. In the context of a social media platform, Brandimarte et al (2012) found that participants who were offered stronger privacy controls would then disclose more personal information compared to those who were offered weaker controls. When users perceived that they had more control over their data, they underestimated the sources of risk that they did not have control over.

201. The framing of privacy notices as more or less protective compared to a reference point (eg a competitor's privacy policy) has also been found to have an impact on the disclosure of personal information. Using an experimental approach, Adjerid et al (2013) found that the impact of privacy notices was sensitive to how they were framed: notices framed as increasing protection resulted in increased disclosure and notices framed as decreasing protection resulted in decreased disclosure. They also found that privacy notices could be used to nudge individuals to disclose different amounts of personal information. They argued that their findings casted doubt on the likelihood that initiatives based on privacy notices and transparency on their own could address online privacy concerns.

202. Acquisti et al (2015) explored the issue of how the framing and presentation of decisions could be used to 'nudge' users to promote the disclosure of personal information. They argued that many of the existing choices around privacy were designed to discourage users from opting to protect their privacy. For instance, they noted that in promotional emails, the option to unsubscribe was placed at the bottom of the email, in small text and bland colours. They also examined the example of a sign-up process to a service in 2010. The user was asked if they would like to 'keep their profile page public,' or 'make it private' with the text implying that keeping the profile public was the default option.

203. **Anchoring effects:** When making a decision, users often make use of information that may or may not be directly relevant as a reference point.

204. Users may be significantly affected by what other users are posting on a social media platform regardless of how comfortable they might be about

revealing personal information or the consequences of revealing personal information. Acquisti et al (2012) found that the extent of the disclosure of personal information was influenced by order effects. That is, participants tended to disclose more sensitive information when the survey started with privacy-intrusive questions.

205. Aesthetic appeal can also influence perceptions of quality: in an on-line environment, users may make rapid assessments of quality / trustworthiness based on superficial design features.

206. **Loss aversion (or endowment effects)**: refers to the tendency for individuals to prefer avoiding losses compared to making equivalent gains. That is, the psychological impact of giving up something which an individual already possesses is more powerful than the benefit that is derived from the acquisition of the same item.

207. An example of this phenomenon can be seen in terms of comparisons between the amount that consumers are prepared to accept to disclose their personal data and the amount they are prepared to pay to regain control of their personal data. That is, where consumers feel in control of their personal data, they value it more and where they feel they have lost control of it, they value it less.

208. In behavioural experiments, Grossklags and Acquisti (2007) showed that people needed to be paid more in exchange for disclosing personal information than they are willing to pay to regain control over the same information. The authors observed that their results showed the benefits of separating decision making around privacy issues into decisions to protect and decisions to reveal data. They argued that the literature on the economics of privacy and security implicitly assumes that the behaviour of individuals should be identical in relation to those choices but related literature in the field of psychology and results of their experiments suggested that this was not the case.

209. More recently Winegar and Sunstein (2019) found that in a survey of 2,416 Americans, the median a consumer was willing to pay was $5 per month to maintain their data privacy (along specified dimensions). In contrast, they would require $80 per month to allow others access to their personal data. The authors termed this a ‘super endowment effect’ in that it was significantly higher than the 1:2 ratio that was often found between measures of willingness to pay versus willingness to accept. They argued that a lack of information and behavioural biases meant that both measures would be unreliable guides to the welfare effects of retaining or giving up data privacy without being able to address the lack of information and behavioural biases.

210. **Myopia / hyperbolic discounting**: Users do report that they are concerned about privacy, but they then heavily discount the risks associated with disclosing personal information. Acquisti (2004) argued that an accurate evaluation of potential privacy threats requires processing quite a lot of information and this is information that users either typically do not have or information that is likely to prove superfluous anyway, as the probability of a future privacy violation is difficult for most users to assess. It is also suggested that individuals tend to heavily discount the low probability of high future risk (eg identity theft) and that a lack of privacy protection knowledge can lead to the misinterpretation of the likelihood of actual privacy violations (Acquisti and Grossklags, 2005)[214].

211. '**Hot' decision-making**: this is where an individual's decision-making can be influenced by their emotional state. For instance, privacy decision making may involve disclosures which bring individuals some immediate gratification, such as social interaction or access to desired services, while at the same time subjecting them to privacy costs that may only be incurred months or years later. If individuals are excited about the prospect of accessing a new service or product, they can respond emotionally to decisions about privacy settings rather than rationally. Firms may exploit these first order (ie impulsive) preferences.

212. Acquisti et al (2017) also noted two other behavioural biases which they considered to be relevant to decision-making in an online environment.

213. **Inattention:** The tendency of individuals to restrict their attention to a subset of the options (or information) available to them.

214. They argue that web interfaces encourage users to 'click away' dialogue boxes or agreements that stand in the way of completing the primary action. The information in the dialogue boxes may be perceived to be of low importance because it is possible to continue by simply clicking away. They also argue that users have a tendency to select the top search results / options they are presented with.

215. **Optimism / Overconfidence**: Users have a tendency to underestimate the probability of being subject to a negative event. Users may also over-estimate their decision-making skills resulting in excessive confidence. In this case, users may be overconfident in their assessment of the privacy risks or about their ability to take steps to address. For example, contrary to consumers'

---

[214] For instance, of the respondents who suggested that individual's privacy should be protected with the help of technology, 63 percent never used encryption, 44 percent did not use email filtering technologies, and 50 percent did not use shredders for documents to avoid leaking sensitive information.

perception that they can ignore a behaviourally targeted ad, Matz et al (2017) shows that ads targeted on psychological traits inferred from Facebook data resulted in the consumers being 40% more likely to click on the ad and 50% more likely to make a purchase.

216. It is notable that the academic literature does not discuss how these different biases might interact or which might have the most significant impact in any given situation. It is also possible that other behavioural biases will be relevant in specific contexts but there is less evidence or research on their effects.

Is choice architecture used to push consumers into making certain choices?

217. From a behavioural insights' perspective, it is important to distinguish the underlying biases on the one hand and the choice architecture mechanism on the other. For example, status quo bias may be the underlying bias whereas the default setting default is the choice architecture design. Whereas cognitive limitations and biases will always exist, firms do have control over whether they design their choice architecture to exploit these biases.

Academic Research

218. Following Thaler and Sunstein (2008) we use the term 'choice architecture' to refer to the process and outcome of design decisions about user interfaces in an online environment. Any choice architecture – whether deliberate or not – will impact on how users interact with a system.

219. As set out above, the way a choice is presented to a user will influence the user's decision and there can be a number of different ways of presenting that choice. Johnson et al (2012) divide the tools available for choice architects into two categories: how the choice is structured; and, how the choice is described. They argue that there is no such thing as neutral architecture: any way a choice is presented will influence how a consumer makes a choice.

220. In terms of the structure of the decision, they point to a range of factors such as:

- the number of options;
- the use of defaults;
- the use of technology;
- the use of decision aids (eg recommendations); and
- short and long-term considerations.

221. In terms of describing the decision, they point to the way in which options/attributes can be grouped together or separated out, and the way in which different attributes are presented.

222. They also argue that individual differences can influence how choice architectures play out in the market. To be effective, choice architects need to know about the decision environment and also about the characteristics of the decision-makers they are targeting: how they will process and draw meaning from information, what their goals are etc.

223. A number of studies have examined specific aspects of the choice architectures being presented to users in an online space. As indicated above, Acquisti et al (2015) have argued that the most obvious, brightest, or easiest option can discourage users from selecting privacy friendly options. In the example of the sign-up process, the authors argued that as well the text implying that keeping the profile public was the default option, the ‘keep public’ button itself was also in a brighter colour, making it more attractive, and on the right side of the dialog box, a position that was typically used for buttons that moved the consumer on to the next stage.

224. These effects can be just as prevalent with mobile apps as well. Egelman et al (2013) explored how choice architecture could affect smartphone users’ stated willingness to install applications that request varying permissions. They found that people were willing to pay more for Android apps that requested fewer permissions when they had several options for price and permissions. However, when only given one choice, participants were not as willing to pay for privacy. They suggested that applications that only gave users the option of installation with a fixed set of permissions could be nudging users away from selecting privacy-friendly options.

225. More recently, research has focused on the way in which firms harness behavioural biases in the design of user interfaces to steer or mislead users into making unintended and potentially harmful decisions. These are sometimes referred to as ‘dark patterns’ or ‘sludge’ techniques. The term ‘sludge’ is used to describe deliberate frictions used by firms to exploit cognitive biases and psychological weaknesses in order to make it harder for consumers to make good choices (Behavioural Insights Team, 2019).

226. Mathur el (2019) analysed approximately 53,000 product pages from around 11,000 shopping websites and identified 1,818 instances of the use of dark patterns. They categorised these practices into 15 different types of dark patterns.

227. Other studies have focused in detail on the role that choice architecture – in particular the use of default settings – can have on users' choices about privacy settings. For instance, in two reports which look at the interfaces used by Facebook and Google,[215] the Norwegian Consumer Council ('NCC') pointed to the use of 'privacy-intrusive' default settings ie disclosing data as the default. This meant that users who wanted to choose privacy friendly options then had to go through a number of different steps to access those options.

228. The NCC argued that these firms make use of a variety of different techniques in the design of interfaces which it considered to be unethical. It argued that the way in which information was presented to users could be misleading or unbalanced;[216] and the set-up process was subverted by changing the function of a key button mid-way through the process.[217]

229. The Behavioural Insights Team (2019) has also argued that consumers' behaviour in an environment is shaped by the design and characteristics of websites, platforms and apps that they interact with in the same way that they are in an offline environment. In fact, they suggest that behavioural biases could be amplified in an online setting because users are often required to make decisions quickly at the same time as processing significant amounts of information. They also suggest that the presence of large amounts of personal information combined with improved analytical and computer processing power, gives firms more opportunities to exploit users' cognitive biases and psychological weaknesses. They point to firms adding deliberate frictions to decision-making processes and harnessing information deficits.

230. We note that a number of studies have pointed that users may in fact be constrained about the choices that they can make. In the context of making privacy decisions about mobile apps, Zafeiropoulou et al (2013) argue that users are in fact constrained by the choice architecture. Users are expected to accept certain requirements if they want to install and use a certain app and this means that sharing personal information becomes perceived as normal in social life.

231. Following on from the idea of a lack of choice, Shklovski et al (2014) argue that the repeated invasion of privacy boundaries can lead to a state of

---

[215] Norwegian Consumer Council (2018). Deceived by Design; and Every Step You Take
[216] In the case of Google's Location History, the NCC argues that the visible information is only contains positive examples.
[217] The NCC point out that at the start of the set-up process, Google uses a Blue button in the bottom right hand corner of the screen which is marked 'Next'. However, later on in the process the same coloured button in the same position on the screen changes to 'Accept' and unless the user is attentive, they could miss this change in function.

resignation on the part of the user. That is, users do accept privacy policies despite privacy concerns because of the 'all-or-nothing' nature of the consent process. As a result, users become resigned to the idea that they possess little power to change this situation.

232. Quinn (2016) also develops the idea that habit can inhibit user engagement with privacy management tools on social networks, despite the increased experience with social networking. This eventually leads to a disconnection between privacy concerns and behaviours.

233. It is clear that choice architecture can have a significant impact on users' decision-making and number of studies point to the negative consequences of existing choice architecture structures. However, other studies have suggested that the choice architecture could be adapted to work in the favour of consumers. The use of choice architecture to improve consumer decision-making is discussed in more detail in the section dealing with the implications for remedies.

TOPIC 3

What are consumers' attitudes towards data processing and personalised advertising?

234. Consumers' knowledge, understanding and attitudes towards data processing are closely linked but separate concepts. In this section, we make the distinction that consumer attitudes can involve a strong emotional component. Furthermore, those attitudes will often, but not always, be influenced by the consumer's knowledge and understanding of the data processing involved. As such, in describing consumers' attitudes towards data sharing, this section will necessarily involve some discussion of consumers' knowledge of data processing as well.

To what extent do consumers value their data or privacy?

Academic Research

235. Academic research clearly indicates that privacy is important to consumers, but it is hard to determine exactly how much consumers value their data or their privacy. Some researchers have even suggested that it may not be possible to determine the value which consumers assign to their data or privacy.

236. As indicated above, Winegar and Sunstein (2019) found that consumers were only willing to pay $5 per month to maintain data privacy but demanded $80 per month to provide access to their data. As a result of a lack of information and behavioural biases, they suggested that neither measure would provide a reliable guide for estimating the value of data or privacy.

237. A difficulty faced by consumers is that privacy trade-offs often mix immediate tangible benefits with future intangible harms (Acquisti et al, 2016). Coupled with the lack of a market for personal data, there is no obvious way for consumers to properly value privacy and personal data (Strandburg, 2013). As a result, it is hard for consumers to weight up the costs and benefits of disclosing their data or protecting their privacy.

238. Consumers could also have different attitudes towards privacy according to the type of data involved. For instance, work by Skatova et al (2019) points to data on banking transactions being consistently considered to be the most sensitive with the evidence about the sensitivity of location data, social media and browsing history being more mixed. Their work also indicates that the context in which sharing occurs will influence users' willingness to share their data.

Consumer research

239. It is clear from survey responses that consumers report that they value their privacy deeply:

- In 2019 the ICO found that 80% of respondents thought it was important that their personal information is protected when they share it with businesses, up 5 percentage points from 2018.[218]
- In 2018 the European Commission found that 82% of UK respondents agreed that they avoid disclosing personal information online.[219]
- In 2016 the European Commission found that 96% of UK consumers thought it was important their personal information on their computer, tablet or smartphone could only be accessed with their permission.[220]

[218] Information Commissioner's Office (2019). Information Rights Strategic Plan: Trust and Confidence.
[219] European Commission (2018). Special Eurobarometer 480: Europeans' attitudes towards Internet Security.
[220] European Commission (2016b). Flash Eurobarometer 443: e-Privacy

- In the same survey, the European Commission also found that 79% of UK respondents thought it was at least fairly important that tools for monitoring activities online can only be used with permission.

- In 2016 Citizens Advice found that most focus group participants feel they have a fundamental right to privacy of their data.[221]

How do consumers perceive data processing?

Consumer Research

240. Most consumers now see data processing as a fact of modern life. Both Which? and Doteveryone found that the majority of respondents in their qualitative interviews believed that data processing was a part of everyday life and it was only going to become more prevalent.[222,223] In 2015 the European Commission found that:[224]

    - 83% of UK respondents agreed that providing personal information is an increasing part of modern life;

    - 66% of UK respondents agreed that there is no alternative than to provide personal information if you want to obtain products or services; and

    - 56% of UK respondents agreed that they feel they have to provide personal information online.

241. Despite this, it appears that many consumers do not fully understand the role data processing plays. The ICO found that there was a general feeling amongst consumers that data processing was a necessary evil for using online services.[225] Which? found that only the more informed consumers understood that data processing is the 'price' they pay for accessing free online products or services.[226]

---

[221] Illuminas for Citizens Advice (2016). Consumer expectations for personal data management in the digital world.
[222] Data and Marketing Association and Acxiom (2018). Data privacy: What the consumer really thinks.
[223] Which? (2018). Control, Alt or Delete? Consumer research on attitudes to data collection and use.
[224] European Commission (2015). Special Eurobarometer 431: Data protection
[225] Information Commissioner's Office (2015). Data protection rights: What the public want and what the public want from data protection authorities.
[226] Which? (2018). Control, Alt or Delete? Consumer research on attitudes to data collection and use.

To what extent are consumers comfortable with and accepting of data processing?

Academic Research

242. It is difficult to assess how comfortable consumers are in relation to data processing. As indicated above, research points to the existence of 'privacy paradox' in that consumers report that privacy is very important, but their actions indicate that they are less concerned about privacy in practice. This has implications for the design of policy.

243. Athey et al (2017) found that small incentives, costs or misdirection can lead people to safeguard their data less and argued that this had two interpretations. On the one hand it could lead policy makers to question the value of stated preferences for privacy when determining privacy policy. At the same time, it could point to a need for more extensive privacy protections in that consumers need to be actively protected from a willingness to share data in exchange for relatively small monetary incentives. They argued that the prevalent 'notice and consent' mechanism might not be sufficient to protect consumers.

244. Consumers' attitudes towards data processing may not be straight-forward and Martin and Shilton (2016) have argued that consumers' general privacy preferences are of limited significance in predicting privacy decisions in specific scenarios. They argue, instead, that more attention should be given to particular contextual influences and how the data is used. Emotions such as anxiety can also have a role to play in consumers' privacy decisions: in general, the more anxious a consumer is about disclosing personal data, the more negative their attitude toward disclosing information online. (Robinson, 2018).

Consumer research

245. Consumer research points to consumers not being comfortable with different aspects of data processing.

246. Qualitative surveys have found that data processing is not a top of mind concern for most consumers when using the internet. Instead, both Which? and Doteveryone found that the majority of initial concerns revolved around the use of online platforms rather than data processing.[227,228] Similarly,

---

[227] Which? (2018). Control, Alt or Delete? Consumer research on attitudes to data collection and use.
[228] Miller, C., Coldicutt, R., & Kitcher, H. (2018) for Doteveryone. People, Power and Technology: The 2018 Digital Understanding Report.

Citizens Advice found that most respondents were not spontaneously concerned about data privacy when discussing smart home technology.[229] That is, respondents were not instinctively worried about data manipulation or misuse. It was only after discussions that they wondered how data correlation and aggregation could be used against them.

247. This does not mean that consumers are comfortable with data processing. Instead, there is evidence that the majority of consumers are either uncomfortable with data processing or concerned about their privacy:

- In 2019 Ofcom and the ICO found that 57% of respondents had at least one concern about data or privacy.[230]
- In 2019 Which? found that when segmenting their respondents based on their attitudes towards data collection, 71% of respondents were characterised as being more concerned about data processing and collection.[231]
- In 2017 Demos and Opinium found that 69% of respondents were uncomfortable sharing personal information with social media organisations.[232]
- In 2017 the DMA found that 75% of respondents were concerned about online privacy.[233]
- In 2016 Ipsos MORI found that 67% of all internet users were at least fairly concerned about their privacy online.[234]
- In 2016 the European Commission found that 78% of UK respondents who used the internet and online platforms were concerned about the data collected about them on the internet.[235]

[229] Traverse for Citizens Advice (2018). The future of the smart home: Current consumer attitudes towards smart home technology.
[230] Ofcom and the Information Commissioner's office (2019). Internet users' concerns about and experience of potential harm online – data table.
[231] Which? (2019). Data dozen segmentation update
[232] Bartlett, J. & Gaston, S., (2017). Public views on technology futures.
[233] Data and Marketing Association and Acxiom (2018). Data privacy: What the consumer really thinks
[234] Ipsos MORI (2016). Digital footprints: Consumer concerns about privacy and security.
[235] The European Commission (2016c). Special Eurobarometer 447: Online platforms

- In 2015 the European Commission found that 59% of UK respondents were concerned about their everyday activities being recorded on the internet.[236]

248. The majority of consumers also have at least one concern about data processing:

- In 2020 Doteveryone found that 77% of respondents were concerned about companies selling data about them.[237]
- In 2019 the European Commission found that 73% of UK respondents who did not feel in complete control of their information were concerned about not having full control.[238]
- In 2018, the European Commission found that 47% of UK respondents are concerned about someone misusing their personal data when using the internet for activities such as buying goods and services online.[239]
- In the same survey, the European Commission found that 71% of UK Respondents are concerned that their online personal information is not kept secure by websites.
- In 2018 Which found that 71% of respondents were worried about organisations using information they had gained through observation.[240]
- Which? also found that 81% of respondents were concerned about the sharing of data with third parties.
- In 2015 the European Commission found that 80% of UK respondents were concerned about authorities or privacy companies using information for a different purpose than the one it was collected for, without informing them.[241]

249. Furthermore, there is evidence that as consumers learn more about data processing they become increasingly concerned (although this does not necessarily lead imply that it will lead to a change in behaviour):

---

[236] The European Commission (2015). Special Eurobarometer 431: Data protection
[237] Miller, C., Kitcher, H., Perera, K. & Abiola, A., (2020) for Doteveryone. People, Power and Technology: The 2020 Digital Attitudes Report.
[238] European Commission (2019). Special Eurobarometer 487a: The General Data Protection Regulation.
[239] European Commission (2018). Special Eurobarometer 480: European attitudes towards Internet security
[240] Which? (2019). Data dozen segmentation update.
[241] European Commission (2015). Special Eurobarometer 431: Data protection

- Which? found that concern increased after respondents learnt about the extent to which data is collected, shared and used.[242]

- Citizen's Advice found that after discussing how much data current technology collects, data privacy became a key concern for most respondents.[243] Respondents also began to consider how data correlation and aggregation could be used against them.

- Harris Interactive research for the ICO found that after describing how the real-time ad-tech bidding processing worked, the proportion of respondents who thought it was unacceptable that websites displayed advertising in return for being free rose from 14% to 43%.[244]

- The CDEI found that focus group participant's concerns regarding online targeting increased in seriousness as their understanding and awareness increased.[245]

250. However, Which? also found that as some respondents learnt why some data is collected, they could understand why data collection was necessary or how it benefited them.[246] In turn, this led to more positive attitudes towards data processing amongst some respondents.

251. The degree to which consumers are uncomfortable or concerned with data processing varies widely across the population. In 2016 Ipsos MORI found that 20% of internet users were very concerned about their privacy online, while 47% were fairly concerned, 22% were not very concerned and 10% were not concerned at all.[247] Which? similarly found that consumers' attitudes and concerns towards data processing varied greatly amongst their respondents.

252. Overall, younger consumers and those who describe themselves as confident internet users are more likely to be comfortable with data processing. For example:

    - In 2018 Ofcom found that 28% of respondents aged between 16-24 were not happy for companies to collect and use personal information for any

---

[242] Which? (2019). Data dozen segmentation update.
[243] Traverse for Citizens Advice (2018). The future of the smart home: Current consumer attitudes towards smart home technology.
[244] Harris Interactive (2019) for the ICO. Adtech – Market research report
[245] Centre for Data Ethics and Innovation (2019). Interim report: Review into online targeting.
[246] Which? (2018). Control, Alt or Delete? Consumer research on attitudes to data collection and use.
[247] Ipsos MORI (2016). Digital footprints: Consumer concerns about privacy and security.

reason as opposed to 34% of those between 25-34 and 56% of those between 55-64.[248]

- In 2017 Demos and Opinium found that 21% of respondents aged between 18-34 were comfortable sharing their personal information with social media organisations compared to 5% of those over 55.[249]

- In 2016 Ipsos MORI found that 19% of respondents who described themselves as confident internet users were very concerned about privacy online compared to 31% of respondents with low confidence.[250]

- Ipsos MORI also found that 50% of respondents who described themselves as confident internet users agreed that they would be willing to give their personal information to a brand they trusted compared to 38% of those with low confidence.

253. Finally, there is mixed evidence on whether consumers are becoming more comfortable with data processing:

- Which? found that the proportion of consumers who they characterised as being less concerned about data processing decreased from 48% to 29% between 2018 and 2019.[251]

- Ofcom found that the proportion of respondents who were not happy for companies to collect and use their personal information slightly decreased from 41% to 39% between 2017 and 2018 but then increased again to 45% in 2019.[252]

- The DMA found that proportion of consumers who were largely unconcerned about data collection increased from 16% to 25% between 2015 and 2017.[253] and

What influences consumer acceptance and comfort with data processing?

Consumer Research

[248] Ofcom (2019). Adults Media Use and Attitudes report - data tables. Table 98
[249] Bartlett, J. & Gaston, S., (2017). Public views on technology futures.
[250] Ipsos MORI (2016). Digital footprints: Consumer concerns about privacy and security.
[251] Which? (2019). Data dozen segmentation update.
[252] Ofcom (2020). Online nation 2020 report
[253] Data and Marketing Association and Acxiom (2018). Data privacy: What the consumer really thinks

254. The acceptance of data processing is heavily influenced by the context in which it takes place. What, how and why data is processed are very important to consumers, in addition to who has access to the data.

The type of data being processed

255. Consumers are more willing to share data they do not consider sensitive or unique.[254] For example:

- In 2018 the DMA found that while 30% of respondents were comfortable sharing their interests for marketing purposes only 10% were willing to share their online browsing and history details.[255]
- In 2018 the Open Data Institute ('ODI') similarly found that while 53% of respondents were comfortable sharing their name with an organisation they knew, only 22% were comfortable sharing their medical records.[256]

256. In deliberative discussions with consumers, Citizens Advice found that sensitive information was perceived to include financial details, medical records, house occupancy, location sharing, private conversations and passwords.[257] Data involving behavioural patterns or personal details that can lead to conclusions about personal lives and leave consumers vulnerable also felt too sensitive to share.

257. Which? found that another important consideration for most consumers was whether the data being collected felt relevant to the service or good, such as location data being used in map services.[258]

How the data is processed

258. There is evidence that consumers are more willing to share anonymised and aggregated data:

- The Wellcome Trust found that 77% of respondents agreed that they were willing to share anonymised medical records for research.[259]

---

[254] Sensitive data can include financial details, medical records, location sharing, private conservations, habits and more.
[255] Data and Marketing Association (2018). Data privacy: What the consumer really thinks
[256] Open Data Institute (2018). Attitude towards data sharing – Europe.
[257] Traverse for Citizens Advice (2018). The future of the smart home: Current consumer attitudes towards smart home technology.
[258] Which? (2018). Control, Alt or Delete? Consumer research on attitudes to data collection and use. .
[259] Wellcome Trust (2016). Wellcome trust monitor report.

- The Royal Statistical Society found that the addition of safeguards such as the anonymisation of data, or punishment for data misuse, improved the level of support for sharing data within government departments from 33% to 51%.[260]

- Ipsos MORI found that 61% of respondents do not mind companies using information collected about them as long as it is anonymised and cannot be linked back.[261]

Who processes the data

259. Consumers are more willing to share data with the NHS, public authorities and banks when compared with private businesses, especially social media platforms. For example:

- The DMA found that 41% of respondents were willing to share data with government departments to improve the efficiency of public services but only 29% were happy for businesses to share information to provide a more tailored service.[262]

- The Royal Statistical Society found that while 42% of respondents supported government bodies sharing anonymised data with charities who provide services on behalf of government to help improve services they provide, only 36% of respondents supported companies who provide services on behalf of government doing the same.[263]

- The European Commission asked UK respondents who they trusted to protect their personal information and found that:[264]

  (i) 81% trusted health and medical institutions;

  (ii) 70% trusted banks;

  (iii) 69% trusted national public authorities; and

  (iv) 32% trusted online businesses.

---

[260] Royal Statistical Society (2014). Royal Statistical Society research on trust in data and attitudes towards data use / data sharing
[261] Ipsos MORI (2016d). Use of anonymised personal information.
[262] Data and Marketing Association and Acxiom (2018). Data privacy: What the consumer really thinks
[263] Royal Statistical Society (2014). Royal Statistical Society research on trust in data and attitudes towards data use / data sharing
[264] European Commission (2015). Special Eurobarometer 431: Data protection

- The ICO found that 66% of UK respondents trust the NHS or their local GP in storing and using their personal information but only 15% trust social messaging platforms to do the same.[265]

- Demos and Opinium found that while 60% of respondents were comfortable sharing their personal information with government departments only 11% were comfortable sharing it with social media organisations.[266]

Why the data is processed

260. Consumers are more willing to share data if there is a clear benefit to them or society. The Royal Statistical Society found that many studies concluded that if there was a clear personal, local or societal benefit, respondents were more likely to support data sharing.[267] Similarly, Ipsos MORI found that a clear benefit for both individuals and society was the seen as the only good rationale to justify a different approach to privacy with regards to health data.[268] The CDEI also found that support for online targeting appears highest in situations where the targeting clearly benefits the individual or others.

261. For example, the Royal Statistical Society found that 50% of respondents supported government bodies sharing anonymised data with researchers in universities and similar organisations to help them conduct government funded research.[269] In contrast, roughly 26% of consumers supported sharing anonymised data with companies to help them improve their products or services. The presence of strict controls on how the companies access and use the data made little difference in consumer support.

Academic Research

262. The information from academic research largely reflects the consumer surveys. Some specific examples from academic research are:

- *Type of data:* Winegar and Sunstein (2019) found that consumers demanded significantly more money for access to their data when personal data was explained with health data than when it was explained with demographic data.

---

[265] Information Commissioner's Office (2019). Information Rights Strategic Plan: Trust and confidence.
[266] Bartlett, J. & Gaston, S., (2017). Public views towards technology futures.
[267] Royal Statistical Society (2017). Data governance: public engagement review.
[268] Ipsos MORI (2016c). The one-way mirror: Public attitudes to commercial access to health data.
[269] Royal Statistical Society (2014). Royal Statistical Society research on trust in data and attitudes towards data use / data sharing

- *Who is processing the data:* Martin and Shilton (2016) found that privacy expectations vary depending on the type of data collected and the context in which it would be used.

- *Why the data is processed:* Robinson (2018) found that participants were significantly more likely to disclose data online if they could perceive purchase benefits.

Do consumers trust organisations with their data?

Academic Research

263. There is some evidence that users may take into account considerations other than a firm's privacy policy when deciding to trust a firm with their data. Bechmann (2015) suggests that a consumer's decision to consent increasingly relies on group processes. For example, consenting to an online service can be dependent on the reputation of the service rather than seeking out relevant information in the online policies relating to the service. Consumers may also use different methods such as detailed research into how a service operated or the use of proxy assurances, such as online reviews. (Whitley and Pujadas, 2018),

Consumer Research

264. There is clear evidence that consumers do not trust companies with their data. Both the Royal Statistical Society and the ICO concluded this finding in their literature reviews and in addition, a separate survey by the ICO also found that only 28% of respondents trusted companies and organisations with their personal information. [270,271,272]

265. Social media or messaging networks are the least trusted online platforms, with only a minority of consumers reporting that they trust social media platforms with their data:

    - In 2019 the ICO found only 15% of respondents trusted social messaging platforms in regard to storing and using their personal information.[273]

[270] Information Commissioner's Office (2015). Data protection rights: What the public want and what the public want from data protection authorities.
[271] Royal Statistical Society (2017). Data governance: public engagement review.
[272] Information Commissioner's Office (2019). Information Rights Strategic Plan: Trust and Confidence.
[273] Information Commissioner's Office (2018). Information Rights Strategic Plan: Trust and Confidence.

- In 2017 the ODI found that only 10% of respondents trusted social media organisations with their data.[274]

- In 2016 Ipsos MORI found that only 9% of respondents trusted networks with their data.[275]

266. Out of 13 online platforms, Ofcom and the ICO found that Facebook was the least trusted platform amongst adult respondents.[276] Similarly, out of 10 online platforms, they found that TikTok was the least trusted platform among kids aged 12-15 although Snapchat, Twitch and Facebook also had low levels of trust.

267. Some consumers also believe that platforms will do what they want with their data regardless of what the consumer agrees to. Doteveryone found that almost half (45%) of respondents said there is no point reading terms and conditions because companies do what they want anyway.[277] In qualitative interviews by Which? some respondents felt that companies would just find another way to gather the data they wanted.[278]

268. This finding is striking as consumers report that trust is one of the most important considerations for them when making decisions in the online environment. For example:

- In 2020 The CDEI found that the level of acceptability for online targeting is related to a respondent's level of trust in the organisation utilising the targeting.[279]

- In 2018 the DMA found that trust was consistently ranked as one of the top three most important factors a respondent considers when deciding whether or not to share data.[280]

- In 2018 the ODI found that 94% of respondents indicated that trust was important when deciding to share their data.[281]

---

[274] Open Data Institute (2018). Attitude towards data sharing – Europe.
[275] Ipsos MORI (2016a). Digital footprints: Consumer concerns about privacy and security.
[276] Ofcom & Information Commissioner's Office (2019). Internet users' concerns about and experience of potential online harms. Pages 70-71
[277] Miller, C., Kitcher, H., Perera, K. & Abiola, A., (2020) for Doteveryone. People, Power and Technology: The 2020 Digital Attitudes Report
[278] Which? (2018). Control, Alt or Delete? Consumer research on attitudes to data collection and use.
[279] The Centre for Data Ethics and Innovation (2020). Review of online targeting: Final report and recommendations.
[280] Data and Marketing Association and Acxiom (2018). Data privacy: What the consumer really thinks
[281] Open Data Institute (2018). Attitudes towards data sharing.

- In 2016 Ipsos MORI found that 49% of respondents agreed that they are only willing to give access to their personal information to a company or brand they trust.[282]

269. There is evidence that younger consumers are more likely to trust platforms with their personal data. For example, the ODI found that while 25% of 18-24-year olds trusted social media platforms with their data, only 5% of those aged between 45-54 did.[283] Similarly, Ofcom found that children aged 12-15 were more likely to trust social media platforms than adults.[284]

What are consumers' attitudes towards personalised advertising?

270. In the case of advertising, platforms are looking to find a balance between the level of advertising that provides consumers with information about products and services in a welfare enhancing way but avoids tipping into being intrusive or annoying and thus making consumers less receptive to the marketing messages.[285]

271. Tucker (2013) has suggested that giving consumers explicit control over how their data is being used (and so potentially increasing information about the data collection process) may be able to help platforms alleviate some of the trade-off between how informative advertising can be and how intrusive consumers find it.

272. We note that there is evidence that some consumers are not aware of the role advertising plays in funding online platforms. In 2020 Doteveryone reported that just under two thirds (62%) of people think that social media is funded through advertising that is based either on relevance or personalised targeting. This was largely unchanged from their findings in 2018.[286]. Ofcom also found that just over half (53%) of respondents knew that advertising was the main source of funding for search engines.[287]

---

[282] Ipsos MORI (2016a). Digital footprints: Consumer concerns about privacy and security.
[283] Open Data Institute (2018). Attitudes towards data sharing.
[284] Ofcom & Information Commissioner's Office (2019). Internet users' concerns about and experience of potential online harms. Pages 70-71
[285] If a consumer perceives an advert to be overly intrusive or encroaching this can prompt 'reactance' on the part of the consumer. That is, they resist in behaving in the opposite way to the one intended which in this case would be not finding the advert appealing (Tucker, 2012).
[286] Miller, C., Kitcher, H., Perera, K. & Abiola, A., (2020) for Doteveryone. People, Power and Technology: The 2020 Digital Attitudes Report
[287] Ofcom (2020). Online nation 2020 report

Do consumers want personalised ads?

Consumer Research

273. It should first be noted that not all consumers are aware that the ads they receive can be personalised. For instance, Ofcom found that only 60% of respondents were aware that someone who visits the same website or app might see different adverts to the one they see.[288]

274. There is evidence that initially consumers who do not mind or enjoy advertising would prefer to see adverts that are relevant to them instead of seemingly random ads:

- In 2020 The CDEI found that 54% of respondents considered the personalisation of online adverts acceptable.[289]
- In 2019 Harris Interactive research for the ICO found 54% of participants in an online survey would prefer to see adverts that are relevant to them rather than seemingly random adverts.[290]
- In 2018 Ofcom found that 38% of respondents did not mind seeing ads provided the ad is for something they are interested in.[291]
- In 2018 when segmenting their respondents based on attitudes towards personalised advertising, the DMA characterised 57% of respondents as preferring personalised advertising to random advertising.[292]
- In 2018 Which? found that most focus group participants preferred targeted advertising and personalised discounts to non-targeted advertising and generic discounts.[293]

275. That being said, only a minority of consumers are happy to share their data to receive ads that are relevant to them:

[288] Ofcom (2019). Adults Media Use and Attitudes report - data tables. Table 93
[289] The Centre for Data Ethics and Innovation (2020). Review of online targeting: Final report and recommendations
[290] Harris Interactive (2019) for the ICO. Adtech – Market research report
[291] Ofcom (2019). Adults Media Use and Attitudes report - data tables. Table 94
[292] Data and Marketing Association (2018). GDPR: A consumer perspective.
[293] Which? (2018). Control, Alt or Delete? Consumer research on attitudes to data collection and use.

- In 2019 the Oxford Internet Institute found that 32% of respondents were comfortable with the use of targeted advertising and the use of tracking data for commercial purposes.[294]

- In 2019 Ofcom found that only 13% of respondents were happy for online companies to collect and use their data to show more relevant adverts or information.[295]

- In 2018 Ofcom found that only 24% of respondents did not mind if organisations used their information to decide what ads they are shown.[296]

- The DMA found that only 6% of respondents ranked receiving personalised advertising as one of the top factors that would make them happy to share their personal information.[297]

276. Although consumers prefer the advertising they see to be relevant, there is evidence that as consumers learn more about the data processing behind personalised advertising, they become more uncomfortable and uneasy. In turn, personalised advertising becomes less desirable. Harris Interactive research for the ICO found that after providing a description of how 'real-time bidding' in advertising worked, the percentage of respondents who said they did not prefer relevant ads increased from 20% to 61%[298] and the number of consumers who thought it was unacceptable for websites to display targeted advertising in order to remain free increased from 14% to 43%.

277. Which? found that participants initially thought personalised advertising operated on relatively broad categories such as sex or age range.[299] After the extent of data profiling was explained participants became more concerned, and even those with initially tolerant attitudes became negative towards personalised advertising. Another survey also found that consumers can become uncomfortable with labels that seem to get attached to them by online targeting.[300]

How do consumers interact with personalised ads?

Academic Research

---

[294] Oxford Internet Institute (2019). Perceived threats to privacy online: The internet in Britain.
[295] Ofcom (2020). Online nation 2020 report
[296] Ofcom (2019). Adult Media Use and Attitudes report - data tables. Table 94
[297] Data and Marketing Association & Acxiom (2018). Data privacy: What the consumer really thinks.
[298] Harris Interactive(2019) for the ICO. Adtech – Market research report
[299] Which? (2018). Control, Alt or Delete? Consumer research on attitudes to data collection and use.
[300] Bucher, T. (2018). If... Then: Algorithmic power and politics. Oxford University Press.

278. The research finds that consumers find it difficult to avoid on-line tracking, but they can develop coping strategies in respect of digital advertising.

279. In general terms, consumers' actual scope to prevent personalised data being collected may be limited by 'take it or leave it' privacy policies (Shklovski et al (2014)). A consequence of such privacy policies is that consumers cannot avoid their personal data being collected and this can then be exacerbated through network and lock-in effects eg with respect to social media platforms. Frequent changes in the privacy policies of websites and products may also thwart consumers who attempt to find ways to escape such tracking. For instance, many companies will reinstall cookies that have been deleted.

280. However, some consumers develop strategies to avoid personalised advertising. For instance, using eye-tracking technology Drèze and Hussherr (2003) document consumers physically avoiding looking at banner advertisements when surfing the Internet. There is also mechanical avoidance ie the use of ad blocking software and Rejón-Guardia et al (2014) also describe 'cognitive avoidance' which relates to consumers' selective attention to advertising.

Consumer research

281. There is some evidence that consumers do not feel in control of the ads they see online. In 2019 Harris Interactive research for the ICO found that 42% of respondents felt like they had no control over the ads they see.[301] After real time bidding in digital advertising was described to these consumers, the percentage of consumers who felt like they had no control increased to 59%.

282. Despite this, most consumers report having taken action to avoid seeing online ads. For example, in 2018 Ofcom found that 73% of respondents reported taking steps to avoid ads online. [302] The most commonly reported method for avoiding ads was to opt-out of receiving marketing information from an online platform:

- In 2018 Ofcom found that 58% of respondents claimed that they used opt-out options.[303]

[301] Harris Interactive (2019) for the ICO. Adtech – Market research report
[302] Ofcom (2019). Adults: Media use and attitudes report 2019 – data tables. Table 95
[303] Ofcom (2019). Adults: Media use and attitudes report 2019 – data tables. Table 95

- In 2016 Ipsos MORI found that 75% of respondents said they often opted-out of receiving marketing information.[304]

283. The second most common method was to use ad blockers:

- IAB UK found that just under 23% of respondents reported currently using ad blockers in 2019.[305]
- Ofcom found that 34% of respondents reported currently using ad-blocking filters or software in 2018.[306]
- Harris Interactive research for the ICO found that just under 23% of respondents have tried to stop websites displaying adverts using an adblocker.[307]
- The DMA found that 32% of respondents reported currently using ad-blocking software in 2017.[308]
- The European Commission found that 36% of UK respondents reported currently using software that protects them from seeing online adverts in 2016.[309]

284. There should be some caution when interpreting self-reported ad-blocking usage. IAB UK found in their survey that 13% of respondents selected anti-virus software or a non-existent ad blocker as their only means of blocking ads.[310] It is possible that real ad-blocking levels are lower than the self-reported rates. Furthermore, the majority of ad-blocking software tended to be installed on laptops or desktops whereas consumers spend a significant proportion of their time on mobile devices.

[304] Ipsos MORI (2016a). Digital footprints: Consumer concerns about privacy and security.
[305] YouGov for IAB UK (2019). Ad blocking: Consumer usage and attitudes.
[306] Ofcom (2019). Adults: Media use and attitudes report 2019 – data tables. Table 95
[307] Harris Interactive (2019) for the ICO. Adtech – Market research report
[308] Data and Marketing Association and Acxiom (2018). Data privacy: What the consumer really thinks
[309] European Commission (2016b). Flash Eurobarometer 443: e-Privacy
[310] YouGov for IAB UK (2019). Ad blocking: Consumer usage and attitudes.

Consumer perceptions of the benefits and harms of data processing and behaviourally based targeted advertising

Are consumers aware of the potential benefits of personalised advertising and data processing?

285. Few surveys have specifically examined what UK consumers perceive the benefits or harms of behaviourally based targeted advertising and data processing to be.[311] Instead, many surveys focus on broader benefits and harms resulting from all forms of online targeting. As such, this and the next section utilise qualitative work by Which? supplemented with broader surveys to explore the benefits and harm of targeted advertising and data processing.

286. Which? found that many participants struggled to perceive any specific benefits of data processing until they were provided with examples of services and products that utilised data processing to operate, such as price comparison sites.[312] Consumers were then able to perceive various benefits of data processing, such as receiving more relevant information or collecting traffic information to improve customer journeys.

287. Consumers recognise that personalised advertising increases the relevance of what they are shown. Indeed, as noted above, some consumers voice frustration when ads are not related to their interests. For example, Which? found that participants who preferred relevant ads, said they feel they are more likely to use the ad and benefit from it.[313]

288. However, there is also evidence that very few consumers are willing to share their data in return for these benefits. For example:

- In 2018 Ofcom found that only 15% of respondents were happy for online companies to collect and use their data in return for a personalised service. [314]

- In 2016 Ipsos MORI found that only 5% of respondents felt that companies using their personal information to send more personalised adverts and marketing materials to try and sell more goods and services benefited them greatly.[315]

[311] For the purpose of this report we do not include political advertising.
[312] Which? (2018). Control, Alt or Delete? Consumer research on attitudes to data collection and use.
[313] Which? (2018). Control, Alt or Delete? Consumer research on attitudes to data collection and use.
[314] Ofcom (2019). Adults: Media use and attitudes report 2019 – data tables. Table 98
[315] Ipsos MORI (2016a). Digital footprints: Consumer concerns about privacy and security.

- Ipsos MORI also found that only 9% of respondents felt it benefitted them greatly if companies used their information as a way to keep the prices they charge for goods or services cheap or free.

- In 2015 Deloitte found that only 22% of respondents agreed they were happy for companies to use their information to offer personalised products.[316]

289. Most consumers also believe that companies should still ask for permission even if the data processing will benefit the user. For example, the European Commission found that 81% of UK respondents felt it was unacceptable for a company to share information about them without permission, even if this helps the company provide new services the user may like.[317]

Are consumers aware of the potential harms of behaviourally based targeted advertising and data processing?

290. Which? found that most participants did not have immediate concerns about personalised advertising per se.[318] These participants felt that they still retained ultimate control over what they purchased and could not pinpoint any specific harm that might result from targeted advertising. For example, participants felt that they could just ignore targeted advertising if they were not interested in the ad.

291. Consumers also struggled to identify specific tangible harms from data processing. Nevertheless, there were a number of recurring general concerns about data processing that were present in the surveys we have reviewed.

Loss of privacy

292. A common concern across surveys was the potential for data processing to harm consumers through a loss in privacy.

293. Most survey participants were concerned about the impact of data processing on their privacy in general. For example, Ipsos MORI found that 67% of internet users were concerned about their privacy when going online.[319] The

[316] Deloitte (2015). The Deloitte consumer review. Made-to-order: The rise of mass personalisation.
[317] The European Commission (2016b). Flash Eurobarometer 443: e-Privacy
[318] Which? (2018). Control, Alt or Delete? Consumer research on attitudes to data collection and use.
[319] Ipsos MORI (2016a). Digital footprints: Consumer concerns about privacy and security.

Royal Statistical Society also found that a common concern for participants of research studies was that data about them could be traced back to them.[320]

294. Which? also found that participants were concerned about organisations inferring characteristics that they did not want to be shared. This included factors that participants considered to be personal, such as sexual orientation, or factors they felt were subjective, such as IQ. [321]

295. Participants deemed to be vulnerable were also more likely to be concerned about a loss in privacy.[322] These participants felt that the loss of privacy through data collection was both discomforting and had the potential to cause harm through discrimination. For example, participants with a health condition were concerned that data collection could allow organisations to make assumptions about their conditions and they could be stigmatised as a result.

296. These findings indicate that consumers perceive two separate types of privacy harms from data processing. The first relates to a general loss of privacy whereby data processing leads to reduced levels of privacy as more and more personal data is collected and shared. The second harm refers to the loss of privacy in areas which are considered sensitive, such as sexual orientation or health status. This has more immediacy for consumers and they are better able to visualise the harm from the loss of privacy.

Use of personal data for automated decisions

297. Another concern is the use of personal data for automated decisions such as targeted advertising. For example, the ICO found that 54% of participants were concerned that personal information will be used in an automated way to make decisions about them.[323]

298. Which? found that as the data ecosystem was explained to participants, they became concerned about the frequency and range of decisions that organisations could make using inferred data.[324] As highlighted above, participants were also concerned that organisations may use data that they do not wish to share against them.

---

[320] Royal Statistical Society (2017). Data governance: public engagement review.
[321] Which? (2018). Control, Alt or Delete? Consumer research on attitudes to data collection and use.
[322] Vulnerable consumers were defined as: older people aged 80 years and over; people belonging to a lower SEG group (DE); people with a long-term physical or mental health condition/disability; and people who do not feel confident speaking, reading or writing in English.
[323] Information Commissioner's Office (2019). Information Rights Strategic Plan: Trust and Confidence.
[324] Which? (2018). Control, Alt or Delete? Consumer research on attitudes to data collection and use.

299. Which? further found that participants who did not have confidence in the accuracy of algorithmic inferences felt that demographic information was likely to stereotype them.[325] These participants were concerned that by attempting to target consumers using personal data, incorrect data could be accidentally collected and this would result in outcomes that did not reflect their true preferences.

300. Which? also found that participants felt that they were unable to challenge or rectify the results of automated decisions as they did not know what assumptions an organisation held about them. Vulnerable participants in particular were concerned that organisations could have acquired data from third parties and could use this data but not reveal that they held it. [326]

Loss of control

301. Consumers also report feeling a lack of control over both the ads they see and the data processing to support those ads. For example, the Centre for Data Ethics and Innovation [CDEI] found that only 36% of their survey respondents believe they have meaningful control over online targeting systems.[327] Ofcom and the ICO similarly found that only 18% of participants agreed they had full control over the ads they see.[328]

302. In relation to data processing, the European Commission found that only 14% of UK respondents felt that they had complete control over their online data compared to 84% who felt they had little or no control over their data.[329] Ipsos MORI also found that only 6% of consumers felt like they had a great deal of control over their online data compared to 69% who felt they had little or no control over their data.[330]

303. Some participants in the Which? focus groups reported that it was difficult to determine if the targeting was accurate because it was difficult for consumers to determine the basis on which they were being targeted and whether the data being used was accurate.

Data security

304. Consumers are also aware that their data could be stolen or leaked when used in online targeting. For instance, participants in Which?'s focus groups

---

[325] Which? (2018). Control, Alt or Delete? Consumer research on attitudes to data collection and use.
[326] Which? (2018). Control, Alt or Delete? Consumer research on attitudes to data collection and use.
[327] The Centre for Data Ethics (2020). Review of online targeting: Final report and recommendations.
[328] Harris Interactive (2019) for the ICO. Adtech – Market research report.
[329] European Commission (2019). Special Eurobarometer 487a: The General Data Protection Regulation.
[330] Ipsos MORI (2016a). Digital footprints: Consumer concerns about privacy and security.

were able to specifically identify potential harms from financial data being hacked or stolen.[331] However, it should be noted that while some participants reported experiences of data breaches, none claimed to have fallen victim to fraud as a result. Instead, these consumers' concerns may reflect potential psychological harm from the anxiety of possibly falling victim to fraud.

305. Which? found that the security of personal data was not a strongly held concern when participants thought about their data or online services, especially when considering non-financial data. Which? found that was due to three reasons:

- Participants were unable to identify the harm of non-financial information being stolen.
- Participants believed that they would be compensated should they fall victim to financial fraud.
- Participant's perceived data security to be out of their control and that data breaches were inevitable.

306. There is limited evidence on what consumers understand are the benefits of data processing.

Lack of trust

307. Participants pointed to a lack of trust towards data processing, targeted advertising and the organisations that provided them. Which?, for example, found that many participants believed there was no point in engaging as any potential benefit was minimal and far outweighed by the costs of engaging.

308. Underlying this belief was a widespread sense of distrust towards the organisations that enabled these activities. For example, the CDEI found that many participants believed organisations purposefully made their user controls to be difficult to find, complicated in their layout and overly burdensome to navigate.[332] Both the Royal Statistical Society and the ICO found that consumers did not trust commercial organisations with their data. A separate survey by the ICO also found that only 28% of respondents trusted companies and organisations with their personal information.

309. The lack of trust and disengagement are harmful for consumers as they inhibit consumers' perceived choices and feeling of control. For example, Which?

---

[331] Which? (2018). Control, Alt or Delete? Consumer research on attitudes to data collection and use.
[332] The Centre for Data Ethics (2020). Review of online targeting: Final report and recommendations.

found that participants believed there was little use to paying services a fee in exchange for halting third party data sharing because they felt organisations would still share their data regardless.[333]

What influences consumers' perception of potential harms and benefits?

310. As set out in Topic 1, survey evidence indicates that very few consumers fully understand what, how and why data is collected and shared or how personalised advertising operates. As Which? explains, this inherent opaqueness limits consumers' ability to anticipate potential benefits or harms.

311. We note that it was reported in the Which? focus groups that participants would often talk about the convenience and data-driven platforms being free to use.[334] These same participants would then immediately start talking negatively about data processing. As the focus groups progressed, it became clear that these participants were not making the connection that data processing was integral for these data-driven platforms. Ipsos MORI also found in qualitative interviews that respondents struggled to recognise the benefits of sharing their personal data. [335]

312. Which? also found that few participants were aware that their data is often shared and aggregated by data brokers to create detailed data profiles which could then be used to target them. Few participants were aware of the breadth and depth of information that could be collected about them.

313. Recent, qualitative research from Which? has focused on the methods used to collect data for personalised advertising.[336] This qualitative research found that:

- A majority of participants had a preference to receive targeted, rather than generic, adverts but they were unaware of the extent of data collection used to inform the targeting. This lack of awareness of the depth and breadth of data collection was particularly associated with third-party data collection methods and it led to perceptions of a lack of transparency over the use of such methods. Whilst participants assumed that the consent was in terms and conditions, they felt it wasn't acceptable to "bury" them in this way.

[333] Which? (2018). Control, Alt or Delete? Consumer research on attitudes to data collection and use.
[334] Which? (2018). Control, Alt or Delete? Consumer research on attitudes to data collection and use.
[335] Ipsos MORI (2016a). Digital footprints: Consumer concerns about privacy and security.
[336] Which? (2020). Are you following me? Consumer attitudes towards data collection methods for targeted advertising.

- Third-party data collection was generally considered less acceptable than first-party data collection. These feelings are informed by a number of factors including the perceived legitimacy of the data collection, privacy issues, and the relevance and proportionality of the data collection for targeted adverts.

- Participants had a clear preference that they should have to opt-in to data collection for targeted advertising, rather than opt-out, and they wanted to be asked to consent to each data collection method individually. It was noted that if a user was asked about each method separately their consent could be fluid, so that they could change what collection methods they opted-in to should there be times when they wanted targeted adverts on a specific content or to improve the relevance of adverts in general.

What are the potential implications for remedies?

314. The academic literature and consumer survey material has also addressed a number of ways of thinking about potential consumer facing remedies. The role of consumer biases and choice architecture

315. As indicated above, as well as identifying that behavioural biases and choice architecture can lead users to make decisions which do not necessarily reflect their actual preferences, research indicates that the same techniques can be harnessed to help shape interventions to assist users in making better choices.

316. Interventions in this area can take a number of different forms depending on the issue that is being addressed. The academic research discusses the role of interventions based on nudging consumers. ‘Nudging’ interventions are ones which are designed to address issues arising from specific behavioural biases. A key aspect of a nudge intervention is that it should change the choice architecture to nudge consumers to make decisions that are better aligned with their privacy objectives but does not actually restrict the user’s set of choices.

317. Acquisti et al (2017) bring together research from different fields and propose a taxonomy of different nudge-based interventions according to the cognitive or behavioural bias the nudge is designed to address. One important aspect of their research is that the different approaches should be regarded as complements rather than substitutes. They suggest that although the target of an intervention might be a particular ‘bias’ (eg providing additional information to reduce information asymmetries or reducing the consumer effort by configuring default settings to align with their expectations / preferences),

other factors are likely to be relevant to the success of the intervention. Thus, a mechanism for providing feedback to the consumer can help to improve the effectiveness of an information remedy. Similarly, a remedy which focuses on how information is presented to a consumer will need to take into account other factors such as the framing, ordering and saliency of the information.

318. The research on these issues as it relates to the design of information and presentation interventions is discussed in more detail below.

Information-based remedies: simplified privacy policies

319. A major stream of research has centred around simplifying privacy policies. This has arisen from the premise that it is the opportunity cost of reading terms and conditions that stops consumers from engaging with them.[337]

320. Researchers have experimented with easy-to-use language and concise information as well as with web-design and software tools. The evidence from these studies is mixed as is described in the box below.

McDonald et al (2009) compared three different formats for privacy policies:
(i) layered policies, which present a short form with standardized components in addition to a full policy;
(ii) a Privacy Finder privacy report, which standardizes the text descriptions of privacy practices in a brief bulleted format; and,
(iii) conventional non-standardized human-readable policies.

The study focused on the impact of the different approaches on the accuracy and recall of participants. They applied these formats to the privacy policies of 6 large companies: Disney, Microsoft, Nextag, IBM, Walmart and O'Reilly. Their sample consisted of 749 participants across 15 different treatments.

In fact, the authors found that participants were not able to reliably understand companies' privacy practices with any of the formats. In terms of comparisons between the three different formats they did find that participants were faster with standardized formats compared to natural language formats but that accuracy suffered. They also found that the Privacy Finder format was better for accuracy on harder questions that natural language formats.

321. In contrast to the McDonald et al (2009) results, in an experiment by the European Commission in 2016, simplifying and shortening terms and conditions had a small positive effect on readership and understanding.[338] It was also found to increase trust and the perceived quality of the terms and conditions, while also reducing consumer frustration.

[337] For example, the amount of time and effort required to read and understand online policies.
[338] European Commission (2016a). Study on consumers' attitudes towards online terms and conditions.

322. The European Commission also found that adding a reading cost cue with free exposure to the terms and conditions doubled the number of consumers opening the terms and conditions from 9.4% to 19.8%. It was suggested that adding a reading cue could also act as an incentive for traders to reduce the length of their terms and conditions. Research by the Behavioural Insights Team (2019) also indicates that telling customers how long a privacy policy takes to read can increase the 'opening rates' for privacy policies by 105 per cent.

323. There have also been experiments with the use of privacy labels (eg like the ones used in food labelling) and icons. In the same 2016 study the European Commission found that adding a quality cue increased consumer trust on both the online platform and the terms and conditions.[339] However, the results of such experiments have been mixed and indeed in some cases there is a risk that such approaches may trigger misconceptions about the protection of their personal data.

324. Kelley et al (2010) found that standardized privacy labels, assisted by consumer education, can have a significant impact on users' understanding of privacy policies in an online user study. Their results show that standardized privacy formats which have been designed with usability in mind meant that participants were more accurate and faster in reading the standardized notices and could better compare different policies. Participants' enjoyment of the privacy policies also increased. The authors argued that the large amount of text in full-text policies and the need to drill down through a layered policy to the full policy to understand specific practices, lengthened the amount of time and effort required to understand a policy.

325. In a survey for the Financial Services Consumer Panel, Whitley and Pujadas (2018) asked participants what they thought would be ideal in a terms and condition statement.[340] The three highest rated statements were:

- a shorter length of text;
- highlighting of potential consumer risks at the start of the terms and conditions; and
- simple use of language and fewer technical terms.

[339] European Commission (2016a). Study on consumers' attitudes towards online terms and conditions.
[340] Whitley, E. & Pujadas, R. (2018) Report on a study of how consumers currently consent to share their financial data with a third party.

326. Participants in the CDEI's review of online targeting also agreed that significant changes to the design of online services and the information and controls offered to users is required.[341] These participants felt that companies should reduce the burden on users, particularly due to the complexity of decisions and judgements that are required online.

The Role of Feedback

327. Studies have looked at the impact on decision-making of providing users with a degree of feedback in real time as a way of helping them manage their privacy. As a relatively simple example, Ur et al (2012) looked at the impact of password strength meters which provided that provided visual feedback on password strength. They found that users who were shown password strength meters created longer passwords, and in the case of the more stringent password strength meters, also created passwords that were more difficult to guess. The study did, however, also report that users were likely to consider the stricter meters as 'annoying,' suggesting that nudges that tried to push users' expectations too far might not be as effective.

328. Tsai et al (2011) examined how online purchasing decisions were affected when the search engines they used included information about the merchants' privacy practices in their results. Web retailers will typically detail their information practices in their privacy policies, but most of the time this information remains invisible to consumers. The paper considered whether a more prominent display of privacy information would cause consumers to incorporate privacy considerations into their online purchasing decisions. Their research showed that providing accessible privacy information reduced the information asymmetry gap between merchants and consumers. This reduction tended to lead consumers to purchase from the online retailers that better protected their privacy.

329. Tsai et al (2009) looked at feedback in the context of location-sharing mobile apps. This included the field deployment of an interface that allowed users to see who had requested their information. In one treatment, users were given feedback in the form of a history of requests for their locations while the second treatment group were not given any feedback at all. They reported significant changes in privacy settings by users who are given such feedback. They argued that feedback was an important factor in improving user comfort levels and allaying privacy concerns. Users were found to refine their settings

[341] The Centre for Data Ethics and Innovation (2020). Review into online targeting: Final report and recommendations.

and selectively open-up, thereby deriving more value from the location-sharing app while having a better sense of control over their privacy.

330. Almuhimedi et al (2015) examined how interfaces and services can be designed to counter biases responsible for consumers making decisions about their security and privacy which were not necessarily in their interest. In a field study they evaluated the impact of giving users an app permission manager and sending them daily nudges eg informing Android users about the frequency with which their mobile apps were accessing sensitive data. They found that the combination of the two could motivate users to review and modify their permission settings. For instance, even after a week with access to the permission manager, 95% of participants reassessed their permissions, and 58% of them further restricted some of their permissions.

The Role of Framing

331. The way in which questions about privacy issues are framed or presented to users will have an impact on the information that is disclosed. Braunstein et al (2011) found that wording a survey question to remind users that they are revealing sensitive information had an effect on how much information they were willing to reveal. In particular, a reminder that data is sensitive would result in less disclosure.

332. Baek (2014) looked at harnessing the endowment effect in the way in which privacy decisions were framed. In Baek's experiment, users who were confronted with a privacy-related message were more likely than those in the control group to engage in thinking about their online privacy, protection, and disclosure behaviours. That is, when the concept of privacy was introduced, the subjects were more likely to consider privacy-protective behaviour. In particular, this persuasion effect was pronounced among people with a low level of online knowledge. This approach could mean that individuals would be less vulnerable to disclosure influences as a result of their loss aversion and their sensitivity to loss.

333. The content as well as the format (or presentation) of privacy notices can also be important in determining consumers’ decisions about the amount of information they disclose. In an experimental setting, Samat and Acquisti (2017) manipulated the content as well as the format of privacy notices shown to participants who were asked to choose whether they would like to disclose personal information. They found that participants were significantly less likely to share their personal information when the privacy notice was presented in terms of a 'Prohibit [disclosure]' frame, as compared to an 'Allow [disclosure]' frame. Importantly, they found that the effect of changes in framing became

larger when the risk to consumers attached to the disclosure of information was increased (eg when it related to more sensitive personal information).

The Role of Timing / Saliency

334. The timing at which privacy notices are presented to users will also be important in terms of how deeply users engage with those policies.

335. Schaub et al (2015) carried out a review of the literature on privacy notices. They found that 'just-in-time' notices providing relevant, clear, and contextual information could help to mitigate information asymmetries. They argued that a key aspect of effective notice design was the understanding that a privacy policy, which might be necessary for regulatory compliance, was not sufficient and was often unsuitable for informing users. Among a number of relevant factors, they found that 'actionability' was important: privacy notices without control could leave users feeling helpless. They argued that empowering users with privacy controls increased their trust and could result in increased use and disclosure. They considered that best practice involved providing notices and control options at different times in the information lifecycle.

336. Egelman et al (2009) investigated whether participants in a lab study were more likely to pay a premium for websites with good privacy practices. They found that the timing of the privacy notice was important; viewing privacy indicators before visiting the website had a greater impact than seeing the indicators once the users already arrived at the website.

337. In contrast, in the context of mobile apps, Balebaka et al (2015) found that showing privacy notice during app use significantly increased recall rates compared to showing it in the app store. They used a web survey and a field experiment to isolate different timing conditions for displaying privacy notices in mobile apps: in the app store, when an app is started, during app use, and after app use. Participants installed and played a history quiz app, either virtually or on their phone. After a distraction or delay they were asked to recall the privacy notice's content with recall being used as a proxy for the attention paid to and salience of the notice.

338. We note from consumer survey evidence that consumers value upfront communications about the benefits of sharing their data. In the surveys examined, roughly 85-91% of consumers agreed that transparency about how

data is collected and used is a key factor in their willingness to share data.[342,343,344]

339. Citizens Advice also found that one of the most important aspect of opting in or out of data sharing was clear visibility of what data smart products collect from the moment they sign up and start using them.[345]

340. In line with this, consumers expressed a desire for more transparency compared to what already exists. For most consumers this desire was focused around terms and conditions or privacy policies:

- Doteveryone found that 89% of respondents agreed that terms and conditions should be made clearer.[346]
- In their qualitative interviews, Ipsos MORI also found that there was a strong desire for 'executive summaries' for terms and conditions.[347]
- The DMA also found that 87% of respondents thought that when sharing their information with a company it was important that the terms and conditions are easy to read and understand.

Improving consumer understanding

341. There have been various attempts to improve consumers' understanding. Researchers have looked at harmonised information provisions to reduce the burden on consumers in terms of reading and understanding. Again, the use of icons is something that has been explored in this context and icons can generate trust on the part of consumers where they embody a certification scheme.

342. It has also been found that where privacy policies reflect individual's cultural background and preferences, then that tends to contribute to a better understanding. (WIK-Consult, 2015)

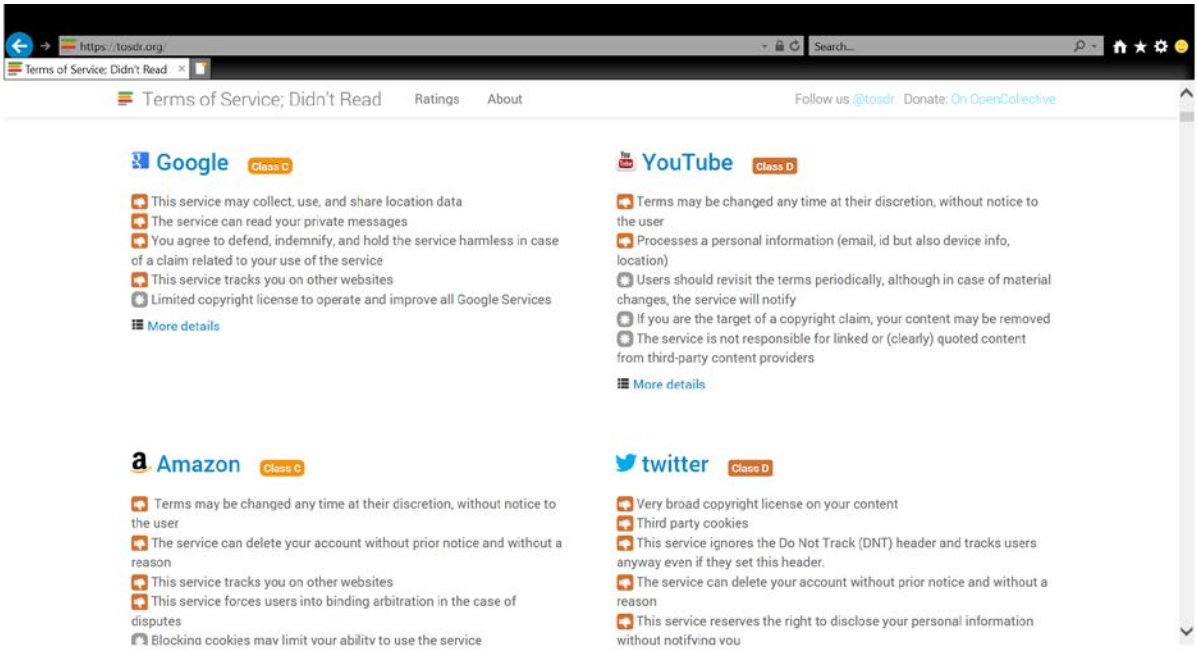
343. Other approaches have included the use of web / software-based tools that include the use of automated information extraction systems which can provide warnings about unexpected terms in a privacy policy. For instance,

---

[342] Data and Marketing Association and Acxiom (2018). GDPR: A consumer perspective.
[343] Miller, C., Coldicutt, R., & Kitcher, H. (2018) for Doteveryone. People, Power and Technology: The 2018 Digital Understanding Report.
[344] Data & Marketing Association & Acxiom (2018). Data privacy: What the consumer really thinks.
[345] Traverse for Citizens Advice (2018). The future of the smart home: Current consumer attitudes towards smart home technology.
[346] Miller, C., Coldicutt, R., & Kitcher, H. (2018) for Doteveryone. People, Power and Technology: The 2018 Digital Understanding Report.
[347] Ipsos MORI (2016a). Digital footprints: Consumer concerns about privacy and security.

the website 'Terms of Service Didn't Read' offers a browser add-on that provides easy to understand feedback to consumers about the quality of service of the terms of service they most likely have not read.

Figure L.1: Screenshot from 'Terms of Service didn't Read'



Source: https://tosdr.org/ (Accessed on 17th June 2020).

344. There have also been experiments involving the design of user interfaces. Ataei et al (2018) experimented with designing a user interface for the fine-grained management of location privacy settings on mobile devices. The prototype interface they used increased the transparency about what location data was being shared with whom, when and where, and also provided controls for adjusting their location sharing preferences. They found that it was possible to come up with an interface that led to a greater sense of control, was usable and well received, and that participants were keen on using it in real life.

345. The Behavioural Insights Team (2019) carried out a series of experiments which were intended to identify those approaches which were effective in improving consumers' understanding and, as importantly, identifying those measures where the evidence was more mixed or indeed suggested that certain approaches were not effective. Techniques which were found to be effective included:

- displaying key terms as frequently asked questions;
- using icons to illustrate key terms;

- showing customers your terms within a scrollable text box instead of requiring a click to view them
- providing information in short chunks at the right time

346. Techniques where the evidence was mixed or indicated that techniques were not effective included:

- presenting key points in a summary table;
- adding examples and icons to the full terms;
- shortening the full terms;
- Using simpler language;
- making summaries expandable, allowing customers to click each summary point for more information; and,
- adding emoji symbols to terms.

Is it possible to ensure that consumers take action?

347. The results of a number of experiments suggest a more contextualised and adaptive approach is important to ensure consumers take action. As part of this there is the suggestion that 'nudging' may be another approach to remind people of their choices and options with respect to their personal data. Researchers have considered the use of: visual ratings on privacy policies of mobile apps; opt-outs; and a mobile privacy nudge that provided concise privacy-relevant information.

348. One specific experiment explored the use of nudges in the context of social media platforms to examine whether it was possible to help users avoid posting embarrassing messages using potential privacy nudges (Wang et al,

Wang et al (2013) examined whether it was possible to helps users of a social network (Facebook) avoid posting embarrassing messages ie over-sharing personal information they later regretted. The authors developed an experimental platform that modified the Facebook interface and allowed collecting users' behavioural data.

The study focused on two types of nudges: one to remind users about the audience for their post (by showing profiles/pictures of the recipients of the post), and one to encourage users to pause and think before posting (by introducing a short time-delay). Across a 6-week period, the researchers collected data without the nudging interventions in the first 3- week period and then in the second three-week period they introduced the nudges.

2013). Although the field trial was exploratory – see box below – the authors concluded that privacy nudges could be a powerful instrument to make consumers think about the consequences of their actions.

349. Other research indicates that seemingly small implementation decisions can have a significant impact on whether and how consumers interact with consent notices. For instance, how data privacy options are displayed in a screen vertically (ie whether one option is positioning higher than the other) may influence the proportion of users that will choose a given option (Acquisti et al, 2013).

350. More recently, in a series of experiments involving 80,000 unique users on a German website, Utz et al (2019) identified that consumers were more likely to interact with a notice placed in the lower (left) part of the screen compared to other positions. They suggested that an explanation for the higher interaction rates with notices displayed at the bottom was that these notices were more likely to cover the main content of the websites and that if consumers used their thumbs to navigate websites on a smartphone, it was easier to tap elements on the bottom part of the screen than those at the top. An explanation for higher interaction rates with notices displayed on the left of the view could be due to the left-to-right directionality of Latin script.

351. These results point to the need to take into account factors a range of factors (including the ergonomics of design features) when presenting choices to consumers and the importance of trialling different approaches in order to ensure that consumers are able to make properly informed choices. These findings also point to the need to trial different approaches.

352. An important finding in the academic research is that there is no single solution or ‘silver bullet’ to address all the various issues around privacy and personal data (WIK-Consult, 2015). One particular finding was that awareness of the consumer is key, and that consumer information should be regarded more as a process rather than a one-off act. This could mean that there should be more focus on emphasising the specific adverse effects that may emerge from the collection and analysis of personal data. This would help raise awareness among consumers and could increase motivation to engage with terms and conditions.

Do consumers want more control over their data? If so, is that level of control practical?

353. There is evidence that control over data is very important for the vast majority of consumers. In particular, there was a strong emphasis on controlling who

the data was shared with. For example, in 2018 Doteveryone found that 91% of respondents felt it was important they choose how much data they share with companies.[348] In 2016, the European Commission found that 81% of UK respondents thought it was unacceptable for companies to share information without their permission in return for new services.[349]

354. There is some evidence that consumers desire more control over their data:

- In 2017 the DMA found that 86% of respondents wanted more control over the personal information they give companies.[350]
- The European Commission also found that 73% of UK consumers who did not have complete control over their data were concerned about not having full control.[351]
- Which? found that when participants learnt about the full data eco-system, they felt unable to control their data and desired more control over their data.[352]

355. However, Which? has argued that it might not be practical to give consumers themselves more control for three key reasons:

- the data ecosystem is too big and complex for them to keep control;
- people are unlikely to perceive that the benefit is worth the cost of engaging, because concerns are mostly intangible at the moment and detriment is hard for them to identify; and
- cognitive and behavioural biases may limit the effectiveness of many measures.

356. Instead, Which? argues that when consumers want more control, they often mean there should be more control in the data ecosystem.

---

[348] Miller, C., Coldicutt, R., & Kitcher, H. (2018) for Doteveryone. *People, Power and Technology: The 2018 Digital Understanding Report.*
[349] European Commission (2016b). *Flash Eurobarometer 443: e-Privacy*
[350] Data & Marketing Association and Acxiom (2018). *GDPR: A consumer perspective.*
[351] European Commission (2019). *Special Eurobarometer 487a: The General Data Protection Regulation.*
[352] Which? (2018). *Control, Alt or Delete? Consumer research on attitudes to data collection and use.*.

Do consumers want regulation?

357. Consumers perceive online media to be less regulated than traditional media. For example, Ofcom found that roughly 19% of respondents believed that social media or video share sites are unregulated.[353]

358. Perhaps spurred by this, there is strong evidence that consumers favour increased regulation for online platforms and media:

- This year the CDEI found that 61% of respondents preferred giving an independent regulator oversight of the use of online targeting systems, rather than self-regulation.[354]
- Doteveryone found this year that 58% of respondents' thought the tech sector is regulated too little.[355]
- In 2018 Doteveryone found that 66% of respondents wanted the government to help enforce rules that ensure service providers treat their customers and society fairly.[356]
- Ofcom found that 66% and 57% of consumers wanted more regulation for social media sites and video sharing sites respectively.[357]

359. There is also evidence that past regulation has made consumers feel more in control of their data:

- In an experiment with Croatian participants, Škrinjarić et al (2018) found that the perceived effectiveness of government regulation reduced online privacy concerns.
- In 2018, the ICO found that 65% of respondents would feel better if companies were required to inform customers if they had been affected by a data breach.[358]

[353] Ofcom (2020). Internet users' experience of harm online – data tables. Table 275 & 276
[354] The Centre for Data Ethics and Innovation (20200. Review of online targeting:
[355] Miller, C., Kitcher, H., Perera, K. & Abiola, A., (2020) for Doteveryone. People, Power and Technology: The 2020 Digital Attitudes Report
[356] Miller, C., Coldicutt, R., & Kitcher, H. (2018) for Doteveryone. People, Power and Technology: The 2018 Digital Understanding Report.
[357] Ofcom (2020). Internet users' experience of harm online – data tables. Table 281 & 282
[358] Information Commissioner's Office (2018). Information Rights Strategic Plan: Trust and Confidence.

- In 2017, the DMA found that 62% of respondents felt that the then upcoming GDPR would improve their confidence in sharing data with organisations.[359]

360. The Stigler Center (2019) also provides several reasons as to why government regulation is necessary for consumers best interests:

- the harms of privacy and security breaches are not internalized by firms;
- it is costly for consumers to monitor the consequences of privacy and security breaches;
- a great deal of information is held by firms with which consumers have no direct contact and little influence over; and
- consumers are often left to bear the burden of privacy and security breaches themselves despite rarely knowing what actions they can take.

361. The Stigler Center report also put forward a specific legal rule that that could apply to 'dark patterns.'[360,]

- 'Where a firm's choice architecture more than doubles the percentage of users who agree to share information, when compared with a neutral choice architecture, consumers' consent to share such information is not valid. Moreover, dark pattern tactics that satisfy this 'more likely than not' test should be treated as unfair and deceptive practices in trade, which are proscribed by federal and state consumer protection laws'.[361]

[359] Data and Marketing Association and Acxiom (2018). Data privacy: What the consumer really thinks
[360] Dark patterns are user interfaces that make it difficult for users to express their actual preferences or that manipulate users into taking actions that do not comport with their preferences or expectations.
[361] The report also offered a multi-factor balancing test for dark patterns that may be highly problematic but which did not satisfy the criteria for this legal rule. We note that one critique of this proposition is that it is very difficult, if not impossible to achieve a truly neutral choice architecture so that it may not be possible to create a benchmark against which to measure potential 'dark patterns'.

Annex 1: Consumer Survey Methodology

362. When selecting and interpreting the consumer surveys we have used the following criteria:

- Time: We have given prominence to surveys taken within the past three years. The online environment is rapidly changing and there have been numerous and highly covered data leaks.[362] This has been shown to have an impact on consumers and has been taken into consideration.[363]

- Country: We have given prominence to UK surveys or surveys with explicit UK statistics. Where necessary, we have used international surveys to provide some context for the reader, but these statistics should not be taken to be representative of the UK population.

- Methodology: We have given prominence to surveys involving more rigorous methodologies. For example, when considering quantitative surveys, we prioritised face-to-face interviews the most, followed by telephone interviews and online surveys. We then cross-checked each survey with the sampling methodology in these surveys to apply appropriate weighting.

363. When examining the surveys, we noted several factors that are likely to influence the accuracy of the results:

- Due to their very nature, online surveys are likely to overrepresent consumers who are comfortable with technology and being active online. Therefore, it is possible that surveys which only utilised online sampling may produce slightly biased results, even if the data has been weighted to be representative of the overall population.

- The term 'personal data' can be a confusing for consumers and while the majority of consumers believe they understand what 'personal data' is, few understand the legal definition. Furthermore, many privacy policies define 'personal data' differently or may leave the term ambiguous for readers.[364]

---

[362] Such as the Cambridge Analytica scandal.
[363] For example, Which? found that roughly half of respondents reported being more concerned about what organisations can do with their information in light of the Cambridge Analytical scandal.
[364] For example, Digital Catapult found that 96% of participants claimed they could define personal data – however, there was no agreement on the definition and 64% of respondents incorrectly defined it as 'all information about me in existence. Digital Catapult (2015). Trust in personal data: a UK review.

- Consumers are more likely to provide socially acceptable answers or answers that present themselves in a positive light when answering surveys.[365] Therefore, it is possible that the prevalence of privacy behaviour in real life is lower than suggested by the survey statistics.

364. We also note that there a lack of consistency in the language and questions used across the different consumer surveys reviewed. For example, while some surveys asked consumers about data control in general, others focused on specific aspects of control (eg controlling who has access to a consumers' personal data). As a result, it can be hard to directly compare the data from different surveys.

365. We recognise that the consumer survey evidence is based on stated preferences rather than on actual observed behaviour and that in surveys respondents might be stating a preference about privacy without having to consider what a relevant counterfactual might be. However, the purpose of the review of the consumer survey evidence is to build up a picture of consumers' attitudes in general and identify broad themes in terms of issues and concerns. We use this material, combined with the findings from our review of academic research (which does analyse actual consumer decision-making in experimental settings and field experiments) and other data (including platforms' own data on user engagement with Privacy Policies and privacy controls and settings in practice)[366], to inform our evidence base.

[365] Evidence of this 'social desirability effect' can be found in number of consumers who claim to always read privacy policies compared to the statistics found in academic research.
[366] See Chapter 4 of the main report.

Annex 2 – Bibliography

Acquisti, A., (2004). 'Privacy in electronic commerce and the economics of immediate gratification.' In *Proceedings of the 5th ACM Conference on Electronic Commerce*. ACM, New York, NY, 21-29.

Acquisti, A., Brandimarte, L., and Loewenstein, G., (2015). 'Privacy and human behavior in the age of information.' *Science*, Vol. 347, Issue 6221, 509-514.

Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L.F., Komanduri, S., Leon, P.G., Sadeh, N., Schaub, F., Sleeper, M., Wang, Y., and Wilson, S. (2017). 'Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online ACM Computing Surveys, Vol. 50, No. 3, Article 44.

Acquisti, A., and Gross, R. (2006).'Imagined communities: Awareness, information sharing and privacy in Facebook.' In *Proceedings of the 6th International Workshop Privacy Enhancing Technology* (PET'06). Springer, 36-58.

Acquisti, A., and Grossklags, J. (2005) 'Privacy and Rationality in Individual Decision Making.' *IEEE Security and Privacy Magazine*, 3(1):26 – 33.

Acquisti, A., John, L.K., and Loewenstein, G. (2012). 'The impact of relative standards on the propensity to disclose.' *Journal of Market Research* ,49, 2, 160-174.

Acquisti, A., John, L.K. and Loewenstein, G. (2013) 'What is Privacy Worth?' *The Journal of Legal Studies,* Vol. 42, No. 2, 249-274.

Acquisti, A., Taylor, C.R., Wagman, L. (2016) 'The Economics of Privacy.' *Journal of Economic Literature*, Vol. 52, No. 2.

Adjerid, I., Acquisti, A., Brandimarte, L., and Loewenstein, G. (2013) 'Sleights of privacy: Framing, disclosures and the limits of transparency.' In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS13), ACM 1-11.*

Almuhimedi, H., Schaub, F., Sadeh, N., Adjerid, I., Acquisti, A., Gluck, J., Cranor, L.F., and Agarwal, Y., (2015) 'Your Location has been Shared 5,398 Times! A Field Study on Mobile App Privacy Nudging.' In *Proceedings of the Conference on Human Factors in Computing Systems (CHI'15)*, ACM, 1-10.

Ataei, M., Degbelo, A., and Kray, C., (2018). 'Privacy theory in practice: designing a user interface for managing location privacy on mobile devices.' *Journal of Location Based Services,* Volume 12, 3-4, 141-178.

Athey, S., Catalini, C., & Tucker, C. (2017) 'The digital privacy paradox: Small money, small costs, small talk.' *NBER Working Paper No. 23488.*

Baek, Y.M. (2014). 'Solving the privacy paradox: a counter-argument experimental approach.' *Computers in Human Behavior*, Vol.38, 33-42.

Bakos, Y., Marotta-Wurgler, F., Trossen, D.R. (2014) 'Does Anyone Read the Fine Print? Consumer Attention to Standard Form Contracts.' *Journal of Legal Studies, Vol. 43, No. 1.*

Balebaka, R., Schaub, F., Adjerid, I., Acquisti, A., and Cranor, L.F. (2015) 'The impact of timing on the salience of smartphone app privacy notices.' In *Proceedings of the CSS Workshop on Security and Privacy in Smartphone and Mobile Devices (SPSM'15)*, ACM, New York, NY, 63-74.

Bartlett, J. & Gaston, S., (2017). Public views on technology futures.

Bechmann, A. (2015). 'Non-Informed Consent Cultures: Privacy Policies and App Contracts on Facebook'. *Journal of Media Business Studies*. 11(1):21-38.

Behavioural Insights Team. 'The behavioural science of online harm and manipulation, and what to do about it. An exploratory paper to spark ideas and debate.' April 2019.

https://www.bi.team/wp-content/uploads/2019/04/BIT_The-behavioural-science-of-online-harm-and-manipulation-and-what-to-do-about-it_Single.pdf

Behavioural Insights Team. 'Best practice guide. Improving consumer understanding of contractual terms and privacy policies: evidence-based actions for businesses.' (July 2019). https://www.bi.team/publications/improving-consumer-understanding-of-contractual-terms-and-privacy-policies-evidence-based-actions-for-businesses/

Brandimarte, L., Acquisti, A., and Loewenstein, G. (2012). 'Misplaced confidences: Privacy and the control paradox.' *Social Psychology and Personality Science*, 4,3, 340-347.

Braunstein, A., Granka, L., and Staddon, J. (2011) 'Indirect content privacy surveys: Measuring privacy without asking about it' In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS'11)*. ACM 1-14.

Cardogan, R.A. (2004). 'An Imbalance of Power: The Readability of Internet Privacy Policies'. *Journal of Business and* Economic Research.

Centre for Data Ethics and Innovation (2019). Interim report: Review into online targeting.

Data & Marketing Association and Acxiom (2018a). GDPR: A consumer perspective.

Data & Marketing Association and Acxiom (2018b). Data privacy: What the consumer really thinks.

Deloitte (2015). The Deloitte consumer review. Made-to-order: The rise of mass personalisation

Deloitte (2017). 2017 Global mobile consumer survey: US edition.

Demos (2012). The Data Dialogue.

Digital Catapult (2015). Trust in personal data: a UK review.

Digital Content Next (2018): *Google data collection research.*

Drèze, X. and Hussherr, F. (2003) 'Internet advertising: Is anybody watching?' *Journal of Interactive Marketing*, 17(4):8 – 23.

DuckDuckGo (2017). A study on privacy browsing: Consumer usage, knowledge, and thoughts.

Egelman, S., Tsai, J., Cranor, L.F., and Acquisti, A. (2009) 'Timing is everything? The effects of timing and placement of online privacy indicators.' In Proceedings of the 27th International Conference on Human Factors in Computing Systems (CHI'09). ACM, New York, NY, 319-328.

Egelman, S., Porter Felt, A., and Wagner D. (2013) 'Choice architecture and smartphone privacy: There's a price for that.' In The Economics of the Information Society. Springer, 211-236.

European Commission (2015). Special Eurobarometer 431: Data protection

European Commission (2016a) Study on consumers' attitudes towards online terms and conditions.

European Commission (2016b). Flash Eurobarometer 443: e-Privacy

European Commission (2016c). Special Eurobarometer 447: Online platforms

European Commission (2018). Special Eurobarometer 480: European attitudes towards Internet security

European Commission (2019). Special Eurobarometer 487a: The General Data Protection Regulation.

Goldstein, D.G., Johnson, E.J., Herrman, A., and Heitmann, M. (2008) 'Nudge your customers towards better choices.' Harvard Business Review. 86, 12, 99-105.

Good, N., Grossklags, J., Thaw, D., Perzanowski, A., Mulligan, D., Konstan, J., (2006) 'User Choices and Regret: Understanding Users' Decision Process about Consensually Acquired Spyware', Faculty Publications. Paper 621. http://scholarlycommons.law.case.edu/faculty_publications/621

Grossklags, J., and Acquisti, A. (2007) 'When 25 cents is too much: An experiment on willingness-to-sell and willingness-to-protect personal information. In Proceedings of the Workshop on the Economics of Information Security (WEIS'07), 1-22.

Habib, H., Colnago, J., Gopalakrishnan, V., Pearman, S., Thomas, J., Acquisti, A., Christin, N., and Cranor, L.F. (2018). 'Away from prying eyes: analysing usage and understanding of private browsing.' In Proceedings of the Fourteenth USENIX Conference on Usable Privacy and Security, 159-175.

Harris Interactive (2019) for the ICO. Adtech – Market research report

Hoofnagle, C.J., and King, J. (2007) 'Consumer Information Sharing: Where the Sun Still Don't Shine.' Available at: https://www.law.berkeley.edu/files/sb27report.pdf

Hoofnagle, C.J., and King, J. (2008) 'What Californians understand about privacy online' Available at SSRN 1262130 (2008), 1-33.

Hoofnagle, C.J., and Whittington, J. (2014) 'Free: Accounting for the Costs of the Internet's Most Popular Price'. 61 UCLA L. Rev.

Hopkins Van Mil (2015). Big Data: Public views on the use of private sector data for social research.

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

Information Commissioner's Office (2015). Data protection rights: What the public want and what the public want from data protection authorities.

Information Commissioner's Office (2018). Information Rights Strategic Plan: Trust and Confidence.

Information Commissioner's Office (2019). Information Rights Strategic Plan: Trust and Confidence.

Ipsos MORI (2016a). Digital footprints: Consumer concerns about privacy and security.

Ipsos MORI (2016b). Awareness of personal information held by companies.

Ipsos MORI (2016c). The one-way mirror: Public attitudes to commercial access to health data.

Ipsos MORI (2016d). Use of anonymised personal information.

Johnson, E.J. (2012) 'Beyond Nudges: Tools of a Choice Architecture.' Marketing Letters, Vol 23, 487–504.

Kelley, P.G., Cesca, L., Bresee, J., and Cranor, L.F. (2010). 'Standardizing privacy notices: An online study of the nutrition label approach', In Proceedings of the Conference on Human Factors in Computing Systems (CHI'10), ACM,1573-1582.

Lai, Y-L., and Hui, K-L. (2004) 'The Opt-in and Opt-Out debate: is it really necessary?' Available at: http://isr.uci.edu/pep06/papers/PEP06_LaiHui.pdf

Leon, P.G., Ur, B., Balebako, R., Cranor, L.F., Shay, R., Wang, Y. (2011), 'Why Johnny Can't Opt Out: A Usability Evaluation of Tools to Limit Online Behavioral Advertising.' In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 589-598.

MacDonald, A. and Cranor, L.F. (2008), 'The Cost of Reading Privacy Policies.' A Journal of Law and Policy for the Information Society, vol. 4, no. 3, 543-568.

Martin, K. (2015) 'Privacy Notices as Tabula Rasa – How Consumers Project Expectations on Privacy Notices.' Journal of Public Policy and Marketing, 34(2), 210-227.

Martin, K. & Shilton, K. (2016). 'Putting mobile application privacy in context: An empirical study of user privacy expectations for mobile devices.' The Information Society, 32:3, 200-216.

Mathur, A., Acar, G., Friedman, M.J., Lucherini, E., Mayer, J., Chetty, M., and Narayanan, A. (2019) 'Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites.' In Proceedings of the ACM on Human-Computer Interaction Volume 3, Issue CSCW, Article 81.

Matz, S., Kosinski,M., Nave,G., and Stillwell, D. (2017) 'Psychological targeting as an effective approach to digital mass persuasion'. In Proceedings of the National Academy of Sciences. Vol 114, 12714–12719. https://doi.org/10.1073/pnas.1710966114

Miller C. (2019) for Doteveryone. Engaging the public with Responsible Technology Engaging the public with responsible technology

Miller, C., Coldicutt, R., & Kitcher, H. (2018) for Doteveryone. People, Power and Technology: The 2018 Digital Understanding Report.

Miller, C., Kitcher, H., Perera, K. & Abiola, A., (2020) for Doteveryone. People, Power and Technology: The 2020 Digital Attitudes Report.

Norwegian Consumer Council (2018). 'Deceived by Design.

Norwegian Consumer Council (2018). Every Step You Take.

Obar, J. & Oeldorf-Hirsch, A. (2016). 'The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services.' Information, Communication and Society, doi: 10.1080/1369118X.2018.1486870

Ofcom (2019). Adults Media use and attitudes report 2019 – chart pack.

Ofcom (2019). Adults Media use and attitudes report 2019 – data tables.

Ofcom & Information Commissioner's Office (2019). Internet users' concerns about and experience of potential online harms.

Ofcom (2020). Internet users' experience of harm online.

Ofcom (2020). Online nation 2020 report

Open Data Institute (2018). Attitudes towards data sharing

Open Data Institute (2018). Attitude towards data sharing – Europe.

Oxford Internet Institute (2019). Perceived threats to privacy online: The internet in Britain.

Quinn, K. (2016) 'Why We Share: A Uses and Gratifications Approach to Privacy Regulation in Social Media Use.' Journal of Broadcasting & Electronic Media 60(1), 61–86.

Réjon-Guardia, F. (2014) 'A generalization of advertising avoidance model on social network.' Available at: https://pdfs.semanticscholar.org/f475/2034c7054f1ff3f3265120337ccd38985a87.pdf

Robinson, S.C. (2018).' Factors predicting attitudes towards disclosing personal data online.' Journal of Organizational Computing and Electronic Commerce, 28:3, 214-233.

Royal Statistical Society (2014). Royal Statistical Society research on trust in data and attitudes towards data use / data sharing.

Royal Statistical Society (2017). Data governance: public engagement review.

Roy Morgan – prepared for Australian Competition and Consumer Commission (2018). Consumer views and Behaviours on Digital Platforms.

Samat, S., and Acquisti, A. (2017) 'Format vs. Content: The Impact of Risk and Presentation on Disclosure Decisions', In Proceedings of the Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017).

Schaub, F., Balebako, R., Durity, A.L., Cranor, L.F. (2015). 'A design space for effective privacy notices', In Symposium on Usable Privacy and Security (SOUPS)

Schaub, F., Balebako, R, and Cranor, L.F. (2017) 'Designing Effective Privacy Notices and Controls', Journal of IEEE Internet Computing, Vol. 21, Issue 3, 70-77.

Shklovski, I., Mainwaring, S.D., Skúladóttir, H.H., and Borgthorsson, H. (2014). 'Leakiness and Creepiness in App Space: Perceptions of Privacy and Mobile App Use.' In Proceedings of the Conference on Human factors in Computing Systems, (CHI'14): https://doi.org/10.1145/2556288.2557421

Skatova. A., McDonald R.L., Ma, S., and Maple, C. (2019). 'Unpacking Privacy: Willingness to pay to protect personal data.' Working Paper. PsyArXiv available at https://psyarxiv.com/ahwe4

Škrinjarić, B., Budak, J. & Rajh, E. (2018). 'Perceived quality of privacy protection regulations and online privacy concern.'

Stigler Center (2019). Stigler Committee on Digital Platforms – Final Report. Market Structure and Antitrust Subcommittee.

Strandburg, K.J. (2013). 'Free Fall: the Online Market's Consumer Preference Disconnect.' University of Chicago Legal Forum 95; NYU School of Law, Public Law Research Paper No. 13-62; NYU Law and Economics Research Paper No. 13-34.

Stutzman, F., Gross, R., and Acquisti, A. (2012). 'Silent Listeners: The Evolution of Privacy and Disclosure on Facebook.' Journal of Privacy and Confidentiality, 4(2), 7-41.

Thaler, R.H., and Sunstein, C. (2008) Nudge: Improving Decisions About Health, Wealth and Happiness, Yale University Press, New Haven, CT.

Thaler, R. H., Sunstein, C. R., & Balz, J. P. (2014). Choice architecture. The Behavioral Foundations of Public Policy.

Traverse for Citizens Advice (2018). The future of the smart home: Current consumer attitudes towards smart home technology.

Tsai, J.Y., Kelley, P.G, Drielsma, P., Cranor, L.F., Hong, J., and Sadeh, N. (2009) 'Who's viewed you? The impact of feedback in a mobile location-sharing application.' In Proceedings of the Conference on Human Factors in Computing Systems (CHI'09). ACM, 2003-2012.

Tsai, J.Y., Egelman, S., Cranor, L.F., and Acquisti, A. (2011) 'The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study', Information Systems Research, Vol. 22, No. 2, 254-268.

Tucker, C. (2012). 'The Economics of Advertising and Privacy', *International Journal of Industrial Organisation,* 30, no.3, 326-329.

Tucker, C. (2013). 'Social Networks, Personalised Advertising and Privacy Controls.', *Journal of Marketing Research*, Vol. 51, No. 5, 546-562.

Turow, J. Feldman, L., Meltzer, K. (2005) 'Open to Exploitation: American Shoppers Online and Offline'. Annenberg Public Policy Centre.

Turow, J., Hoofnagle, C.J., Mulligan, D.K., Good, N., Grossklags, J. (2007). 'The Federal Trade Commission and Consumer Privacy in the Coming Decade', 3 ISJLP 723.

Ur, B., Kelley, P.G., Komanduri, S., Lee, J., Maass, M., Mazurek, M., Passaro, T., Shay, R., Vidas, T., Bauer, L., Christin, N., and Cranor, L.F. (2012) 'How does your password measure up? The effect of strength meters on password creation.', In Proceedings of the USENIX Security Symposium. USENIX Association, Berkeley, CA, 1-16.

Utz, C., Degeling, M., Fahl, S., Schaub, F., and Holz, T. (2019) '(Un)informed Consent: Studying GDPR Consent Notices in the Field.' In 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19), ACM, New York, NY, USA. https://doi.org/10.1145/3319535.3354212

Wang et al (2013): A Field Trial of Privacy Nudges for Facebook. Published in CHI 2014, Apr 26 – May 01 2014, Toronto, ON, Canada.

Wellcome Trust (2016). Wellcome trust monitor report.

Which? (2018). Control, Alt or Delete? Consumer research on attitudes to data collection and use.

Which? (2019). Data dozen segmentation update

Which? (2020). Are you following me? Consumer attitudes towards data collection methods for targeted advertising.

Whitley, E. & Pujadas, R. (2018), 'Report on a study of how consumers currently consent to share their financial data with a third party.'

WIK-Consult (2015) 'Personal data and privacy. A report for Ofcom.'

Winegar, A.G. & Sunstein, C.R., (2019). 'How much is data privacy worth? A preliminary investigation.' Forthcoming, Journal of Consumer Policy. Available at SSRN: https://ssrn.com/abstract=3413277 or http://dx.doi.org/10.2139/ssrn.3413277

Wu, Y., Gupta, P., Wei, M., Acar, Y., Fahl, S & Ur, B. (2018). Your secrets are safe: how browsers' explanations impact misconceptions about private browsing mode.

Xu, H., Teo, H. H., Tan, B. C., & Agarwal, R. (2012). Research note. Effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: A study of location-based services. *Information Systems Research,* 23(4), 1342-1363.

YouGov for IAB UK (2019). Ad blocking: Consumer usage and attitudes.

Zafeiropoulou, A.M., Millard, D.E., Webber, C., and O'Hara, K. (2013) 'Unpicking the privacy paradox: can structuration theory help to explain location-based privacy decisions? ACM Web Science, Paris, France. http://dx.doi.org/10.1145/2464464.2464503