

# Active Online Choices: Designing to Empower Users

---

Summary of desk research, November 2020

## Contents

<b>Contents</b>	<b>1</b>
<b>Executive Summary</b>	<b>2</b>
<b>2. Primary research</b>	<b>4</b>
2.1 Findings	6
Barriers to early stages of engagement with choices	6
Barriers to deeper engagement with online choices	7
Who is doing things well?	8
2.2 Emerging themes	10
<b>3. Secondary research</b>	<b>11</b>
3.1 People's concerns and feelings of disempowerment	12
3.2 Factors affecting people's behaviour	16
3.3 Designing to help active choice	21
Factors that support information disclosure	23
Factors that support people to express choice	26

# Executive Summary

People cannot currently shape their online environments in line with their own preferences. The *Active Online Choices: Designing to Empower Users* project commissioned by the Centre for Data Ethics and Innovation and conducted by the Behavioural Insights Team and Doteveryone is exploring how to change that.

Our approach combines primary and secondary research to explore the roots of the problem, using prototyping and testing to demonstrate that alternatives to the status quo are possible. This report describes the project's research phase and accompanies the Update Report<sup>1</sup> which summarises all the work undertaken so far.

In our research, we used primary and secondary methods to surface and better understand potential barriers to giving people effective choices online and to inform the prototype development. We were interested in a wide range of choices under the loose (and overlapping) headings of privacy, by which we mean choosing what information to share and with whom, and personalisation, meaning any aspect of the user experience which can be tailored to an individual's needs or interests. Together, these choices range from consent to data use, cookies, location sharing or targeted advertising, through to control over content curated for users in recommendations, social media feeds, or other data-driven content curation.

Throughout the project, we are interested in *where* and *why* people may (or may not) currently exercise active choices in these areas, without assuming that more or less privacy or personalisation is necessarily, in itself, a cause for concern.

In our primary research, where we looked first-hand at the presentation and consequences of choices on a wide variety of digital services, we found:

- Barriers at early stages of engagement with choices, which include a high prevalence of defaults in the businesses' interest,<sup>2</sup> challenges in finding the right place to make choices, and poor timing of prompts to engage.
- Barriers to deeper engagement with online choices, which include a lack of transparency and explanation over the business purpose of data collection and use, unhelpful segregation of settings, and poor explanation of the trade-offs inherent in choices.

In our secondary desk research, we synthesised published research on people's concerns regarding online choices and control, the factors causing people's choices to diverge from

---

<sup>1</sup> Behavioural Insights Team (2020). [Active Online Choices: Designing to Empower Users](#).

<sup>2</sup> Competition and Markets Authority (2020). [Online platforms and digital advertising market study final report](#).

their preferences, and how we can design websites, applications, and their interfaces to support active choice.

Our review of the evidence found that, when asked, people want more control over their online experience in areas such as data collection and use, online targeting (the use of data to target content online), and the role of algorithms in curating content feeds and recommendations.

We also found that people generally have low levels of understanding, and that companies have often failed to effectively explain important (albeit complex) concepts to them. These factors are likely to be major limitations to making active choices. A range of behavioural factors - such as tendencies to stick with a default choice selection and prioritise short term gratification - are also driving people's choices away from their stated preferences.

Finally we identify a number of design principles that can support people to make active choices. These relate to the timing, clarity and ease of navigating information, as well as the use of defaults, suitable granularity of choices, use of visuals to present trade-offs when presenting a choice and the inclusion of feedback of the impact of a given choice.

In the course of this work we came to a working definition of active choices which has provided a focus for the project:

***'Active' choices are made when people are empowered and able to reflect their wishes without obstruction, based on an understanding of the consequences.***

## 2. Primary research

Our primary research aimed to understand first hand what aspects of companies existing choice architecture were likely to act as barriers to consumers exercising active choice.

Given the wide scope we prioritised:

- The most used services in the UK, e.g. by user base, or total or average time spent on service.
- The aspects of choice people are most concerned about (as explored in the [first question](#) of our secondary desk research).
- Where people currently feel least empowered and able to make active choices.

We noted the available choices and consequences of these choices, and whether the presentation of choices was easy to find, clearly explained and/or presented the trade-offs inherent in the choice.

Our approach was similar to the Competition & Markets Authority (CMA) review of consumer control over data collection on different online services, conducted as part of the market study into online platforms and digital advertising.<sup>3</sup> Our primary research considered a broader range of services than the CMA but in less depth (for example, we also looked at voice assistants, privacy pop-ups and browser extensions).

---

<sup>3</sup> Competition and Markets Authority (2020). [Online platforms and digital advertising market study](#). See in particular: [Appendix K Consumer control over data collection](#).

**Table 2: Summary of user contexts considered in the primary desk research, and the user choices reviewed**

User contexts considered		Example user choices reviewed
Account management on online services	<ul style="list-style-type: none"> <li>● Google</li> <li>● YouTube</li> <li>● Facebook</li> <li>● Instagram</li> <li>● Whatsapp</li> <li>● Twitter</li> <li>● Snapchat</li> <li>● Amazon</li> <li>● Ebay</li> <li>● Ocado</li> <li>● Spotify</li> <li>● Compare the Market</li> </ul>	<ul style="list-style-type: none"> <li>● Extent of personal information to share</li> <li>● Who information is shared with (e.g. friends, advertisers)</li> <li>● Ability to share status (e.g. 'last seen' on Whatsapp)</li> <li>● Ability for others to search for you via phone number etc.</li> <li>● Marketing and notifications settings</li> </ul>
Browsers	<ul style="list-style-type: none"> <li>● Firefox</li> <li>● Chrome</li> <li>● Safari</li> <li>● Brave</li> </ul>	<ul style="list-style-type: none"> <li>● Privacy preferences chosen for some (e.g. strict, standard or custom)</li> <li>● Enable/disable cross-site tracking</li> <li>● Block or delete cookies</li> </ul>
Ordering of content and search results	<ul style="list-style-type: none"> <li>● Twitter</li> <li>● Facebook</li> <li>● Instagram</li> <li>● uSwitch</li> </ul>	<ul style="list-style-type: none"> <li>● Ordering of feeds and timelines</li> <li>● Presentation of product search results</li> </ul>
Device set-up	<ul style="list-style-type: none"> <li>● iOS</li> <li>● Android</li> </ul>	<ul style="list-style-type: none"> <li>● Connect with linked devices (e.g. Google Assistant, Siri)</li> <li>● Data transfer from another device</li> <li>● Automatic updates</li> <li>● Location sharing</li> </ul>
Voice assistants	<ul style="list-style-type: none"> <li>● Siri</li> <li>● Alexa / Amazon Echo</li> </ul>	<ul style="list-style-type: none"> <li>● Choose whether to allow employees to listen to recordings (default off)</li> <li>● Acceptance of all general privacy terms</li> </ul>
Privacy tools, pop-ups and controls	<ul style="list-style-type: none"> <li>● Privacy manager pop-ups on websites</li> <li>● DuckDuckGo</li> </ul>	<ul style="list-style-type: none"> <li>● Enable/disable various data sharing purposes and sharing with vendors</li> <li>● Personalise to region-specific results</li> </ul>
Video calling/conferencing apps	<ul style="list-style-type: none"> <li>● Facetime</li> <li>● Google Meet</li> <li>● Zoom</li> </ul>	<ul style="list-style-type: none"> <li>● Recording and taking screenshots of video calls</li> <li>● How people's contact details are used</li> </ul>

## 2.1 Findings

We paid particular attention to the features that behavioural science literature finds to have disproportionate impact on people's choices, such as defaults and friction costs.

Barriers to active choice are generally experienced in two ways: firstly, in the early stages of engagement with a potential choice (e.g. in finding the relevant screen); and secondly, in engaging more deeply with the information around that choice (e.g. in being able to weigh up the decision). We also found examples of companies that were providing good choice environments for their users, though these also had limitations.

### Barriers to early stages of engagement with choices

#### High prevalence of defaults in the businesses' interest

Across nearly all services reviewed, we found that people are confronted with defaults were set in favour of greater data use when users may prefer the default to be more limited data use.<sup>4</sup> For example, live streams are public by default on some social networks<sup>5</sup> and autoplay is the default on most video streaming services. People receive personalised advertising by default on Google Search and Bing.<sup>6</sup> By definition, defaults, as opposed to forced choice presentation formats, decrease the likelihood that people engage with the choice.<sup>7</sup>

#### Finding the right place to make choices

Even if people wish to express their preferences by reviewing their settings, finding the right place to do so can be a hindrance. Instagram's privacy settings are particularly challenging, with people being directed to their Facebook accounts to manage them. In other cases, the privacy settings section is only accessible after multiple clicks through submenus. Twitter users, for example, find privacy settings in the 'More' submenu.

Among videoconferencing services, there were distinct differences in the level of choice afforded to new users as part of the registration process, with some companies allowing users to set preferences only after having completed registration. The selection of some (but not other) options for users to integrate into the sign-up flow may imply to users that these are of greatest importance. And the most prominently displayed options may not correlate to users' concerns.

We also found positive examples of the same choice being accessible through multiple routes. For instance, Facebook users can change their newsfeed preferences within the general 'Settings' menu as well as in the 'Your time on Facebook' overview. Google and

---

<sup>4</sup> Competition and Markets Authority (2020). [Appendix K Consumer control over data collection](#).

<sup>5</sup> Also reported in 5Rights Foundation (2020). [Risky-by-Design. Case Study: Livestreaming](#).

<sup>6</sup> There is no way to opt out at all on Facebook products.

<sup>7</sup> See, for example: [The Failure of Online Social Network Privacy Settings](#) and [Is Facebook Killing Privacy Softly? The Impact of Facebook's Default Privacy Settings on Online Privacy](#).

Spotify provide easy access to their settings for privacy and personalisation, including a clear description of choices.

### **One-off engagement at sign-up and poor timing of prompts**

While platforms and websites tend to emphasise at sign-up that choices can be changed at a later stage, people are unlikely to return to a comprehensive review of their settings. Emphasising the option to review later may foster procrastination.

Prompts to re-engage with settings often, where they are used, appear when opening a website or signing in - in other words, at a moment when the user is keen to access the service, e.g. checking messages on Facebook. The short-term goal of using the service is likely to override engagement with the prompt to review settings. Google helpfully presents newly-registering users with a choice to be actively reminded and prompted at regular intervals to review privacy settings. Testing is needed to identify when prompts are most likely to trigger engagement, given the status quo generally appears suboptimal for enabling active choices.

## **Barriers to deeper engagement with online choices**

### **Lack of explanation of the business purpose of data collection and personalisation**

In many cases, the purpose of data collection is framed around “making advertisements more relevant” to the user and enhancing user experience. It gives little insight into how the user’s data is processed and/or shared with third parties to make this happen. We observed that accessing such information, if available, requires effort (i.e. many clicks) to locate it. For example, Facebook has a section about “Why you see a particular ad” that is located along the following path: “Settings” > “Ads” > “Ad Preferences” > “How Facebook ads work” > “Why you see a particular ad”.

We did not find services in our review that provide illustrative explanations about the implications that various settings may have. In many cases, this may be due in part to the ‘black box’ nature of outcomes determined by algorithms and other complex systems. Businesses may find it difficult to explain the specifics of how and why users see, for example, a particular advert or piece of content. However it might be possible to offer more information on the inputs to these processes. For example, users could be given the list of criteria that an advertiser was using to target an advert.

### **The flow of user data is rarely visible**

Companies often provide little support for people who want to understand how data about them is collected, used and shared ahead of making choices. For example, looking at Twitter’s help pages, the explanation of the data used to determine the order of the timeline states that it is based on account interactions, tweet engagements and “much more”.<sup>8</sup>

### **Privacy settings focus on what is shared with other users rather than with the platform or third parties**

---

<sup>8</sup> <https://help.twitter.com/en/using-twitter/twitter-timeline>

This barrier mainly refers to social media platforms. For example, Facebook’s section on “Privacy” lets people choose who can see their posts or interact with them. In contrast, information about the sharing of data between Facebook and third parties sits under “Your Facebook information” and “Security”, fragmenting the process of reviewing settings. This does not offer a logical choice for the user. We would assume that a user looking to limit the sharing of data about them is most likely to begin in the section labeled “Privacy” but none of the choices available within these settings will affect what information they share with the platform itself.

### Trade-offs inherent in choices are poorly explained

Some user choices directly or indirectly affect the functionality of the services used, for example when restricting cookies in browsers. Our review of Safari and Firefox revealed that both platforms inform users that changing this setting may “break sites”, without offering a more detailed explanation of how this can affect site functionality in practice.

### Who is doing things well?

As well as the barriers above, our research also identified some promising approaches. The first example, Google Privacy Check-up helps to make choices accessible. The second, the DuckDuckGo privacy extension, demonstrates how intermediaries can helpfully make decisions that cut across siloed app settings.

#### Example 1: The Google privacy check-up

The Google privacy check-up allows users to review settings around personalisation and data sharing with others. This includes settings on tracking web and app activity, location history and YouTube history as well as controls for the personal information that is shared with others (name, picture, gender, birthday) and choices over advert personalisation.

#### Positive features:

- Simple language that aids understanding of the consequences of each choice.
- Statements are framed around desired outcomes.
- A relatively comprehensive review of important settings (i.e. there are few places left out that a user could go to to change settings) broken down into simple steps.


#### Limitations:

- Defaults for important choices, such as having ad personalisation on by default, and framing of choices to emphasise the side in Google’s interests, e.g. “Make ads more relevant to you”.




#### Privacy Check-up

Review key settings and the data that Google uses to personalise your experience

 Activity controls reviewed	▼
Help people connect with you	▼
Control what others see about you	▼
Make ads more relevant to you	▼

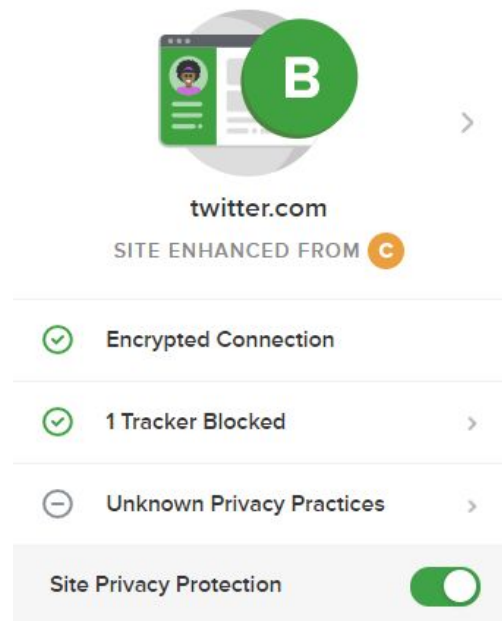


- People may not notice the small pop-up icons under each category that allow people to fine-tune choices (they look like this:  )

However, in spite of the positive features outlined above, it is worth noting that Google data reported to the CMA showed that less than five percent of people engaged with Privacy Check-up over a 28 day period in February and March 2020.<sup>9</sup> This highlights the challenge of engaging users to take active choices. The location of the button to start the check-up, and/or timing of reminders, may be limiting the number of users who begin the process.

### Example 2: DuckDuckGo browser extension

DuckDuckGo offers a browser extension<sup>10</sup> that blocks tracking and enables users to search the internet without storage of their search history or any personal information. Users can see standardised privacy ratings for websites as well as the trackers blocked by the extension.



### Positive features:

- Simple, consistent, at-a-glance privacy rating for websites, to help inform people about website policies rather than having to digest the full privacy policy.
- Allows people to opt in or out of tracking as a rule, without having to change settings on every website visited.

### Limitations:

- Extension might apply restrictions that go beyond people's true preference (e.g. no customisation of search results to always take account of variables such as the country of search).
- Low prevalence: Browser extensions are not a very popular choice among internet users.

<sup>9</sup> Competition and Markets Authority (2020). [Online platforms and digital advertising market study final report](#). Paragraph 4.98, page 175.

<sup>10</sup> <https://duckduckgo.com/app>

## 2.2 Emerging themes

Overall, our primary research suggests that people rarely encounter online environments that encourage and enable them to carefully consider the advantages and disadvantages of their settings and make nuanced choices accordingly.

The research revealed a number of barriers to active choice for users of online services. Specifically, people lack:

- Useful guidance through choice settings including an architecture that is intuitive to navigate and presents practical, relatable information at the moment of choice;
- Balanced and accessible presentation of trade-offs allowing people to understand the consequences of their choices.
- Prompts at convenient moments, when they are likely to have the time and motivation to engage, and opportunities for ongoing engagement.
- The opportunity to make proactive and forced choices over important features, such as the data shared with a platform, when these choices are subject to defaults and hidden out of sight.
- Plain English to explain the inherent trade-offs in certain choices, such as personalised advertising, as well as a lack of transparency over why defaults are set the way they are.

These barriers offered a range of useful challenges to address when developing prototypes.

### 3. Secondary research

Our secondary research draws on academic literature, policy reports from the public sector, and consumer research to address three questions:

1. **People's concerns and feelings of disempowerment:** Where are people's concerns greatest and where do people feel least able to exercise choice?
2. **Factors affecting people's behaviour:** Where and why do online choices appear to be different from stated preferences?
3. **Designing to help active choice:** What forms of disclosure and interfaces help people to make active choices online?

**As a general reflection, we found that online consumer choice research tends to focus on what people don't want rather than what they do want. In addition, there are discrepancies between what people say they want in one context versus what they say or do in another context.** There are many possible reasons for this. It may be driven by practical factors such as the interests of researchers, the influence of the media climate of the day, or that, in the context of consumer research, it may be easier to point to issues rather than generate workable solutions.

There are also somewhat contradictory findings across the consumer research. For example, 65% of people in a Data and Marketing Association (DMA) study<sup>11</sup> do not feel they have control over the information that companies collect, while three quarters of respondents to an Ofcom study<sup>12</sup> feel confident that they are in control of who has access to their data online. While we do not go into detail as to why these differences emerge, we acknowledge that there are many factors at play, such as question framing, social desirability bias,<sup>13</sup> unclear and inconsistent definitions of complex terms, and varied understanding of issues among respondents.<sup>14</sup>

---

<sup>11</sup> Data and Marketing Association (DMA) (2018). Data privacy: [What the consumer really thinks](#).

<sup>12</sup> Ofcom (2019). [Adults' Media Use and Attitudes Report 2019](#).

<sup>13</sup> Where people tend to give answers to survey questions that they think will be seen favourably by others.

<sup>14</sup> Ipsos Mori & Carnegie Trust UK (2018). [Online Data Privacy from Attitudes to Action: an evidence review](#).

## 3.1 People's concerns and feelings of disempowerment

Where are people's concerns greatest and where do people feel least able to exercise choice?

### Key points:

- Key areas of concern reported are privacy, the use of data to shape the content people see online (online targeting), the use of cookies, third-party data sharing, and particular app permissions.
- The level of concern can vary greatly depending on context - for example, 80% of people trust the NHS to use online targeting responsibly, but only 28% feel the same for social media companies.
- Knowledge of how personal data is collected and used is low, and the more people know about topics such as privacy and online targeting, the more concerned they tend to be. Studies that made people more knowledgeable found that this increased participants' concerns.
- While many people appreciate the benefits gained through the use of data about them online (such as with online targeting), consumers are worried about online choice issues and want more control over them.
- Some groups are more concerned than others - in particular, there is an age gap, with older people expressing greater concerns and feeling less able to manage access to their data.

To prioritise areas of focus for the project, we are interested in the areas where people feel most concerned and/or least in control. This section is separated into evidence on these two aspects: concerns and control.

### People are concerned about a variety of aspects of data collection and use

**In general, the research on people's attitudes to data collection and use finds that knowledge about how data is collected and used is low, and the more people learn about these things the more concerned they become.** People tend to desire a greater degree of transparency, accountability and autonomy regarding their data and how it is used.

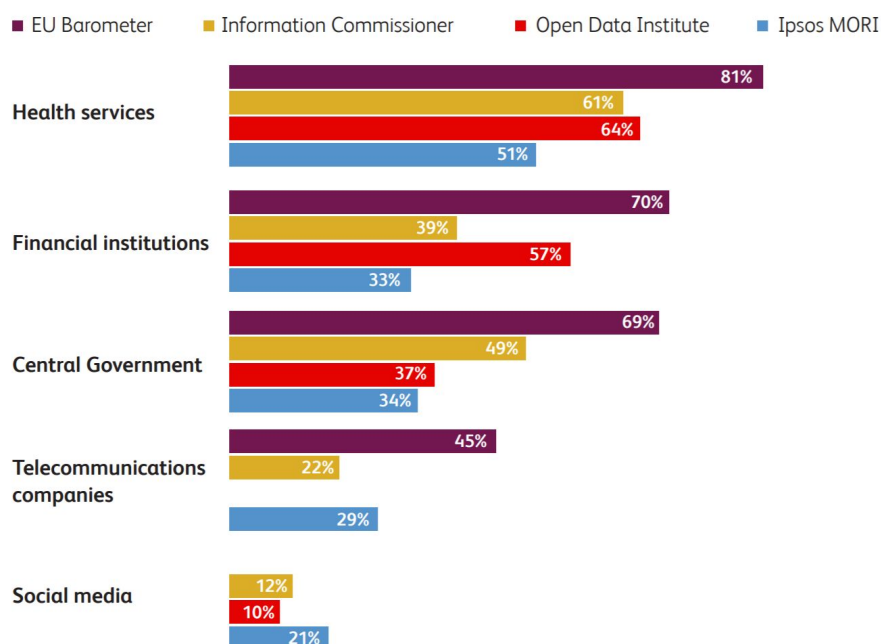
Some platforms and companies are trusted considerably more than others when it comes to collecting and using personal data, meaning that people's concerns vary by context. A 2018 Ipsos Mori review of four different surveys identified social media companies as the least trusted; financial services companies and governments as being more trusted; and healthcare providers as by far the most trusted.<sup>15</sup> This is in line with recent CDEI work finding

---

<sup>15</sup> Ipsos Mori & Carnegie Trust UK (2018). [Online Data Privacy from Attitudes to Action: an evidence review](#).

that only 28% of the public trust social media companies to use online targeting responsibly, compared to 80% for the NHS.<sup>16</sup>

**Figure 1: Public trust in organisations accessing their personal data (2018)**



Source: Ipsos Mori & Carnegie Trust UK (2018). *Online Data Privacy from Attitudes to Action: an evidence review*.

The main areas of concern across the multitude of surveys and studies we reviewed are:

- 1. Privacy and online data collection.** Surveys consistently find people are worried about whether and how information about them is shared online.<sup>17</sup> Those over 55 are much more likely to be concerned about online privacy than those aged 18-24.<sup>18</sup> Older individuals are also much less likely to feel confident in managing access to their personal data online.<sup>19</sup>
- 2. Online targeting.** The proportion of people concerned with this varies. CDEI research found 54% of respondents finding the personalisation of online adverts acceptable, while 11% of people surveyed by the Open Data Institute agreed that they would be happy to share data in exchange for tailored content.<sup>20 21</sup> While people do not want online targeting to be stopped, and people value the convenience it offers, they want a greater degree of transparency and autonomy in how these systems operate.<sup>22</sup>

<sup>16</sup> Centre for Data Ethics and Innovation (2020). [Attitudes to Online Targeting: Public Engagement Research \[Research data\]](#). Table 31.

<sup>17</sup> Ibid.

<sup>18</sup> Data and Marketing Association (DMA) (2018). [Data privacy: What the consumer really thinks](#).

<sup>19</sup> Ofcom (2019). [Adults' Media Use and Attitudes Report 2019](#).

<sup>20</sup> Centre for Data Ethics and Innovation (2020). [Online targeting: Final report and recommendations](#).

<sup>21</sup> Open Data Institute (2018). [Attitudes to data sharing](#). See full dataset LSD Q4. "I would share data about me if it were used to tailor the media content I view and listen to, even if I need to share information about my likes and dislikes."

<sup>22</sup> Ibid.

3. **Cookies.** When provided with more information about cookies, people were more likely to express hostility towards them.<sup>23</sup> In one study, after being taught about cookies, 37% of participants were not willing to accept any cookies and a further 35% would be willing to accept first-party cookies only.<sup>24</sup>
4. **Third-party data sharing.** As with many of the other areas, the more people understand about the data sharing ecosystem the more concerned they become.<sup>25</sup> People do not want - or need - to understand the data ecosystem, but they do want to understand meaningful outcomes of such sharing, such as why their insurance quote has changed or why they see certain product recommendations.<sup>26</sup>
5. **Wide-ranging app permissions.** People assess the acceptability of tablet and smartphone app permission requests by considering the purpose of the app, the kind of permissions requested and who is asking for them.<sup>27</sup> Location data, calendar access and internet access were identified as relatively uncontroversial, whereas apps requesting access to messages, contacts and photos were seen as more suspicious.<sup>28</sup>

### People desire increased control over a number of aspects of their online experience

**People have a combination of tools available to control their online experience, such as the settings on their devices, browsers, and social media platforms, and search engines. Across these contexts, people want greater transparency and enhanced control.** This includes transparency and control over:

1. **Data collected and shared about them.** The 2020 People, Power and Technology report by Doteveryone found that 89% of the UK public felt it was important to “choose how much data they share with companies”.<sup>29</sup> A majority of people say that they would be willing to pay more for services to protect their privacy (although whether they will in practice is a mixed picture, as discussed in the next section).<sup>30</sup> People increasingly feel that they do not have control over their personal data online. Figure 2 below, illustrates this growing perception of a lack of control.<sup>31</sup>
2. **Data used to shape their online experience (online targeting).** CDEI research found that while 68% of respondents agreed that they knew how to change their online settings and preferences, just 36% felt that they had meaningful control over the way that content was recommended and personalised to them.<sup>32</sup>

<sup>23</sup> Marreiros, H., Gomer, R., Vlassopoulos, M., Tonin, M. & Schraefel, M. (2015). Exploring user perceptions of online privacy disclosures.

<sup>24</sup> Smit, E. et. al (2014). Understanding online behavioural advertising: User knowledge, privacy concerns and online coping behaviour in Europe. *Computers in Human Behavior*, 32, 15-22.

<sup>25</sup> Which? (2018). [Control, Alt or Delete? The Future of Consumer Data](#).

<sup>26</sup> Ibid.

<sup>27</sup> Marreiros, H., Gomer, R., Vlassopoulos, M., Tonin, M. & Schraefel, M. (2015). Exploring user perceptions of online privacy disclosures.

<sup>28</sup> Ibid.

<sup>29</sup> Doteveryone (2020). [People, Power and Technology: The 2020 Digital Attitudes Report](#).

<sup>30</sup> Ibid.

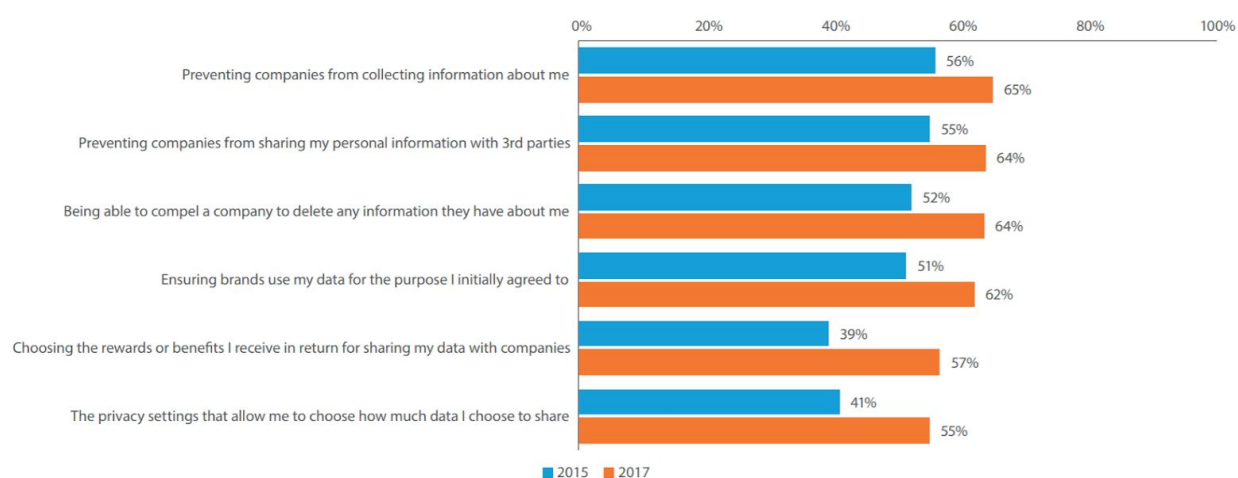
<sup>31</sup> Data and Marketing Association (DMA) (2018). [Data privacy: What the consumer really thinks](#).

<sup>32</sup> Centre for Data Ethics and Innovation (2020). [Attitudes to Online Targeting: Public Engagement Research \[Research data\]](#), Table 65.

3. **Content curated or recommended for them.** For example, the majority of social network users do not understand the factors that drive their news feed.<sup>33</sup> CDEI research found that just 43% of respondents agreed that websites provide settings and preferences to change how what they see online is recommended and personalised to them.<sup>34</sup>

**Figure 2: Perceptions of control over personal data sharing, 2015-2017**

“How much control do you think you have over the following? Please use the scale from 1 to 10 where 1 is ‘I don’t feel I have any control at all’ and 10 is ‘I feel that I have complete control’” | % who feel they are not in control of this (1-4)



Source: Data and Marketing Association (DMA) 2018). *Data privacy: What the consumer really thinks*. Sample size of 1,047.

<sup>33</sup> Pew Research Center. (2018). [Many Facebook users don't understand how the site's news feed works](#).

<sup>34</sup> Centre for Data Ethics and Innovation (2020). [Attitudes to Online Targeting: Public Engagement Research \[Research data\]](#), Table 65.

## 3.2 Factors affecting people's behaviour

### Where and why do online choices appear to be different from stated preferences?

#### Key points:

- People's behaviour can differ from their reported preferences, especially when in-the-moment decisions are automatic rather than deliberative.
- The 'privacy paradox' is one clear example of a mismatch between views and behaviours.
- People's understanding and the failure of companies to effectively explain concepts are likely to be major limitations to effective choice.
- People currently find it hard to engage with information contained in contractual terms, even when they try.
- A range of behavioural factors - such as a tendency to stick with the default selection - are further affecting people's choices.

One measure of how well online environments enable effective decision-making is how well choices match people's preferences.

Researchers have been exploring for decades when, how and why our stated preferences and views differ from our actual choices and actions. One of the most common approaches to human decision-making describes two systems: System 1 and System 2.<sup>35</sup> System 1 operates automatically and quickly and relies on mental shortcuts. The vast majority of day-to-day decisions are made using this system (e.g. when taking a familiar commute to work). System 2 is slower and more deliberate, allowing us to weigh up costs and benefits (e.g. when planning a journey to a foreign country). We rely on System 1 much more than we realise, even in situations that ostensibly demand careful consideration, and this means relying on mental shortcuts and being susceptible to small changes in context that affect decisions in the moment. This affects how we engage with privacy and personalisation choices and can lead to patterns such as the 'intention-action gap', where although we may intend to do something in our best interests (e.g. regularly review our data sharing settings) we don't always follow through.<sup>36</sup> The 'privacy paradox' described below is one clear example of a mismatch between online preferences and behaviours.

This section goes on to outline the evidence of where and why intentions and actions diverge in online user behaviours, and identifies some of the main barriers to people being able to act in line with their preferences. These include:

---

<sup>35</sup> Kahneman, D. (2011). *Thinking, fast and slow*. Macmillan.

<sup>36</sup> Rhodes, R. & De Bruijn, G-J. (2013). How big is the physical activity intention-behaviour gap? A meta-analysis using the action control framework. *British Journal of Health Psychology*, 18(2), 296-309.



- **Limited understandings of how data is used and processed.** People don't tend to know what information is held about them and underestimate the volume that is collected.<sup>37</sup>
- **Difficulty engaging with contractual terms.** Most people do not read or understand privacy notices or terms and conditions. This is concerning, as an understanding of the basic trade-offs is essential to be able to weigh up options.
- **Limited feedback on choices they make.** While feedback is important for people to understand the consequences of their choices and improve the choices they make, privacy and personalisation choices online do not always provide it.

### The 'privacy paradox'

It is often stated that people's stated level of privacy concern has very low or no correlation with their actual privacy behaviours.<sup>38</sup> This inconsistency between how people report the importance of privacy and how they act to protect their privacy is often called the 'privacy paradox'.<sup>39</sup> This paradox is well-illustrated by an online shopping experiment where participants were willing to disclose sensitive information such as their income level to a shop, rather than pay 1 Euro more to purchase from another shop without such a disclosure requirement. At the same time, 95% of participants said that they were interested in protecting their personal information.<sup>40</sup>

### Limited understanding impairs effective choice

The general public seem to have at best a basic understanding of a number of integral processes affecting their online experience. This includes aspects such as data collection and use, online targeting, how online businesses make money, and the role of algorithms.<sup>41</sup><sup>42</sup><sup>43</sup> For example, the majority of social network users do not understand the factors that drive their news feed.<sup>44</sup> Creators on YouTube know little about how the site's recommendation system works.<sup>45</sup> More generally, users are not sure what information is held about them, and are likely to underestimate the volume of information that is collected.<sup>46</sup> People also underestimate the extent that their information can be combined and shared with

<sup>37</sup> Ipsos MORI. (2016). Digital footprints: Consumer concerns about privacy and security.

<sup>38</sup> For example in a meta-analysis of online privacy studies conducted by Baruh, L. et al. (2017). Online Privacy Concerns and Privacy Management: A Meta-Analytical Review. *Journal of Communication* 67 (2017) 26–53.

<sup>39</sup> Kokolakis, Spyros. (2015). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*.

<sup>40</sup> Beresford, A. R., Kübler, D., and Preibusch, S. (2012), Unwillingness to pay for privacy: A field experiment. *Economics Letters*, 117(1), 25-27.

<sup>41</sup> Doteveryone (2020). [People, Power and Technology: The 2020 Digital Attitudes Report](#).

<sup>42</sup> Which? (2018). [Control, Alt or Delete? The Future of Consumer Data](#).

<sup>43</sup> Centre for Data Ethics and Innovation. (2020). [Review of online targeting. Attitudes to Online Targeting: Public Engagement Research](#).

<sup>44</sup> Pew Research Center. (2018). [Many Facebook users don't understand how the site's news feed works](#).

<sup>45</sup> [We don't understand how YouTube's algorithm works—and that's a problem](#).

<sup>46</sup> Ipsos MORI. (2016). Digital footprints: Consumer concerns about privacy and security.

other parties.<sup>47</sup> Some knowledge gaps around data use may be shrinking, but many remain.<sup>48</sup>

49

### People find it hard to engage with contractual terms, even when they try

A large driver of the low levels of understanding is limited engagement with privacy policies and terms and conditions (Ts&Cs). Self-report data finds that just 15% of people report that they read the Ts&Cs for digital services “most or all of the time”,<sup>50</sup> and the amount and quality of engagement is lower still in practice.<sup>51</sup> People say this is because of the length and complexity, as well as a perceived lack of control over the outcome as companies may still do what they want with data (suggesting a degree of ‘fatalism’ about online choices).<sup>52</sup> Even where people do engage fully with an online service’s Ts&Cs, if they want to use the service they often have to accept the terms in full to do so.<sup>53</sup>

There is a lack of transparency by service providers and these gaps are likely to continue given limited incentives for companies to educate their users or differentiate themselves on privacy grounds.<sup>54</sup> Currently, a quarter of users do not understand messages on targeting of ad preference when they do read them.<sup>55</sup> These outcomes may, in part, be due to a lack of visual explainers or the option for people to test/preview the outcome of a choice (which the following section on disclosure suggests could be helpful).

The resulting knowledge gaps - both underlying and at the point of engaging with a given firm - make it hard, if not impossible, to make informed decisions. An understanding of the basic trade-offs is essential to be able to weigh up options. More generally, we suspect that having a limited understanding of underlying data processes reduces people’s feelings of control, and also their willingness and ability to meaningfully engage with choices.

### People lack prompt feedback on the effect of their choices

Prompt feedback, whereby people see how a choice they have made has changed their online experience, is an important factor in decision making.<sup>56</sup> It is often difficult for people to understand the consequences of changing settings such as privacy controls, as it is not

---

<sup>47</sup> Which? (2018). [Control, Alt or Delete? The Future of Consumer Data](#).

<sup>48</sup> Information Commissioner’s Office. (2019). [Information Rights Strategic Plan: Trust and Confidence](#).

<sup>49</sup> Doteveryone (2020). [People, Power and Technology: The 2020 Digital Attitudes Report](#).

<sup>50</sup> Ibid

<sup>51</sup> Obar, J. A., & Oeldorf-Hirsch, A. (2018). The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services.

<sup>52</sup> Doteveryone (2020). [People, Power and Technology: The 2020 Digital Attitudes Report](#).

European Commission. (2015). [Special Eurobarometer 431: Data Protection report](#).

<sup>53</sup> Which? (2018). [Control, Alt or Delete? The future of consumer data](#).

<sup>54</sup> Stigler Center (2019). [Stigler Center committee on digital platforms – Market structure and antitrust subcommittee](#).

<sup>55</sup> Harris Interactive (2019). [Adtech – Market research report](#).

<sup>56</sup> Thaler, R. H., Sunstein, C. R., & Balz, J. P. (2013). Choice architecture. The behavioral foundations of public policy, 428-439. Thaler, R. H., & Sunstein, C. R. (2009). Nudge: Improving decisions about health, wealth, and happiness. Penguin.

always clear how the online world works.<sup>57</sup> This lack of feedback makes it harder for people to learn from experience and create an environment that aligns with their true preferences.

### **Behavioural factors interact with and exacerbate the challenges above**

A systematic review of theories explaining the privacy paradox finds that privacy decision making is not exclusively driven by rational cost-benefit assessments.<sup>58</sup> The following behavioural factors may also contribute to the issue and help explain the privacy paradox. We suspect that many of these factors are likely to be equally relevant to user choices regarding other aspects of their online experience. Some barriers - such as present bias and the intention-action gap - may currently be exacerbated by particular design choices, such as inconvenient timing of pop-ups/prompts to engage.

---

<sup>57</sup> Which? (2018). [Control, Alt or Delete? The Future of Consumer Data](#).

<sup>58</sup> Barth, S., & De Jong, M. D. (2017). The privacy paradox—Investigating discrepancies between expressed privacy concerns and actual online behavior—A systematic literature review. *Telematics and informatics*, 34(7), 1038-1058.

**Table 4: Selection of behaviours factors affecting choice in online environments**

Behavioural factor	Research finding
<p><b>Status quo bias.</b> People are more likely to stick to the defaults, such as those in privacy settings. These are typically set to share lots of information with providers.</p>	<p>Less than 5% of people who joined Facebook in February 2020 engaged with ad preferences or privacy controls within 30 days of registering.<sup>59</sup> When creating a Google account, less than 5% of people change settings that enable location history.<sup>60</sup> Self-report data on how many people adjust their privacy settings varies. Some surveys suggest that 31% of British internet users have adjusted their social media privacy settings from the defaults.<sup>61</sup> Other reports suggest higher figures for particular platforms, such as Facebook (67%) and Instagram (66%).<sup>62</sup></p>
<p><b>Framing.</b> Platforms may highlight the benefits of consenting to sharing data, while not adequately presenting the implications or drawbacks.</p>	<p>For example, tools such as cookies are often framed in purely technical language (e.g. “We use technologies like cookies, pixels, and local storage to provide and understand a range of products and services”), without definitions, so that it’s difficult for people to understand what they are and how they are used in practice.<sup>63</sup></p>
<p><b>Overconfidence.</b> People may be overconfident and over-optimistic about their ability to protect their own information.</p>	<p>Most internet users perceive themselves to be much better at managing privacy settings than other users, and much less vulnerable than others to online privacy risks.<sup>64</sup> At the same time, having previous experience of privacy infringements can reduce the gap between how people see their own vulnerability to privacy risks compared to others. Research also indicates that the majority of people who claimed to understand certain privacy technologies could not correctly answer questions about these technologies.<sup>65</sup></p>

<sup>59</sup> Competition and Markets Authority (2020). [Online platforms and digital advertising market study final report](#). Paragraph 38, page 14, and Table 4.2, page 175.

<sup>60</sup> Ibid. Table 4.1, page 174.

<sup>61</sup> TRUSTe/National Cyber Security Alliance. (2016). [TRUSTe/National Cyber Security Alliance Great Britain Consumer Privacy Index 2016 Infographic](#).

<sup>62</sup> Ofcom. (2016). [Adults’ media use and attitudes report 2016](#).

<sup>63</sup> Marreiros, H., Gomer, R., Vlassopoulos, M., & Tonin, M. (2015). Exploring user perceptions of online privacy disclosures.

<sup>64</sup> Cho, H., Lee, J. S., & Chung, S. (2010). Optimistic bias about online privacy risks: Testing the moderating effects of perceived controllability and prior experience. *Computers in Human Behavior*, 26(5), 987-995.

<sup>65</sup> Jensen, C., Potts, C., & Jensen, C. (2005). Privacy practices of Internet users: Self-reports versus observed behavior. *International Journal of Human-Computer Studies*, 63(1-2), 203-227.

<b>Habits.</b> People are used to accessing digital technologies on a daily basis and accepting terms with little thought or deliberation.	Social networks have become such a normal part of our lives that people use them even if they are concerned about the risks. <sup>66</sup> These platforms have become ingrained into daily routines for some people, and such strong habits are difficult to break. <sup>67</sup>
<b>Intention-action gap.</b> People's intentions do not automatically translate into corresponding actions.	In an experimental study, the actual disclosure of personal information to marketers was much higher than the initial intention to disclose. <sup>68</sup>
<b>Present bias.</b> People value immediate reward disproportionately more than they worry about future risks.	Decision-making models show that even if people are aware of future risks and want to protect themselves, they may not do so due to the effects of immediate gratification so common in the online world. <sup>69</sup>

### 3.3 Designing to help active choice

#### What forms of disclosure and interfaces help people to make active choices online?

Our review of behavioural science literature identified ten principles which affect people's ability to exercise 'active choice' (Table 5). We explored each of these in turn and used this understanding as a foundation for prototyping alternative approaches to online choices.

These principles fall into two groups:<sup>70</sup>

1. Those that support effective information disclosure, i.e. helping people to access and understand information
2. Those that support expression of choice, i.e. helping people to reflect their wishes.

<sup>66</sup> Blank, G., Bolsover, G., & Dubois, E. (2014). A new privacy paradox: Young people and privacy on social network sites. Prepared for the Annual Meeting of the American Sociological Association (Vol. 17).

<sup>67</sup> Debatin, B., Lovejoy, J. P., Horn, A. K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of computer-mediated communication*, 15(1), 83-108.

<sup>68</sup> Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of consumer affairs*, 41(1), 100-126.

<sup>69</sup> Acquisti, A. (2004). Privacy in electronic commerce and the economics of immediate gratification. In *Proceedings of the 5th ACM conference on Electronic commerce* (pp. 21-29).

<sup>70</sup> For other summary tables on 'nudge' techniques relevant for consumer choice and effective interface design see Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., ... & Wang, Y. (2017). Nudges for privacy and security: Understanding and assisting users' choices online. *ACM Computing Surveys (CSUR)*, 50(3), 1-41, and Schneider, C., Weinmann, M., & Vom Brocke, J. (2018). Digital nudging: guiding online user choices through interface design. *Communications of the ACM*, 61(7), 67-73.

**Table 5: Summary of principles to support active choice**

Principles	Key insights
Factors that support effective information disclosure	
1. Recognise users' limited time and mental capacity	<ul style="list-style-type: none"> <li>● Shorten and simplify information as much as possible</li> <li>● Summarise information in bullet-points</li> <li>● Present information in short chunks, e.g. in a speech bubble that appears alongside a certain choice</li> </ul>
2. Maximise ease of navigation	<ul style="list-style-type: none"> <li>● Minimise the friction needed for people to find information (e.g. no. of clicks)</li> </ul>
3. Consider the timing of disclosure	<ul style="list-style-type: none"> <li>● Disclose information at timely moments, such as when a service changes</li> <li>● Disclose information early in a journey</li> </ul>
4. Personalise the content	<ul style="list-style-type: none"> <li>● Tailor information to the user</li> <li>● Only show content that is relevant</li> </ul>
5. Make the information salient or visual	<ul style="list-style-type: none"> <li>● Make key information stand out</li> <li>● Use diagrams, visualisations or comics to help explain concepts</li> </ul>
Factors that support people's ability to express choice	
6. Check framing and defaults	<ul style="list-style-type: none"> <li>● Set fair and transparent defaults, i.e. avoid defaults that are disproportionately in favour of the firm at the users' expense, or against the majority of people's preferences</li> <li>● Avoid steering decision making by removing defaults and forcing choices</li> <li>● Appreciate the nuances of framing, using existing research or by testing</li> </ul>
7. Make the trade-offs interactive	<ul style="list-style-type: none"> <li>● Allow people to interact with, or experience, what the choice means</li> </ul>
8. Find the right granularity of choice	<ul style="list-style-type: none"> <li>● Give choices at a level of granularity which is meaningful to people and can be understood</li> <li>● Offering additional choices can in itself reduce privacy concern and increase willingness to disclose</li> <li>● Intermediaries may usefully aggregate choices for people (e.g. the <a href="#">Jumbo</a> app controls privacy settings across multiple apps in one place)</li> </ul>
9. Ensure comparability of options	<ul style="list-style-type: none"> <li>● Allow people to make direct comparisons across options by providing consistent information</li> </ul>
10. Allow people to help their future selves	<ul style="list-style-type: none"> <li>● Offer tools for people to set reminders, commitments, or time-limits on the choices they set today</li> </ul>

## Factors that support information disclosure

### 1. Recognise people's limited time and mental capacity

Individuals have a finite amount of attention and mental capacity to engage with any given decision that they are faced with.<sup>71</sup> Complex information and language can be difficult to understand and digest. Therefore the most straightforward techniques to increase people's understanding in the first instance may be to **shorten information and make it easy to understand, e.g. by using plain language and short, simple sentences.**

In 2016, a European Commission study found that shortening and simplifying terms enhanced readability and improved users' understanding and trust.<sup>72</sup> Simply shortening terms and conditions may not be sufficient. A more recent BIT experiment shortened contractual terms from 1,400 words to 700 but found no change in people's understanding (measured using multiple-choice questions for 8 of the key terms).<sup>73</sup> This may be because the terms were still too long to be digestible, or because the underlying information was still complex or otherwise hard to understand, which is concerning given the 1,400-word version reflected terms found in practice.

Of the 24 techniques tested by BIT in a study for the Department for Business, Energy & Industrial Strategy (BEIS), two of those with the biggest effect involved **pulling out key terms and presenting them to people as a bullet-point summary**, without users needing to click to view a page with the full terms. Summarising with icons increased average understanding of key terms by 34% (from 42% to 57%), and using a question-and-answer format increased understanding by 36% (from 42% to 58%).<sup>74</sup>

Another highly effective technique was to **break up the information in a privacy notice into small chunks and present it 'just in time'**, e.g. at the moments when people are giving personal data or filling in particular fields of a form. For example, when entering an email address, a pop-up dialogue box said "We will use your email address... to contact you with important information about any changes to your account". This 'just in time' technique increased average comprehension by 9% (from 42% to 46%).

However, comprehension remained very low, even in the most effective conditions, with participants correctly answering on average only 45% of the comprehension questions

---

<sup>71</sup> Kahneman, D. (2003). Maps of bounded rationality: Psychology for behavioral economics. *American economic review*, 93(5), 1449-1475.

<sup>72</sup> Elshout, M., Elsen, M., Leenheer, J., Loos, M., & Luzak, J. (2016). [Study on Consumers' Attitudes Towards Terms Conditions \(Ts&Cs\) Final Report](#). Report for the European Commission, Consumers, Health, Agriculture and Food Executive Agency (Chafea) on behalf of Directorate-General for Justice and Consumers.

<sup>73</sup> Behavioural Insights Team (2019). [Improving consumer understanding of contractual terms and privacy policies: evidence-based actions for businesses](#).

<sup>74</sup> The percentage changes quoted here and below were calculated from the raw data. The percentage change between the (rounded) percentages is different due to rounding.

across all experiments. It's likely that understanding would be even lower still in a real environment, with other tasks competing for attention. **So, while shorter and sharper disclosures can deliver small boosts to understanding, such simple techniques, modifying the status-quo, will not have a transformative effect on understanding.** Furthermore, when poorly designed, additional disclosures can backfire or even be used to coerce people towards more negative outcomes.<sup>75</sup> For this reason, the Australian Securities and Investments Commission publicly “called time” on a reliance on disclosure remedies last year.<sup>76</sup>

## 2. Maximise ease of navigation

**As well as making information easy to digest, it needs to be easy to find.** Combining these factors can be highly effective: the Dutch government, seeking to get companies to download a report on an energy efficiency feedback scheme, found that sending a shorter email to businesses with one fewer click to access the report tripled the download rate.<sup>77</sup>

Dark patterns - intentional design features which confuse, stymie and/or manipulate people's choices - highlight the impact of transparency and ease of navigation when deployed with bad intent. Using design tricks to make it harder to cancel an enrollment in a fraudulent service more than doubled those that remained enrolled; introducing even more aggressive dark patterns (additional screens and trick questions) kept four times as many people enrolled.<sup>78</sup>

The idea of 'layering' privacy notices - where information is grouped under key headings, with links to expand or learn more, as shown in Figure 3 - has been recommended by the OECD since 2006<sup>79</sup> and, more recently, by the Information Commissioner's Office.<sup>80</sup> The BIT study for BEIS, however, found that layering the contents of a privacy notice had no impact on understanding. This may be because it hid information from immediate sight, and added friction (i.e. several clicks) for it all to be revealed. Having all terms presented in full by default in a long, scrollable box within the webpage, actually increased understanding by 26% (from 42% to 54%). Rather than assisting navigation and comprehension of privacy policies this technique, termed 'forced exposure', put the terms in plain sight by default.

---

<sup>75</sup> Adjerid, I., Acquisti, A., Brandimarte, L., & Loewenstein, G. (2013). Sleights of privacy: Framing, disclosures, and the limits of transparency. In Proceedings of the ninth symposium on usable privacy and security (pp. 1-11).

<sup>76</sup> [19-279MR ASIC 'calls time' on disclosure reliance.](#)

<sup>77</sup> Rosenkranz, S., Vringer, K., Dirkmaat, T., van den Broek, E., Abeelen, C., & Travaille, A. (2017). Using behavioral insights to make firms more energy efficient: A field experiment on the effects of improved communication. *Energy Policy*, 108, 184–193.

<sup>78</sup> Luguri, J., & Strahilevitz, L. (2019). Shining a light on dark patterns. University of Chicago, Public Law Working Paper, (719).

<sup>79</sup> OECD (2006), [Making Privacy Notices Simple: An OECD Report and Recommendations](#), OECD Digital Economy Papers, No. 120, OECD Publishing, Paris.

<sup>80</sup> Information Commissioner's Office. Guide to the General Data Protection Regulation (GDPR). [Right to be informed.](#)



### Figure 3: Example of 'layered' privacy notice

Privacy Policy (click below for more information)

- ▶ Information we collect about you
- ▶ Information we collect about how you use Compareeverything.com

We also collect your IP address, your computer's make and model, and how you use our website, such as which links you click on. Learn more in our privacy policy.

- ▶ Giving your information to others
- ▶ Sharing information with other companies in our group
- ▶ Credit checks to obtain quotes
- ▶ Newsletters
- ▶ Our commission model

Source: Behavioural Insights Team (2019). [Improving consumer understanding of contractual terms and privacy policies: evidence-based actions for businesses.](#)

### 3. Consider the timing of disclosure

People respond differently to prompts depending on when they occur.<sup>81</sup> The effectiveness of 'just in time' privacy reminders highlighted above suggest that the right moment to intervene can be very specific, even within a webpage, such as when entering your email. In general, **people are more likely to engage when prompts coincide with relevant events**, e.g. when making other service changes, or when approaching renewals or expirations. To demonstrate, annual statements have no effect on unarranged overdraft charges, while timely text alerts/mobile app notifications reduce them.<sup>82</sup> This principle applies to when information disclosures are made, but equally when a choice is prompted. So people may be more likely to engage with reminders to review certain settings when they are, for example, updating profile information, rather than when first opening the app.

### 4. Personalise the content

**Information which is of direct relevance to the user is more likely to capture our attention and drive engagement**, for example by using a person's name, personalising the contents of a message, or highlighting that the information is being specifically directed at that user.<sup>83</sup> For maximum impact, screens should *only* show information that is immediately relevant to a particular person, to reduce information overload.<sup>84</sup>

---

<sup>81</sup> Karlan, D., McConnell, M., Mullainathan, S., & Zinman, J. (2016). Getting to the top of mind: How reminders increase saving. *Management Science*, 62(12), 3393-3411.

<sup>82</sup> Financial Conduct Authority (2015). [Message received? The impact of annual summaries, text alerts and mobile apps on consumer banking behaviour.](#)

<sup>83</sup> Sahni, N. S., Wheeler, S. C., & Chintagunta, P. (2018). Personalization in email marketing: The role of noninformative advertising content. *Marketing Science*, 37(2), 236-258.

<sup>84</sup> Benartzi, S. and J. Lehrer (2017), *The smarter screen: surprising ways to influence and improve online behavior*, Penguin, New York.

## 5. Make the information salient or visual

Beyond personalisation as a tool to attract attention, there are many ways to make information appear more novel and accessible, i.e. to make it 'salient'. In one study participants were better at recognising advertising online when advert disclosures involved the following:<sup>85</sup>

- Different background colours and borders around adverts;
- Increased text sizes and contrasting colours for disclosures (e.g. "Advertising");
- Relevant placement of the disclosure (e.g. in the top-left for English speakers);
- Clear, consistent use of terminology (e.g. always "Advertising" not "Sponsored").

Visuals can be particularly powerful. Comic strip-style displays can increase understanding of consumer contract terms by 24%.<sup>86</sup> Graphs such as histograms have been found to improve consumer understanding of credit card costs, above and beyond use of annual percentage rates (APR), with different visuals having differing degrees of effectiveness.<sup>87</sup> Based on this evidence, services which visually summarise online information - such as the Firefox plug-in [Lightbeam](#) which maps third party tracking cookies on different websites - may be more effective text-based summaries.

It is also worth considering the emotional connection of information: a study to test warnings to consumers who were about to buy incompatible digital products found that emotive graphics were effective while traditional warning messages had no impact.<sup>88</sup>

While some studies consider age differences, there is little evidence on what techniques work best for different demographics or types of user. **Ideally, designers would draw on insight into what works for different user groups (e.g. people who prefer spatial maps or comic strips to detailed written descriptions) and enable users to select a display format of their choice.**

## Factors that support people to express choice

## 6. Check defaults and framing

As highlighted in the section above on people's behaviours, many behavioural biases affect the way that people make decisions, and subtle changes in the way choices are presented can have material consequences on the choices people make. Two recent papers neatly

---

<sup>85</sup> Federal Trade Commission (2017). [Blurred Lines: An Exploration of Consumers' Advertising Recognition in the Contexts of Search Engines and Native Advertising](#), FTC Staff Report, Washington.

<sup>86</sup> Botes, M. (2017). Using Comics to Communicate Legal Contract Cancellation. *The Comics Grid: Journal of Comics Scholarship*, 7.

<sup>87</sup> Chin, A., & Bruine de Bruin, W. (2019). Helping consumers to evaluate annual percentage rates (APR) on credit cards. *Journal of Experimental Psychology: Applied*, 25(1), 77.

<sup>88</sup> Esposito, G., Hernández, P., van Bavel, R., & Vila, J. (2017). Nudging to prevent the purchase of incompatible digital products online: An experimental study. *PloS one*, 12(3).

summarise the behavioural factors that affect active privacy choices.<sup>89 90</sup> Within these reviews, there are foundational behavioural factors of particular relevance to this project:

1. **Set fair, transparent defaults, or force a choice:** given people's tendency to stick with a default option, they should as far as possible be configured to align with people's expectations and not disproportionately benefit businesses at users' expense. 'Smart' defaults, informed by volunteered user data, could help set defaults in line with expectations on a person-by-person basis. When there is no strong justification for steering decision-making over discrete choices, defaults should be removed.
2. **Consider how framing affects choice:** for example, if the switch to a chronological newsfeed is presented in terms of what is lost ("*do not prioritise content*") rather than what is gained ("*see the most recent content first*").<sup>91</sup> Information surrounding a choice - such as mention of unrepresentative examples, or of unlikely downsides - can also influence decision making. Regulators have a role in addressing exploitative practices such as obviously misleading requests for data collection. A more general remedy to manipulative framing is to present the trade-offs in the round, rather than an unbalanced picture covering only what one will gain or lose from a choice.

Designers need to be aware that seemingly irrelevant cues can affect privacy decisions. For example, people may be more willing to disclose information to websites which look *less* professional.<sup>92</sup>

## 7. Make the trade-offs interactive

As well as making information visually engaging (see point 5) it may be possible to **make the choice itself interactive, and responsive to provisional user selection**. Using an interactive 'slider' to set a chosen credit card repayment amount in a lab experiment, which immediately adjusted information on total costs and the final repayment date, dramatically increased (hypothetical) repayment amounts.<sup>93</sup> This was the case even when the default option was still to make the minimum repayment.

The potential further applications of this in a digital context are endless. For example, a site could give people a visual preview of what their experience would look like under alternative data sharing scenarios.

---

<sup>89</sup> Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., ... & Wang, Y. (2017). Nudges for privacy and security: Understanding and assisting users' choices online. *ACM Computing Surveys (CSUR)*, 50(3), 1-41.

<sup>90</sup> Schneider, C., Weinmann, M., & Vom Brocke, J. (2018). Digital nudging: guiding online user choices through interface design. *Communications of the ACM*, 61(7), 67-73.

<sup>91</sup> Tversky, A., & Kahneman, D. (1989). Rational choice and the framing of decisions. In *Multiple criteria decision making and risk analysis using microcomputers* (pp. 81-126). Springer, Berlin, Heidelberg.

<sup>92</sup> John, L. K., Acquisti, A., & Loewenstein, G. (2011). Strangers on a plane: Context-dependent willingness to divulge sensitive information. *Journal of consumer research*, 37(5), 858-873.

<sup>93</sup> Behavioural Insights Team and Ipsos MORI (2018). [A behavioural approach to managing money: Ideas and results from the Financial Capability Lab](#). The Money Advice Service.

## 8. Find the right granularity of choice

**While increased transparency is an important principle to empower choice, at times it can hinder choice. Providing too much information, particularly when it is complex or ambiguous, can lead to confusion and worse choices.** In addition, providing greater control can lead people to disclose more information than they would otherwise. Where possible the frequency and complexity of these choices should be minimised (e.g. allow people to make a choice once and have it apply across contexts and sites).

BIT worked with the NHS to test ways to improve their data sharing consent forms.<sup>94</sup> There was a particular interest in clarifying the different reasons for sharing data and its use - operational planning, research or both. We found that people found it very difficult to distinguish between the various uses and that hampered their ability to make an informed choice: only around 20% of people correctly identified when data was used specifically for *planning* purposes, but 84% correctly identified when data were used for *research and planning* purposes. Therefore, it was more helpful to provide the information in bundled form - that data can be used for operational planning and research.

There is also a 'control paradox', whereby having increased control over whether certain information is published can increase people's willingness to disclose, even if they are at increased risk of strangers using their data.<sup>95</sup> The reverse is also true: reducing degree of control increases privacy concerns, even when there are lower risks of strangers accessing the data. Taken together, these studies suggest that, from a safeguarding and data protection perspective, care needs to be taken to find a suitable level of granularity of choice in any given context.

## 9. Ensure comparability of options

Effective choice requires people to make judgements and trade-offs between different options, and hence requires an appreciation of the relative merits of the options. For example, what would someone's online experience look like should they opt in to third party tracking cookies, relative to how it looks now; how does each item in a list of settings affect the number of third parties that will have access to their personal information. **In all cases, the comparability of the competing options is especially important for making judgements.** People are much better able to identify the best foreign exchange deal when explanations are transparent *and* consistent; increasing transparency for some but not all suppliers had no positive impact on the ability of consumers to identify the best deal.<sup>96</sup>

People's belief in the potential for change and improvement are also important, which requires an understanding of the purported benefits of alternative options. In a personal

---

<sup>94</sup> Behavioural Insights Team (2018). [Data sharing and the importance of choice architecture in healthcare: new results.](#)

<sup>95</sup> Brandimarte, L., Acquisti, A., & Loewenstein, G. (2013). Misplaced confidences: Privacy and the control paradox. *Social Psychological and Personality Science*, 4(3), 340-347.

<sup>96</sup> Behavioural Insights Team (2018). [The impact of improved transparency of foreign money transfers for consumers and SMEs.](#)

finance context, many consumers are found to be overly pessimistic about their ability to achieve better outcomes if they take an action based on the disclosure, and therefore ignore disclosure information.<sup>97</sup> Therefore the purported benefits of alternative options also need to appear genuine and achievable.

Choice-aggregating intermediaries can reduce user effort and assist in the challenge of granularity, but also help to make choices comparable across services. For example, the *Terms of Service; Didn't Read* website and browser add-on provides consistent ratings and labels to website terms and privacy policies, from very good "Class A" to very bad "Class E". This should greatly facilitate people's assessment of the terms of any given website, by offering simple, familiar summaries over key privacy dimensions, as well as ease comparison across sites.

### 10. Allow people to help their future selves

People can act against their own longer-term interests in the present moment, taking actions which they later regret or where they would have preferred to exercise self-control.<sup>98</sup> This means that **tools which enable people to commit themselves to future actions can be powerful in a variety of contexts**. For example, several banks now enable customers to block future gambling spending. Such commitments can usually be undone, preserving personal freedom, but have some inbuilt 'friction' to remove (e.g. once the block is enabled, Monzo requires users to call customer service and wait 48 hours before being able to spend on gambling<sup>99</sup>).

Looking beyond one-off online choices to an ongoing user experience, there may be opportunities for people to commit to future behaviour - or at least to future review of present choices - when they first engage with a service.<sup>100</sup> For example, to enact screentime notifications, frictions or limits; set auto-expiry of certain permissions (e.g. location services once a holiday is over); or ask the service to remind them in 1 week or 1 month whether particular setting(s) are still optimised. To have real impact on people's lives, such tools must be experimentally tested before firm recommendations can be made.

---

<sup>97</sup> Adams, P. D., Hunt, S., Palmer, C., & Zaliauskas, R. (2019). Testing the effectiveness of consumer financial disclosure: Experimental evidence from savings accounts (No. w25718). National Bureau of Economic Research.

<sup>98</sup> Hoch, S. J., & Loewenstein, G. F. (1991). Time-inconsistent preferences and consumer self-control. *Journal of consumer research*, 17(4), 492-507.

<sup>99</sup> <https://monzo.com/blog/2018/06/19/gambling-block-self-exclusion>

<sup>100</sup> Behavioural Insights Team (2019). [The behavioural science of online harm and manipulation, and what to do about it.](#)