Harmful design in digital markets:

How Online Choice Architecture practices can undermine consumer choice and control over personal information

A joint position paper by the Information Commissioner's Office and the Competition and Markets Authority

Contents

Summary

ICO and CMA concerns

Online interfaces and design choices are a fundamental touchpoint between firms and users who participate in digital markets.

In digital markets, the ways in which firms present information and choices to users of websites and other online services – referred to as Online Choice Architecture or OCA in this paper – play a crucial role in influencing consumer and market outcomes. They influence consumer decisions across a range of competitive parameters, including how firms collect, use and share personal information. This then impacts consumer experiences in digital markets, where many products and services are personalised. In turn, this influences competition outcomes, where firms rely on access to personal information to provide their products and services.

Consumers' ability to exercise meaningful choice and control is fundamental to robust data protection, consumer protection and competition regulation.

The Information Commissioner's Office (ICO) and Competition and Markets Authority (CMA) share concerns that some common online design practices influence consumers' decisions in ways they are not aware of and may not want. Specific design practices can make it difficult for consumers to make informed decisions generally, and firms who make it difficult to make good choices risk infringing consumer protection law. More particularly, design practices can undermine consumers' ability to exercise choice and control over how their personal information gets processed, which risks infringing data protection law. The public feel very strongly about the potential misuse of their personal information – ICO research shows that 90% of people are concerned about organisations using their personal information without their permission.[1]

Where design practices are found to undermine consumers' choice and control over their personal information, this is more likely to infringe data protection or consumer law and cause harm.

The ICO considers it an infringement of data protection law where design practices steer people to decisions that do not reflect their privacy preferences, whilst making it harder for them to choose more privacy-friendly

[1] 56% very concerned, 34% slightly concerned. See ICO Public Awareness Survey, p. 23.

options. The ICO will take formal enforcement action where necessary to protect people's information and privacy rights, particularly where design practices lead to risks or harms for people at risk of vulnerability.

OCA practices, including those which involve the collection and use of personal information, can also negatively impact consumers and competition. The CMA is undertaking a programme of work to tackle problems caused by harmful OCA including through consumer enforcement action. The CMA's annual plan for 2023/24 prioritises tackling misleading online practices including through further consumer education and through exercising its consumer enforcement powers.

Purpose of this ICO-CMA position paper

This position paper is targeted to firms that deploy design practices in digital markets (such as on websites or other online services), as well as product and UX designers that create online interfaces for firms. It provides:

- an overview of how design choices online can lead to data protection, consumer and competition harms, and the relevant laws regulated by the ICO and CMA that could be infringed by these practices; and
- practical examples of design practices that are potentially harmful under our respective regimes when they are used to present choices about personal data processing. These practices are **"harmful nudges and sludge", "confirmshaming", "biased framing", "bundled consent"** and **"default settings"**.

This joint position paper provides further clarity to firms and those who design OCA about how data protection law applies to design practices. Firms must avoid using the harmful practices set out in this paper in order to ensure compliance with data protection law. This will help to protect people's privacy, while also setting clear standards that support a level playing field between competing businesses – to the benefit of consumers.

ICO and CMA expectations

If used responsibly, online choices can be designed to empower consumers to make good choices about the way their personal information is collected and used when they engage with online services. The paper helps firms to achieve this, by setting out the ICO and CMA's shared expectations about how firms present information and choices to users of digital services about how their personal data is processed.

The ICO and CMA share the following expectations of firms that are using OCA in relation to choices about personal data:

- **Put the user at the heart of your design choices:** Are firms building their online interfaces around the user's interests and preferences?
- **Use design that empowers user choice and control:** Are firms helping users to make effective and informed choices about their personal data, and putting them in control of how their data is collected and used?
- **Test and trial your design choices:** Has testing and trialling been carried out to ensure their design choices are evidence-based?
- **Comply with data protection, consumer and competition law:** Do firms consider the data protection, consumer protection and competition law implications of the design practices they are employing?

Next steps for stakeholders

The ICO and CMA expect the positions in this paper to drive improvements to firms' choice of design practices in digital markets. This paper provides further clarity on how certain techniques could contravene data protection law, and may negatively impact consumers and competitive markets. The ICO and CMA are aligned in our concerns about the harmful effects these practices can have on consumers and markets when organisations misuse them.

The ICO may take formal regulatory action against firms which continue to use concerning design practices in ways that it considers to contravene data protection law, including those outlined in this paper. The CMA is already taking action to tackle wider misleading online practices including through exercising its consumer enforcement powers.

We invite stakeholders to get in touch if interested in participating in further engagement with the ICO and CMA on this paper, including a workshop in the autumn about good practices for the design of privacy choices online. We encourage stakeholders invested in the process for designing choices related to the use of consumers' personal information, such as UX designers, information architects and firms themselves, to register interest at:

digitalregulationcooperation@ico.org.uk

1. Introduction

The importance and impact of Online Choice Architecture

The way that information is presented and choices are structured plays an important role in shaping consumers' decision-making and behaviour online. We refer to this as "Online Choice Architecture" (OCA) in this paper.

OCA practices can encompass a wide range of behaviours across digital markets, including, for example, the way prices are displayed and how information is presented to consumers about the goods and services they are purchasing. This position paper focuses specifically on OCA practices in relation to consumers' choice and control over their personal information.[2]

OCA influences user[3] decisions and actions about how firms collect, further process and share their personal information – affecting how users exercise their information and privacy rights. OCA also has an impact on user experiences in digital markets, in which personalised services, such as tailored recommendations, are common. This in turn influences competition outcomes for firms that rely on access to personal data to provide their products and services.

Well-designed OCA can guide users towards choices that align with their goals, preferences or best interests. For example, when used fairly, default security settings can help users avoid computer viruses and stay safe online.[4] Effective choice architecture can also empower users to make good choices about the way their personal information is collected and used when engaging with online services, such as choosing whether to allow a firm to use browsing activity to target adverts. It can also improve their experience by making interfaces more intuitive and easier to use - for example, a quick and seamless returns process.[5] OCA that enables effective user decision-making strengthens incentives for firms to compete fairly.

---

[2] In this paper, the term "personal information" means any information that would be defined as "personal data" under the UK General Data Protection Regulation or Data Protection Act 2018. The terms "personal information" and "personal data" are used interchangeably in the paper.

[3] In this paper, the term "user" or "consumer" is used to refer to individuals using digital services. The equivalent term under data protection law is "data subject".

[4] See p. 2, para. 1.3 of CMA discussion paper Online Choice Architecture - How digital design can harm competition and consumers.

[5] See p. 2, para. 1.2 of CMA discussion paper Online Choice Architecture - How digital design can harm competition and consumers.

OCA practices can also be used to undermine users' control over their personal information and steer their behaviour in harmful ways that do not align with their best interests or preferences about its use. For example, by designing interfaces that nudge users towards decisions that they may not otherwise have made, or by making it unduly difficult to exercise certain choices, harmful OCA can undermine information and privacy rights, consumer rights and market competition.

All of us, as consumers, are often subject to behavioural biases that affect our decision making, such as a tendency to stick with the default option, being more focussed on the present than the future, or a tendency to be overconfident and therefore make riskier decisions.[6] OCA practices can be used to exploit these biases and influence and distort the choices that consumers make.

ICO and CMA interest in Online Choice Architecture

OCA practices are a crucial factor when considering how users' data is collected, used, and shared in digital markets. This makes them of interest to both the ICO, because of their impact on consumers' information and privacy rights, and the CMA, because of their impact on how businesses compete and how consumers are treated.

The CMA has an ongoing and active programme of work in relation to OCA practices in general. It published a discussion paper in 2022 on how digital design can harm competition and consumers.[7] It has also been tackling misleading online practices through further consumer education[8] and consumer enforcement.[9] And it has initiated a broader programme of work tackling harmful online selling practices such as misleading urgency and price reduction claims.[10]

The ICO25 strategy sets out the ICO's commitment to giving people across society more meaningful control and improved confidence when participating in our increasingly digital society and economy.[11] The ICO is intent on driving

[6] See p. 24 of The Behavioural Insights Team and Citizens Advice Bureau report - Applying behavioural insights to regulated markets.
[7] CMA discussion paper Online Choice Architecture - How digital design can harm competition and consumers.
[8] Including through continuing with the CMA's "Online Rip-Off Tip-Off" campaign for raising consumer awareness around harmful online practices.
[9] CMA Annual Plan 2023 - 2024.
[10] CMA Online Choice Architecture Work.
[11] ICO25 Strategic Plan.

higher standards in the way online design is used in relation to personal data processing. We want members of the public to feel confident about how their data is used in digital markets, so they can benefit from innovative products and services on offer without worrying that their information and privacy rights won't be respected.

In our 2021 Joint Statement, the ICO and CMA made clear that meaningful user choice and control are fundamental prerequisites to robust data protection and effective competition. The interests of both policy objectives can be met where consumers are empowered to make effective choices about services or products, providers compete on an equal footing to attract customers, and consumers have control over their personal information and can make meaningful choices over whether and for what purposes it is processed. [12]

Through our participation in the Digital Regulation Cooperation Forum (DRCF)[13], the ICO and CMA have prepared this joint position paper. It sets out our shared views concerning specific OCA practices that are frequently used in online interfaces that ask consumers to make decisions about the ways in which their personal information is collected and processed.

Purpose of this paper

This paper sets out the harms that can arise when OCA practices are poorly designed or misused. We then outline some specific OCA practices which involve the processing of personal data and explain why they can generate shared concerns for the CMA and ICO. The practices in question are **"harmful nudges and sludge", "confirmshaming", "biased framing", "bundled consent"** and **"default settings"**.

The OCA practices set out in this paper do not represent a comprehensive list of the practices that are of interest or could be of concern to the ICO and CMA either jointly or individually, nor does this paper cover all OCA practices that may be relevant to compliance with the laws we oversee. Instead, the aim is to use the examples to illustrate how we might approach the data protection, consumer and competition impacts of OCA practices across a range of cases. Through these illustrations, we seek to give firms greater clarity on OCA practices that concern us when personal information is processed, as well as

[12] See pp. 19-21 of Competition and data protection in digital markets: a joint statement between the CMA and the ICO.
[13] See p. 9 of DRCF Workplan for 2023-24.

provide steers on how different design choices could be used to encourage better privacy and competition outcomes for consumers accessing and using online services. By setting out these expectations, we aim to assist firms that use OCA practices to comply with relevant laws and help shape user experience testing and research that informs these practices.

Where expectations are not met and there is potential for harm to consumers, firms risk facing regulatory action.

- The **ICO's regulatory approach**[14] sets out that, where there is noncompliance with data protection laws, we can use our formal enforcement actions as necessary to protect people and prevent harm.
- The **CMA's general regulatory approach** is to create a framework in which competitive businesses and consumers are protected, taking enforcement action where necessary to achieve these aims. The CMA has already taken enforcement action against firms in relation to the use of wider OCA practices.[15]

We invite stakeholders to get in touch if interested in engaging further on the issues discussed in this paper, including a joint ICO-CMA workshop in the Autumn. You can get in contact with us at:

digitalregulationcooperation@ico.org.uk

[14] ICO25 – Our regulatory approach.
[15] See Emma Group consumer protection case and Wowcher Group consumer protection case.

2. How online choice architecture can lead to data protection, consumer and competition harms

As set out in our 2021 Joint Statement, the ICO and CMA support measures that enhance consumers' ability to control their personal information, decide the purposes for which and how it should be processed, and exercise their rights. These consumer outcomes are heavily influenced by the OCA used by firms. When used responsibly, OCA can allow consumers to make decisions freely and create an online environment in which they can easily make decisions that are in their own interests. However, OCA can also steer behaviour in ways that lead to harm.

Data protection harms

UK data protection law takes a flexible, risk-based approach that puts the onus on the firms that decide to process personal data[16] to think about and justify how and why they use that data. Potential harms from processing need to be considered by firms as part of this risk-based approach. Furthermore, the ICO's Data Protection Harms Taxonomy[17] sets out a framework for understanding how the infringement of data protection laws can lead to harm for individuals and society. Poor OCA practices can infringe data protection laws and lead to, or heighten, risks of harm, for example:

- **Bring about unwarranted intrusion:** Poor OCA practices can manipulate and influence users of digital services to make choices about their personal information that do not align with their preferences, such as sharing more personal information than they would otherwise volunteer. This can lead to more extensive processing about their behaviour, preferences and attitudes and, ultimately, unwarranted intrusion, such as unwanted targeted advertising or profiling.

- **Loss of control or autonomy:** Poor OCA practices can make it unduly difficult for users to choose freely how their data is processed and

[16] Referred to as "controllers" under data protection law. Controllers are the main decision-makers that exercise overall control over the purposes and means of processing persona data. See ICO guidance on controllers and processors for more information.
[17] ICO document Overview of Data Protection Harms and the ICO's Taxonomy.

deprive them of meaningful control over the way in which their personal information is used. Users may feel powerless to stop the use of their personal information in ways they do not want.

- **Costs of avoiding or mitigating harm:** Poor OCA practices can increase the amount of time users must spend to make informed choices about personal information processing or to take actions that align with their privacy preferences.

At an individual level, the data protection harm experienced by users may be annoyance and inconvenience. However, if a user is in a vulnerable situation, the impact could be more acute, such as financial loss or emotional distress. For example, poor OCA practices could lead to a user with a gambling addiction consenting to the use of their personal information for targeted advertising when they would not otherwise have done so. This could lead to them being shown a gambling advert which encourages them to gamble, in turn leading to financial loss and possible negative impact on their mental health.

Widespread use of poor OCA practices that undermine free user choice and normalise lower levels of privacy can also have an adverse impact on individuals' fundamental rights and freedoms. For example, where poor OCA practices are used for obtaining non-compliant consent, this can result in a user's personal information entering complex adtech ecosystem supply chains. Users may have no idea about the organisations that hold their data and therefore cannot effectively exercise their privacy and information rights. This could increase the risk of harms, such as those outlined above. The public feels very strongly about the potential misuse of their personal information – with ICO research showing that 90% of people are concerned about their personal information being used without their permission.[18]

This paper sends firms a clear signal on examples of OCA practices that are of concern, and the steps they can take to improve their practices. Where firms use OCA practices, including those outlined in this paper, in a way that we judge to unfairly steer users towards decisions that may not be consistent with their privacy preferences, or makes it harder for them to exercise their rights, the ICO is likely to consider this an infringement of data protection law. This may result in formal regulatory action being taken against firms that use such practices, particularly where it leads to risks or harms for people at risk of vulnerability.

[18] 56% very concerned, 34% slightly concerned. See ICO Public Awareness Survey, p. 23.

Annex 1 sets out the UK data protection laws that are especially relevant to the OCA practices set out in this paper.

Competition and consumer protection harms related to personal data processing

Depending on the specific context, OCA practices may benefit or harm competition and consumers. Examples of positive OCA can include a quick and seamless returns process, relevant recommendations for further products or services, and opportunities for consumers to commit to beneficial future actions.[19] However, OCA can also be used in ways that could harm competition and/or consumers. For instance, firms may use OCA practices to nudge consumers towards choices in a way that reinforces their market position and therefore could weaken competition. For example, this could be done by using OCA to collect more personal data from consumers than they would be willing to give by choice and by preferencing data collection for the firm's own services over its competitors.

With more consumer data, firms could then **leverage network effects** to:

- strengthen their market position, without necessarily doing so based on the merits of their product or service (e.g., by using this additional personal data to target advertising)[20],
- create lock-ins that make it difficult for consumers to switch from current providers[21], and
- ultimately make it harder for rivals to compete e.g., creating barriers to entry and expansion.[22]

OCA can be used to **distort consumer choices** by making certain options easier or more desirable to choose over others. This can:

- discourage more conscious deliberation of choices (e.g., by undermining the ability to process and assess information independently, or making it more difficult to shop around),

[19] See p. 2, para. 1.2 of CMA discussion paper Online Choice Architecture - How digital design can harm competition and consumers.
[20] See p.13 of CMA research paper Evidence Review of Online Choice Architecture and Consumer and Competition Harm.
[21] Acquisti, A., Brandimarte, L., and Loewenstein, G. (2020). Secrets and Likes: The Drive for Privacy and the Difficulty of Achieving It in the Digital Age. Journal of Consumer Psychology, 30(4).
[22] CMA Online platforms and digital advertising" market study final report.

- misrepresent choices available to consumers, and
- lead consumers to consent to potentially undesirable services or actions (e.g., to access a desired functionality).

This can result in ill-considered or inadvertent decisions that may decrease consumers' welfare and may not align with their preferences.

Annex 2 sets out how consumer and competition laws enforced by the CMA may apply to the OCA practices set out in this paper.

3. Examples of potentially harmful Online Choice Architecture practices

Data protection, competition and consumer protection harm can arise when OCA practices are not used in consumers' interests. The practices set out below are not a comprehensive list of OCA practices that are of interest or could be of concern to the ICO and CMA, either jointly or individually. Instead, we have presented a selection of practices where we feel our collective consideration can provide greater regulatory clarity for firms and help to prevent harm for consumers in digital markets. The examples given are illustrative only. Whether relevant laws have been infringed in any particular case would involve an assessment of the practice in question and all the relevant facts.

Harmful nudges and sludge

"Harmful nudges" (also called "dark nudges"[23]) are when a firm makes it easy – or "nudges" – users to make inadvertent or ill-considered decisions. These decisions can also be encouraged by creating excessive or unjustified friction – or "sludge" – that makes it difficult for the user to get what they want or to do as they wish.[24]

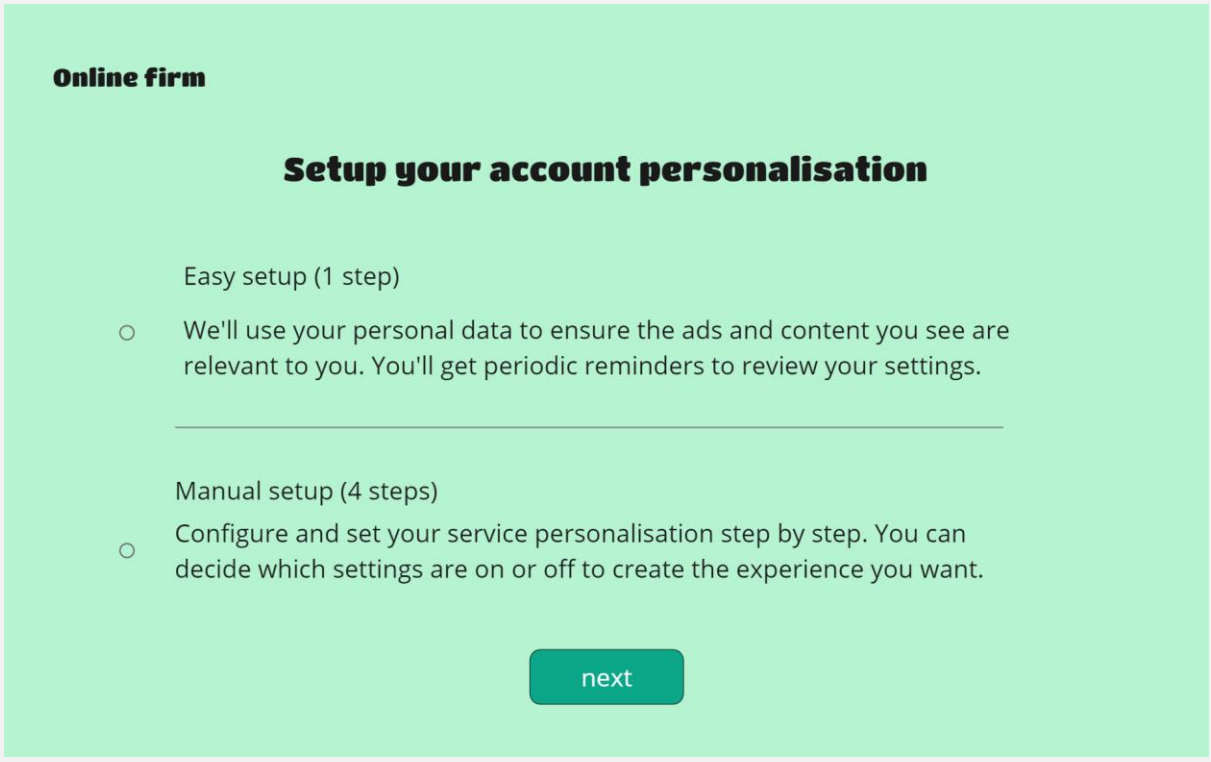
For example, a firm may make one option much less cumbersome or time consuming than the alternative. This can distort consumer choices by making certain options easier to choose over others. In turn, this can discourage more conscious deliberation of choices, resulting in ill-considered or inadvertent decisions that may decrease consumers' welfare or may not align with their preferences.[25]

When harmful nudge or sludge techniques are used, consumers may make choices they wouldn't otherwise have made and that do not align with their best interests or preferences.[26] For example, it could lead consumers to select

[23] For instance, see Newall, P. W. S. (2019). Dark nudges in gambling. Addiction Research and Theory, 27(2), pp. 65–67 for examples of dark nudges in the gambling industry.
[24] Sunstein, C. R. (2020). Sludge Audits. Behavioural Public Policy, pp. 1–20.
[25] CMA research paper Evidence Review of Online Choice Architecture and Consumer and Competition Harm.
[26] CMA discussion paper Online Choice Architecture - How digital design can harm competition and consumers.

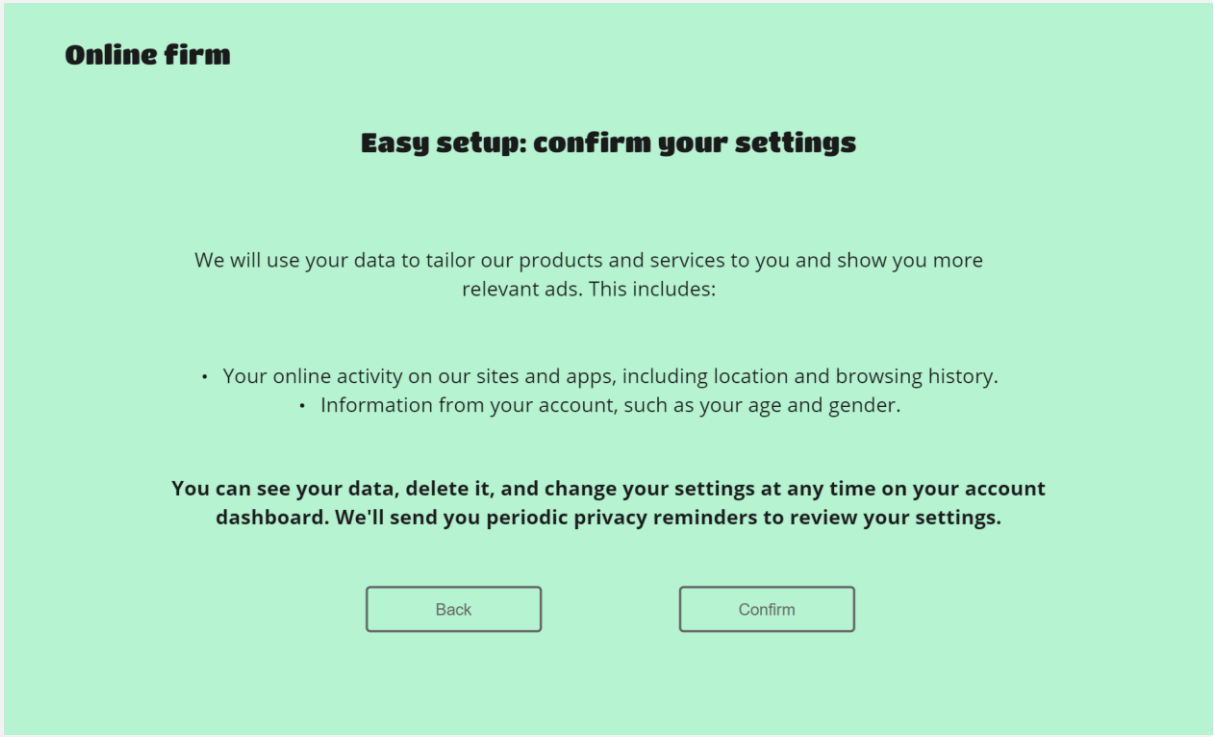
less privacy-enhancing choices when personalising their privacy settings or make it hard to change their privacy settings.[27]

Example: During its account setup process, a firm asks users to configure the level of personalisation of the service it offers, based on personal data such as the user's browsing history. The user is able to turn all personalisation on in a single step. However, the user has to go through several steps to turn personalisation off, with no option to simply reject all personalisation in a single step. This therefore nudges the user towards accepting all personalisation (which is more intrusive and also more beneficial for the firm) whilst discouraging them from exercising more granular control over what personal data they allow the firm to use for personalisation, or rejecting personalisation altogether.

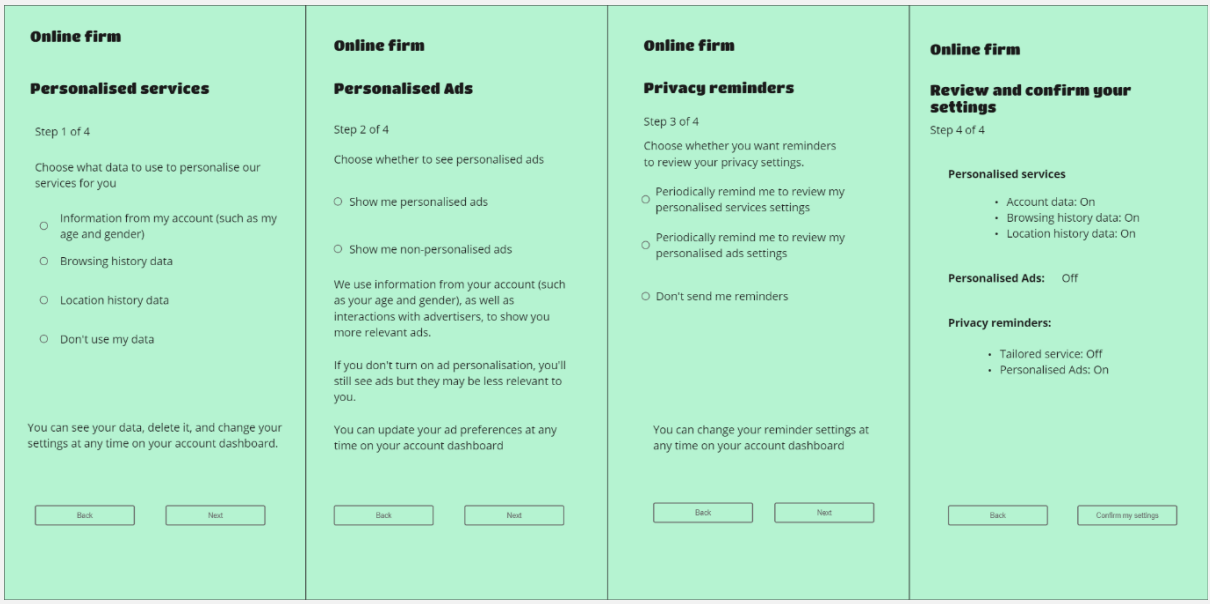


[27] A study analysing 300 data collection cookie consent notices from news outlets found that all websites provided a one-click option to accept the consent notice, however only 15 of the websites provided a one-click deny option. Further, the study identified the presence of excessive friction or sludge with regards to cookie preferences wherein about half of the websites examined required the user to undertake 10 to 12 clicks to opt out of all cookies. See: Soe, T. H., Nordberg, O. E., Guribye, F., and Slavkovik, M. (2020). Circumvention by design - dark patterns in cookie consent for online news outlets. Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society, pp. 1–12.

If user selects “Easy setup”

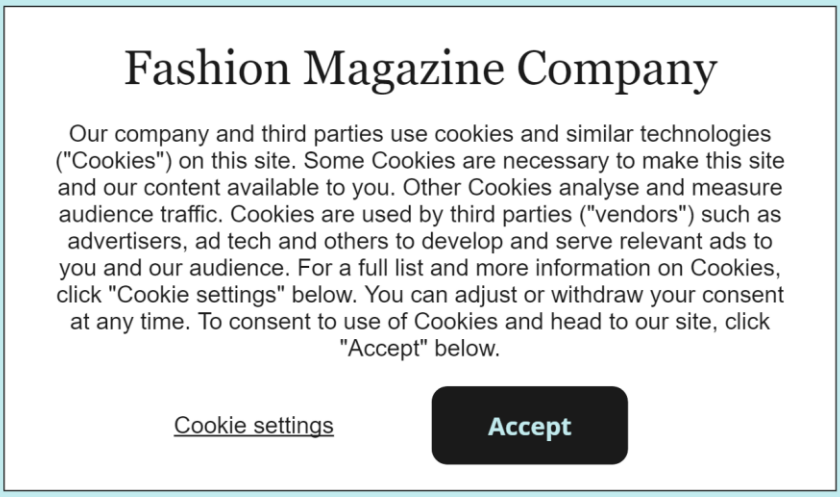


If user selects “Manual setup”



Harmful nudges and sludge are also often used in cookie permission pop-ups to encourage users to consent to non-essential cookies. For example, a cookie pop-up may include an option to consent to non-essential cookies with a single click (such as “Allow all”) but not include an equivalent option to refuse consent to non-essential cookies with the same ease, at the same layer (such

as “Reject all”). Instead, if users do not wish to consent to non-essential cookies, they must go into a settings page to do so and, in some cases, refuse consent to individual cookies. This process is much more time consuming and onerous; instead, users may simply click “Accept all” to make the pop-up go away.



ICO concerns: Using harmful nudges and sludge to create asymmetric friction between different choices discourages users from more conscious consideration of their decisions, particularly in situations where they wish to access content quickly or otherwise do not have the time or expertise to go through more detailed settings. Its use is therefore likely to infringe the “fairness” and “transparency” principles of Article 5(1)(a). Consent to process personal data collected using this practice is unlikely to be informed and therefore unlikely to meet the definition of consent under Article 4(11). This in turn would lead to an infringement of the lawfulness requirement of article 5(1)(a).[28]

Regulation 6 of PECR is likely to be infringed where a cookie banner that incorporates these practices is being used to obtain consent for placing

[28] See Annex 1 for more detail on how invalid consent under Article 4(11) leads to a breach of Article 5(1)(a) of the UK GDPR.

cookies.[29] Users must be able to refuse non-essential cookies with the same ease as they can accept them, without having to take any additional steps.[30] Where the user is presented with an option that allows them to skip more granular settings then the ICO expects, as a minimum, an equivalent option allowing them to refuse as well (e.g., a "Reject all" option as well as an "Accept all"). These must be presented with equal prominence; the user must understand what they mean and must not be nudged towards one over the other. This is more likely be compliant with data protection law, as firms will be better placed to demonstrate that the user has a genuine free choice.

CMA concerns: The use of harmful nudges and sludge in the design of online services can encourage users to provide more personal information than they would otherwise choose to as part of receiving those services. In the Final Report of the CMA's Online Platforms and Digital Advertising Market Study[31], it found that access to this personal information may confer a competitive advantage to certain large platforms and inhibit entry and expansion by smaller businesses. Where these techniques make certain options easier to choose over others and discourage more conscious deliberations of choices, this can result in ill-considered or inadvertent decisions that may decrease users' welfare or may not align with their preferences.[32]

Importantly, not all "nudges" in OCA design are harmful. When implemented responsibly, they can be used to steer users towards decisions that may be of benefit to them, for example by making it easy for users to switch to another bank account if they wish to do so. Similarly, "sludge" is not simply any friction. Friction may not be harmful if it is used to confirm or validate an important decision, for example, asking a user to confirm that they want to transfer a large sum of money to another bank account to reduce the risk of them being defrauded.

Confirmshaming

The term "confirmshaming" refers to the practice of pressuring or shaming someone into doing something by making them feel guilty or embarrassed for

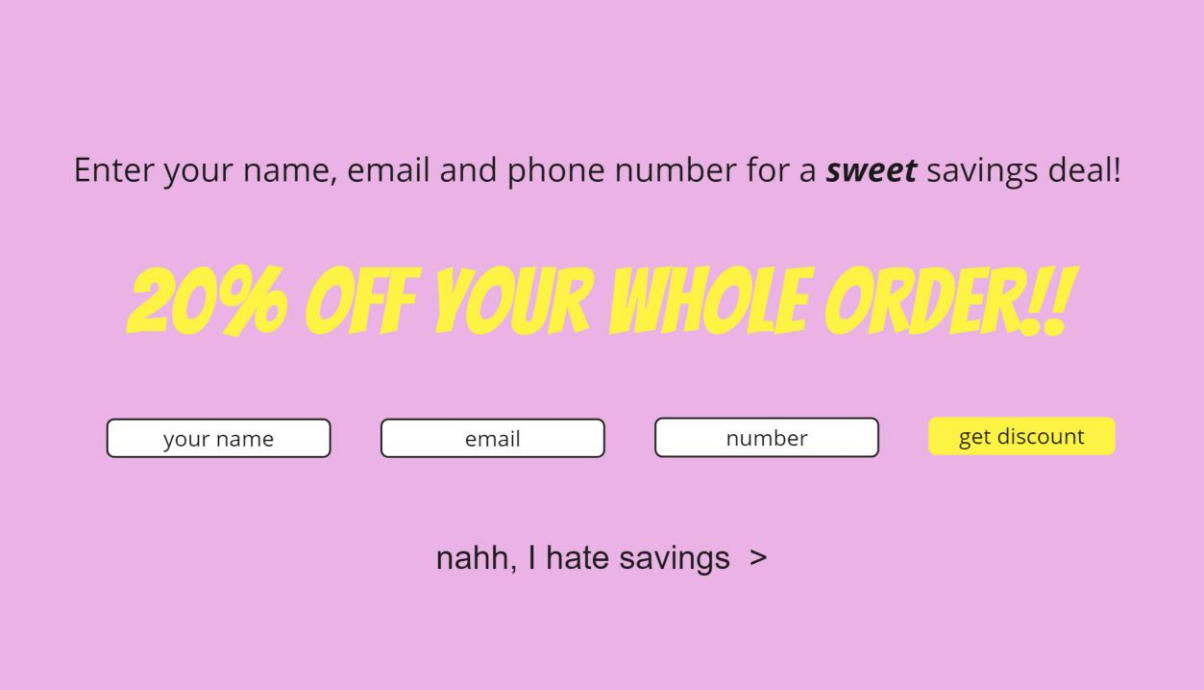
[29] See Annex 1 for more detail on the requirements of Regulation 6 of PECR, and how the definition of consent under PECR is taken from the UK GDPR.
[30] For example, if they can "accept" with a single click or tap then they must also be able to "refuse" with a single click or tap.
[31] CMA Online Platforms and Digital Advertising" market study final report.
[32] CMA research paper Evidence Review of Online Choice Architecture and Consumer and Competition Harm.

not doing it.[33] This can be done by using language that clearly suggests that there is a "good" and "bad" choice, and in more extreme cases that the user is morally wrong or socially unacceptable for not taking a particular action.

Confirmshaming practices can ultimately adversely affect users' choices, for example, by causing them to agree to the use of their personal information in a way that they would not otherwise agree to. Research has found that participants were more likely to accept a dubious service when the option to decline the service was framed as being shameful.[34] Use of confirmshaming practices can therefore distort users' choices by associating guilt or embarrassment with certain choices and not others.[35]

Example: Confirmshaming can be used in popups that ask a user to provide their email address in exchange for a discount.[36] A firm may offer users a discount in exchange for providing their email address and phone number so they can be used to send the user direct marketing. To decline this, the user must click a button that says:

"Nahh, I hate savings".



[33] Brignull, H, www.deceptive.design/types/confirmshaming
[34] Luguri, J., and Strahilevitz, L. J. (2021). Shining a Light on Dark Patterns. Journal of Legal Analysis, 13(1), pp. 43–109.
[35] Mathur, A., Kshirsagar, M., and Mayer, J. (2021). What Makes a Dark Pattern... Dark?. Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, pp. 1–18.
[36] Mathur, A., et al., (2019). Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites. Proceedings of the ACM on Human-Computer Interaction, Volume 3, Number CSCW, November 2019

ICO concerns: Whilst the UK GDPR does not prevent firms from offering users incentives to share their personal data or agree to its processing[37], using language similar to that described above to put pressure on users to do so is likely to infringe the "fairness" principle in Article 5(1)(a) of the UK GDPR.

Consent obtained in this manner is unlikely to be "freely given" and therefore likely to be invalid under Article 4(11) of the UK GDPR, leading to the "lawfulness" principle in Article 5(1)(a) being infringed. Use of confirmshaming in the manner described above is therefore almost always likely to lead to an infringement of data protection law and could lead to firms being subject to regulatory action from the ICO.

CMA concerns: Similar to our concerns with harmful nudges and sludge, confirmshaming could also nudge users towards choices to share more personal data than they otherwise would when receiving services. In certain markets, access to such data may confer a competitive advantage to existing incumbents and inhibit entry by smaller challenger businesses.

Biased framing

"Biased framing" refers to the practice of presenting choices in a way that emphasises the supposed benefits or positive outcomes of a particular option, in order to make it more appealing to the user ("positive framing"). It can also be used to emphasise the supposed risks or negative consequences of a particular option to discourage a user from selecting it ("negative framing"). An experimental study found that subjects were more likely to choose protective disclosure settings when the disclosure settings were framed in a manner that highlighted privacy protection goals compared to when they were framed in a manner which did not highlight privacy concerns.[38]

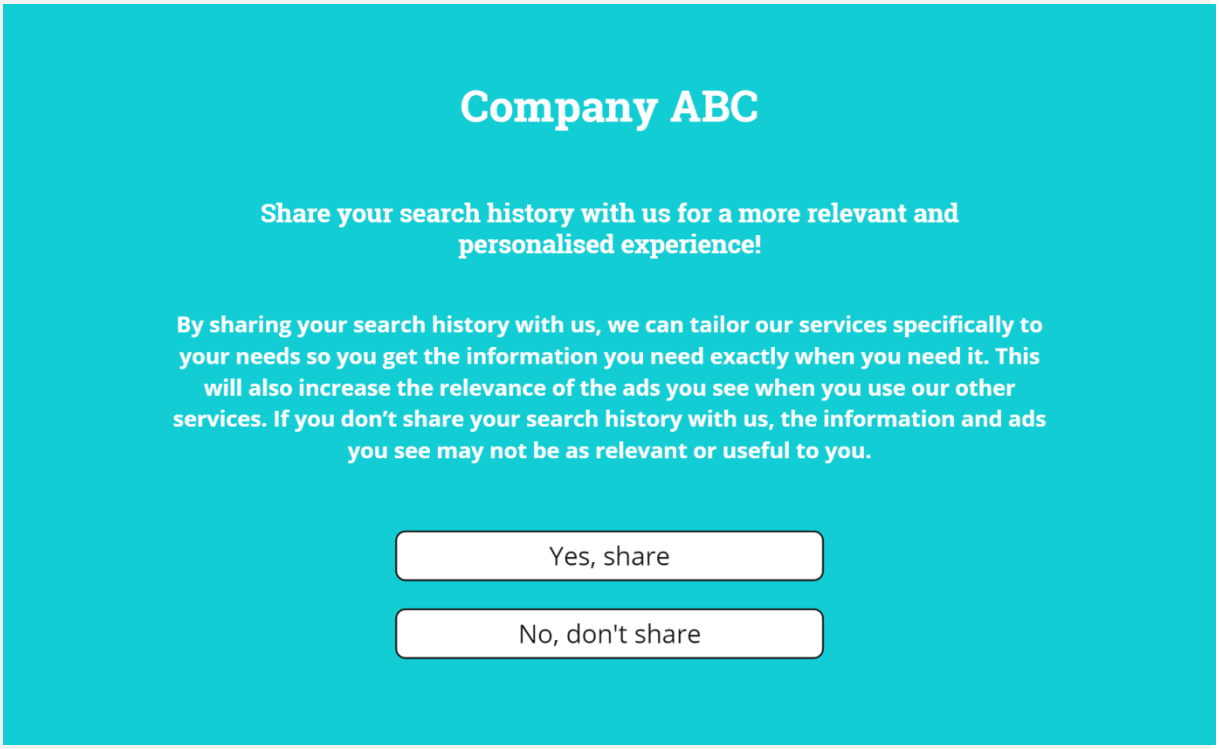
The misuse of positive and negative framing techniques can lead users to make ill-informed choices, distorting their decision-making by nudging them towards the more favourably framed choice (or away from the unfavourably framed choice). In digital markets, this could lead to unwanted personal data processing taking place, such as targeted advertising or unexpected marketing, potentially heightening risks of harm to an individual. ICO research shows this

[37] See ICO guidance on "What is valid consent?" and p. 30 of the ICO's Direct Marketing: detailed guidance.
[38] Adjerid, I., Acquisti, A., and Loewenstein, G. (2019). Choice architecture, framing, and cascaded privacy choices. Management Science, 65(5).

processing can often be unwanted by individuals, with 50% of people not happy with their personal information being used to suggest adverts to them.[39]

Example: a firm's website asks users if they are willing to share their search history in the following way:

"*By sharing your search history with us, we can tailor our services specifically to your needs so you get the information you need exactly when you need it. This will also increase the relevance of the ads you see when you use our other services. If you don't share your search history with us, the information and ads you see may not be as relevant or useful to you.*"



This approach uses positive framing to emphasise the potential positive impact of sharing search history whilst minimising or ignoring the potential risks of negative impacts from sharing search history (e.g., the increased collection and use of personal data in a potentially intrusive way, including tracking the user's activity to target ads at them). If the sharing of search history was framed differently (for example, "*We will track your search activity in order to target ads to you when using our other services*" or *"Yes, track my search activity"*), it is likely that users would be less willing to agree to it.

[39] 29% not particularly happy, 21% not happy at all. See ICO Public Awareness Survey p. 24

Furthermore, this approach uses negative framing to emphasise the potential negative impacts of not sharing search history (e.g., the possibility of the service not being as useful or relevant). It ignores the positive impact of refusing (e.g., reducing the risk of intrusive processing, retaining more control over personal data).

ICO concerns: Not giving equal weight to the risks and benefits of a decision about personal data processing means it is harder for users to properly assess the information and make an informed choice. This can lead to both the "fairness" and "transparency" principles in Article 5(1)(a) of the UK GDPR being infringed.

Consent obtained using biased framing that is not fair or transparent (because it deceives or misleads and is not open and honest) is also likely to be invalid, on the basis that it is not fully informed, thereby leading to infringement of the "lawfulness" requirement of Article 5(1)(a) and Article 7 of the UK GDPR.

This does not mean that users should be overloaded with information. Instead, firms should present users with sufficient information to make an informed decision in a clear, easy to understand and neutral way.

CMA concerns: The misuse of biased (positive or negative) framing generally can undermine users' ability to process and assess information independently, and therefore adversely affect their decision making. If it is misleading, it may breach consumer protection law.[40] With respect to data sharing choices, users can feel disempowered by their lack of knowledge about how businesses collect, use and share their data[41] which can make them vulnerable to how information about such choices are framed.

Businesses can also use biased framing to discourage users from making choices that could result in reduced information sharing. Incumbent businesses may apply these techniques to collect personal data which they may use to confer competitive advantages and inhibit entry and expansion by smaller challengers.[42]

Biased framing can also be used by businesses to preference their own services over services provided by rival providers; for example, by framing privacy

[40] See Annex 2, in particular, Regulations 3 and 5-7 of the CPRs.
[41] Which? research paper "Control, Alt or Delete? Consumer research on attitudes to data collection and use".
[42] CMA "Online platforms and digital advertising" market study Appendix Y: choice architecture and Fairness by Design.

choices in a manner which can potentially encourage users to opt-in to sharing data with the platform's own services while influencing users to opt-out from sharing data with third-party services.[43]

As with nudges, it is important to recognise that framing is not, in itself, harmful. It can be used to guide users towards choices that benefit them or away from choices that could cause harm. However, it can also be used in a way that results in harm. Where it is being used in ways that are not fair or transparent, the ICO is likely to consider this a breach of data protection law.

Bundled consent

"Bundled consent" involves asking the user to consent to the use of their personal information for multiple separate purposes or processing activities via a single consent option. This makes it harder for users to exercise granular control over what they do and don't wish their personal information to be used for.

Bundling multiple personal data processing activities or purposes into a single consent request can make it difficult for users to understand exactly what they are agreeing to and can make it more difficult for them to exercise granular control over their personal information. Whilst users may be able to exercise more granular control if they wish to do so (for example by finding the relevant option in their account settings), the offer of an "accept all" option increases the likelihood that they will consent to all processing, even if this does not actually align with their preferences.

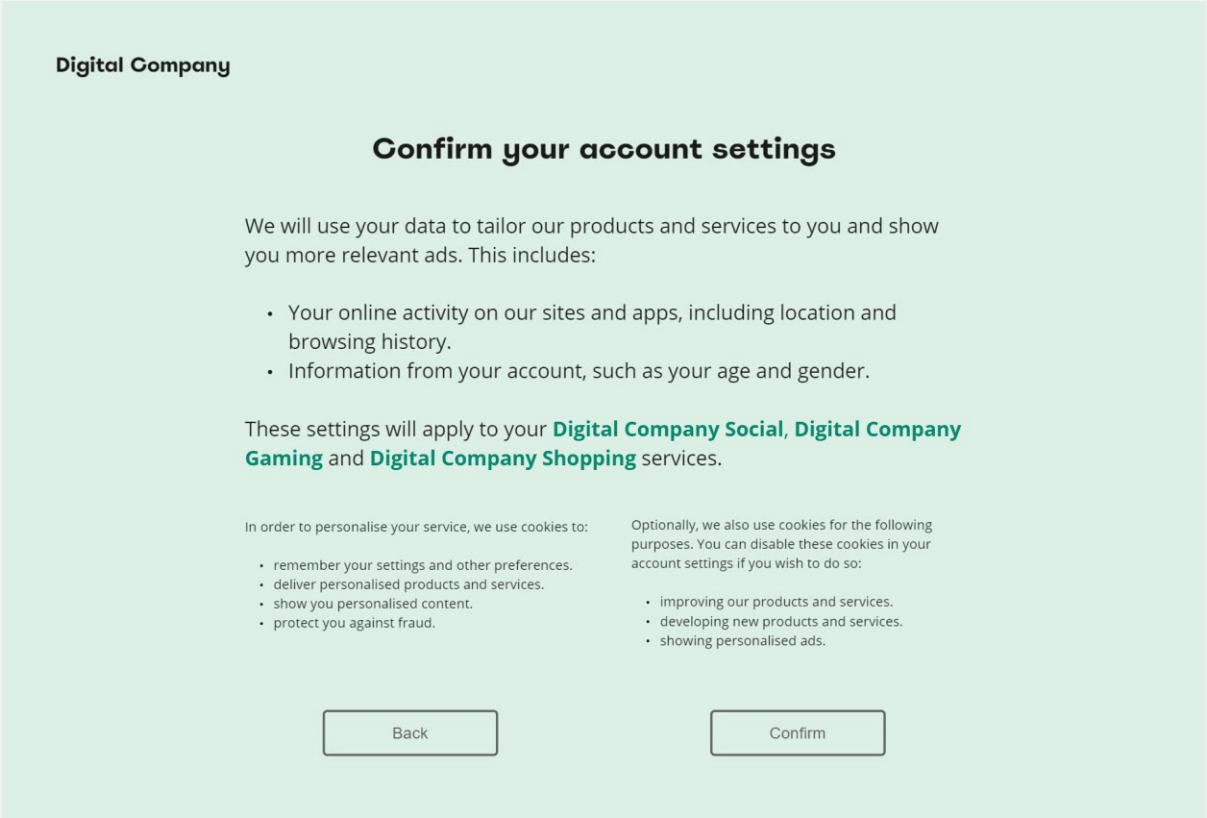
Bundled consent can lead to users making poor decisions and inadvertently or unwillingly consenting to personal data processing they may not want, such as targeted advertising or direct marketing, in order to access some other desired functionality. It is often used when people are asked to accept terms and conditions, privacy policies, or cookie preferences in order to access other services. For instance, a website might bundle consent for both the terms of use as well as for receiving marketing emails before one can create an account.[44]

[43] CMA Mobile ecosystems market study, Appendix J: Apple's and Google's privacy changes.
[44] Mathur, A., Kshirsagar, M., and Mayer, J. (2021). What Makes a Dark Pattern... Dark? Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, pp. 1–18.

Bundled consent practices may also be used in conjunction with the harmful nudge and sludge techniques described above to make it easier for users to consent to all personal data processing activities and more onerous to exercise more granular control over their consent.

Example: A firm offers multiple distinct services to users. As part of its account sign-up process, it asks users to provide a single consent to the processing of their personal data for use in personalising the services they receive (such as personalised recommendations and personalised advertising), as well as to set cookies for various purposes, including some not directly related to the personalisation of the account. The user can therefore consent to all the services offered by that company being personalised and cookies being set, or refuse consent for all of them.

The user can change the individual consents at a later date in their account settings. However, by presenting the bundled option initially, the company increases the likelihood of users consenting to all processing activities and reduces the chances that they will withdraw that consent at a later time.



ICO concerns: Consent for separate processing activities needs to be "specific" under Article 4(11) of UK GDPR, and Article 7(4) is clear that consent should

not be bundled up as a condition of service unless it is necessary for that service.[45] Bundled consent is therefore more likely to be invalid than unbundled, granular consent options because it is unlikely to be "specific" and may not be fully "informed", thereby increasing the risk of infringing the "lawfulness" requirements of Article 5(1)(a).[46]

In this particular example, consent to set cookies which are not necessary for the personalisation of the account, is also included in the bundled consent. Again, this consent is likely to be invalid for the purposes of PECR Regulation 6.

CMA concerns: Bundling practices can result in poor consumer outcomes by limiting users' freedom of choice. Bundling consent for different agreements (such as Terms and Conditions for using a service, Privacy Policy, Data Policy and Cookie Policy) can also reduce the salience and user awareness of the data processing being consented to. This can restrict users' ability to make informed and effective choices about the uses of their personal data when receiving services.

Competition concerns may arise where certain businesses use such practices to bundle consent for data sharing across all their first-party services, thus leading to greater extraction of user data. While any competitive advantages this data provides can improve the value of the product or service provided to consumers, it can also decrease competitive pressures leading to excessive market power.[47] Where businesses with substantial market power that provide multiple services can bundle their services, this can also result in them leveraging their existing market position to enter related markets and increase barriers for rivals in those markets.

Default settings

When designing "default settings", firms apply a predefined choice that the user must take active steps to change. This can include default settings

[45] Article 7(4) of the UK GDPR says: "When assessing whether consent is freely given, utmost account shall be taken of whether…the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract". Recital 43 says: "Consent is presumed not to be freely given…if the performance of a contract, including the provision of a service, is dependent on the consent despite not being necessary for such performance."

[46] In some limited circumstances you might be able to overturn this presumption that bundled consent is not freely given and argue that consent might be valid even though it is a precondition and the processing is not strictly necessary. You need to be able to demonstrate a very clear justification for this, based on the specific circumstances. See ICO guidance "What is valid consent?".

[47] CMA research paper Evidence Review of Online Choice Architecture and Consumer and Competition Harm.

(including privacy or security features), default choices (such as automatically selected add-ons or pre-ticked boxes), default brands (like the browsers or other apps that come pre-installed with electronic devices) or automatic renewal of subscriptions by default. Default settings reduce user friction which may align with user preferences, but can also be used strategically by firms to reduce the ability of users to make effective choices.

A user can be dissuaded from changing the default setting because they need to dig deep into a service's settings to make adjustments, or even need to contact the service via a different means, such as telephoning to cancel a recurring subscription (i.e., using "sludge" techniques as described above to discourage individuals from changing the default settings).

Defaults are one of the strongest and most reliable practices that influence user behaviour. They are effective – and also concerning – for a number of reasons:

- They require less effort than making an active choice.[48] They leverage users' status quo bias to do nothing or maintain a current/previous decision, which means that users who are in a hurry, not interested, or who are more focussed on other factors are more likely to stick with a default than to change it.
- A default might imply endorsement or a recommendation by the firm, or that most users have chosen it.[49]
- Defaults may lead users to act as if they have already chosen the default option (called the "endowment effect") and, consequently, they use the default as a reference point to construct their preferences.[50]

In fact, defaults are so powerful that, even when users are told they are about to be defaulted to a random choice, they can strongly influence important decisions.[51] A meta-analysis of studies into defaults has shown that a pre-

[48] Smith, N. C., Goldstein, D. G., & Johnson, E. J. (2013). Choice without awareness: Ethical and policy implications of defaults. Journal of Public Policy & Marketing, 32(2), 159-172

[49] Jachimowicz, J. M., Duncan, S., Weber, E. U., & Johnson, E. J. (2019). When and why defaults influence decisions: A meta-analysis of default effects. Behavioural Public Policy, 3(2), 159-186

[50] Dinner, I., Johnson, E. J., Goldstein, D. G., & Liu, K. (2011). Partitioning default effects: why people choose not to choose. Journal of Experimental Psychology: Applied, 17(4), 332.

[51] Loewenstein, G., Bryce, C., Hagmann, D., & Rajpal, S. (2015). Warning: You are about to be nudged. Behavioral Science & Policy, 1(1), pp. 35-42

selected default option is on average 27% more likely to be chosen out of two options than if there were no default option.[52]

Example: A social network allows users to choose how widely content they post is visible on the platform – either not at all (i.e., entirely private), with friends only (i.e., a restricted set of other people) or everyone with an account (i.e., the content is visible to anyone else using the social network). By default, the user's posts can be viewed by everyone, and they must go into their account settings to make their content more private if they wish to do so. Most users are unlikely to do this (or may not even know that they can), thereby increasing the risk of their personal data being made available more widely and used without their knowledge or understanding.

ICO concerns: Article 25 of the UK GDPR requires a "data protection by design and default" approach to the processing of personal data.[53] While Article 25 of UK GDPR does not require firms to adopt a "default to off" approach, they must consider the circumstances of their processing and the risks posed to

[52] Jachimowicz, J. M., Duncan, S., Weber, E. U., & Johnson, E. J. (2019). When and why defaults influence decisions: A meta-analysis of default effects. Behavioural Public Policy, 3(2), pp. 159-186; Smith, N. C., Goldstein, D. G., & Johnson, E. J. (2013). Choice without awareness: Ethical and policy implications of defaults. Journal of Public Policy & Marketing, 32(2), pp. 159-172.

[53] See ICO guidance Data protection by design and default.

individuals. Article 25 also requires firms to ensure that "…by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons". Therefore, in many cases (such as the above example) it will be hard for firms to argue that more intrusive settings should be on by default. Failing to comply with Article 25 also increases the risk of breaching other provisions, such as the "fairness" principle in Article 5(1)(a) and the data minimisation requirements of Article 5(1)(c).

It is also unlikely that consent obtained via default settings (i.e., assuming consent on the basis that the individual has not changed their settings from the default without confirming this choice) will be valid, because individuals must take a positive action to indicate their consent. This could lead to infringement of the lawfulness principle of Article 5(1)(a) if relying on consent as a basis for processing because an individual has not changed the default setting, and infringement of Regulation 6 of PECR if relying on unchanged default settings as consent to set non-essential cookies.

CMA concerns: The use of defaults can lead users to make choices about their personal data that may not be in their best interests, for example, sharing more data than they would like to when receiving services or inadvertently enrolling into auto-renewing subscription plans.[54] The CMA has considered the impact of defaults in consumer choices in various areas such as mobile browsers[55], data privacy[56], search engines[57], auto-renewing anti-virus software subscriptions[58] and online video-gaming.[59] Once users are defaulted into a certain setting or product, changing the default option might require them to undertake multiple steps which may not be obvious or intuitive (i.e. sludge).[60]

Default options can also restrict users' ability to shop around or explore alternative products and services, which may benefit incumbent businesses

[54] CMA discussion paper Online Choice Architecture: How digital design can harm competition and consumers.
[55] CMA Mobile ecosystems market study, Appendix G: pre-installation, default settings and choice.
[56] CMA Online platforms and digital advertising market study final report.
[57] CMA Online platforms and digital advertising market study final report.
[58] CMA consumer enforcement case – Anti-virus software.
[59] CMA consumer enforcement case – Online console video gaming.
[60] For instance, the CMA's Online platforms and digital advertising market study noted that data and privacy control settings on social media platforms can be difficult to access thus encouraging consumer inertia to the default settings. See Online Platforms and Digital Advertising Market Study. Appendix K: consumer controls over platforms' data collection. The CMA's Mobile ecosystems market study also found that the process for changing the default browser within device settings on both iOS and Android mobile devices can involve a number of potentially complex steps which could discourage users from changing default browser settings. See Mobile ecosystems market study, Appendix G: pre-installation, default settings and choice architecture for mobile browsers.

that acquire the least active customers or the most useful data first.[61] The use of defaults in markets with network externalities can then make it harder for rivals to compete. Businesses can also leverage their market power to secure default positions for their products and services which can create barriers for expansion for rival providers.

Like nudges and biased framing, it is important to recognise that default settings are not always bad. If the default settings are those that protect a user's privacy, for example by defaulting optional data sharing to off and requiring an individual to make a positive change to enable it, this can be positive for privacy. The ICO's Age appropriate design code requires that when designing services for children, settings should be set to "high privacy" by default (unless the firm can demonstrate a compelling reason for a different default setting, taking account of the best interests of the child).[62]

[61] CMA discussion paper Online Choice Architecture: How digital design can harm competition and consumers.
[62] See ICO guidance Age Appropriate Design Code Standard 7 - Default settings.

4. Supporting good Online Choice Architecture practices

Given the harms that OCA practices can create from a data protection, competition and consumer protection perspective, both the ICO and CMA are keen to support firms in adopting and maintaining good OCA practices. Supporting good practice can mitigate data protection harms and compliance risks, as well as help avoid the consumer detriment and weakening of competition that can arise when OCA is used poorly.

Below are questions that firms should consider to inform the OCA design they employ when seeking to engage users about how their personal data is processed. Factoring in these questions into OCA design – in the context of the OCA practices featured in this paper and more broadly – will support good practice OCA that can drive pro-privacy and pro-competition outcomes in digital markets.

1. Put the user at the heart of design choices

Are firms building their interfaces around the user's interests and preferences?

Choice architecture and default settings should be designed in a way that **reflects users' interests**. Where interventions relating to user prompt design and user data are being explored by firms, it is beneficial for these to enhance user control and ability to exercise their privacy preferences.

2. Use design that empowers user choice and control

Are firms helping users to make effective and informed choices about their personal information, and putting them in control of how it is collected and used? Is the information clear and not misleading?

OCA should be designed in a way that supports the provision of **easy to understand, balanced information** about what personal data is collected and how it is used, helping users to make **meaningful, freely given decisions** over whether to accept the terms offered about the processing of their personal data. Information should be provided in a way that ensures users can comprehend the choice they face **and**

enables them to make effective decisions, without being confused or overloaded with information.[63]

3. Test and trial design choices

Do firms use testing and trialling to ensure OCA design is evidence-based?

The design of OCA practices is best informed through **testing of behaviour as well as consumer comprehension, experience and feelings of control**. Testing can involve a variety of methods such as A/B tests[64], online experiments[65], customer surveys, usability testing[66], and user interviews.[67] Such testing helps to understand how harm occurs and mitigates the risks of poor consumer outcomes. This can inform the development of responsible OCA practices which enable effective user choices. The CMA has recently published high-level principles as to when it will use field[68] and online experiments, and best practice as to how they can be conducted.[69] We also note that the CMA's proposed new statutory powers, under the Digital Markets, Competition and Consumers Bill will enable it to order trialling when exercising certain market investigations and digital market functions.[70]

[63] Recital 32 of the UK GDPR makes clear that electronic consent requests must not be unnecessarily disruptive to users. ICO guidance outlines the importance of giving some thought to how best to tailor consent requests and methods to ensure clear and comprehensive information without confusing people or disrupting the user experience – for example, by developing user-friendly layered information and just-in-time consents. See ICO guidance on "What is valid consent?".

[64] Randomised experiments run on websites to test the effect of small changes in user experience. See Experiments at the CMA: How and when the CMA uses field and online experiments.

[65] Online experiments involve recruiting people to participate in an online task, where they are randomly assigned to be exposed to interventions, and their decisions, recall or comprehension are measured. See Experiments at the CMA: How and when the CMA uses field and online experiments.

[66] A user research method where participants are asked to perform tasks using one or more user interfaces while the researcher observes the participant's behaviours and records their feedback. See Nielsen Norman Group Usability Testing 101.

[67] A user experience research method where users are asked questions about a topic of interest. See Nielsen Norman Group User Interviews: How, When, and Why to Conduct Them.

[68] Field experiments involve randomly assigning people to a control group, which gets business as usual, and one or more treatment groups, who are exposed to an intervention under investigation.

[69] See CMA guidance Experiments at the CMA: How and when the CMA uses field and online experiments.

[70] The Digital Markets, Competition and Consumers Bill gives the CMA new, targeted powers to drive competition and protect consumers. For more details, see the Digital Markets, Competition and Consumers Bill.

4. Comply with data protection, consumer and competition law

Have firms considered the data protection, consumer protection and competition law implications of the OCA practices they are employing?

As outlined above, depending on their context, OCA practices can undermine consumer choice and potentially reduce competition and innovation. In some cases, **OCA practices may break the law – whether data protection, consumer protection or competition law**. Firms should ask themselves whether their OCA practices could be unfair to users or anti-competitive (for example, by giving themselves an unfair advantage over their competitors). Firms should seek to ensure that their OCA practices relating to personal data processing always comply with competition, consumer protection and data protection requirements.

We encourage stakeholders to act on the joint positions in this paper. These positions are based on existing guidance and publications of the two regulators, and do not supersede or reopen existing legal guidance. In this context, we would welcome views on how effective the examples and steers outlined in this paper are at informing OCA design practices which relate to the processing of personal data. Views on testing and trialling, and technology for detecting harmful OCA practices[71], are also welcome.

The ICO and CMA invite stakeholders to get in touch if interested in participating in further engagement with us on this paper, including a joint ICO-CMA workshop in the autumn about good practices for the design of privacy choices online. We encourage stakeholders invested in the process for designing choices related to the use of consumers' personal information, such as UX designers, information architects and firms themselves, to register interest at:

digitalregulationcooperation@ico.org.uk

[71] The 2023/24 DRCF workplan sets out that DRCF regulators will introduce more practical forms of technical collaboration across regulators, to realise the full benefits of regulatory and supervisory technologies, which can increase our productivity and effectiveness.

Annex 1 – ICO legal frameworks

Legal requirements

The following data protection and privacy laws overseen by the ICO are relevant to the use of OCA and the contents of this paper:

- the UK General Data Protection Regulation (UK GDPR);
- the Data Protection Act 2018 (DPA 2018); and
- the Privacy and Electronic Communications Regulations 2003 (PECR).[72]

Under the UK GDPR and DPA 2018, firms **must** consider data protection and privacy issues upfront in everything it does. Firms **must** bake in privacy considerations from the design stage throughout the product development lifecycle. We may ask firms to demonstrate how they have done this, if appropriate.

UK GDPR sets out seven key principles:

- lawfulness, fairness, transparency;
- purpose limitation;
- data minimisation;
- accuracy;
- storage limitation;
- integrity and confidentiality (security); and
- accountability.

These principles lie at the heart of UK GDPR, informing everything that follows, and are key to firms' compliance with the legislation's detailed provisions. The principles should therefore underpin firms' design approach.

UK GDPR also gives everyone rights over how their personal information is used. These individual rights include a right to:

- be informed;

[72] For more specific information on compliance with these pieces of data protection legislation, please see the ICO's Guide to Data Protection and Guide to Privacy and Electronic Communications Regulations.

- access and receive a copy of their personal data;
- have inaccurate data rectified;
- not be subject to automated decision-making and profiling; and
- have personal data erased.

Firms which act as controllers **must** ensure people can exercise these rights. Thoughtful design helps people have a good experience while doing this.

PECR sits alongside UK GDPR. If you send electronic marketing or use cookies or similar technologies, you **must** comply with PECR, alongside the UK GDPR. For more information on PECR, please see the ICO's Guide to PECR[73].

Specific laws and guidance

The OCA practices outlined in this paper can often increase the risk of infringing the following regulatory provisions (relevant guidance is linked below):

- Article 5(1)(a) of the UK GDPR requires personal data to be processed fairly and in a transparent manner (the "lawfulness, fairness and transparency principle"). This principle can be infringed where an OCA practice unfairly exploits a person's biases or does not present information in a way that gives equal weight to risks and benefits of a decision. This can lead to personal data processing that is unfair and not fully transparent to users.

  Article 5(1)(a) also requires personal data to be processed "lawfully". As well as being generally compliant with other laws, the processing must satisfy one of the "lawful bases" listed within Article 6 of the UK GDPR to comply with this requirement, one of which is consent. Where consent is relied upon, it must be valid consent (see next point on Article 4(11) and Article 7).
- Articles 4(11) and 7 of the UK GDPR respectively define consent and set out the conditions for relying on consent as a lawful basis under the UK GDPR. This includes that consent be freely given, specific, informed and be as easy to withdraw as it is to give. Where firms rely on consent as their lawful basis for processing, but users are asked to give that consent using OCA practices that do not meet this standard – for

[73] See ICO guidance Guide to Privacy and Electronic Marketing Communications.

example, because they put pressure on users to give consent or make it harder to withdraw consent than it is to give – the consent may not be valid and therefore lead to firms not having a valid lawful basis to process the personal data in question. This, in turn, would infringe the lawfulness requirement in Article 5(1)(a) set out above.

- Regulation 6 of PECR requires firms to obtain consent to the UK GDPR standard in order to set cookies or other similar technologies (except in certain specific circumstances). Firms therefore also risk contravening Regulation 6 of PECR when users are asked to give consent to cookies or other similar technologies using OCA practices that do not meet the standard of consent set out in the UK GDPR.
- Article 5(1)(c) of the UK GDPR requires personal data to be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (the "data minimisation principle"). This principle can be infringed where an OCA practice leads to the collection of more personal data than is necessary. This principle applies alongside requirements under Article 25 of the UK GDPR that requires data controllers to take a "data protection by design and default" approach to their personal data processing. This requires data protection principles, such as data minimisation, to be considered at the design phase of any system, service or product and then throughout its lifecycle.

This should not be taken to mean that all uses of OCA practices will automatically infringe these provisions, or that their misuse will not cause infringements of other provisions within data protection law. Instead, the ICO considers these provisions to be the ones that are most commonly at risk of being infringed when OCA practices are used to distort or steer consumer choices in harmful ways.

This paper should also be read in conjunction with ICO guidance that set out our positions on relevant OCA practices and interface design:

- Privacy in the product design lifecycle
- Age appropriate design code (or Children's Code)[74] and The Children's Code design guidance
- Data protection by design and default

[74] Whilst the Age Appropriate Design Code focusses on protecting children online, many of the key design principles are applicable to privacy friendly design of online services more widely.

- Guidance on Principle (a) of the UK GDPR: Lawfulness, fairness and transparency
- Guidance on Consent
- Guidance on the use of cookies and similar technologies.

Annex 2 – CMA legal requirements

Consumer law

Consumer law and data protection law are generally complementary and, in many senses, pursue similar objectives, in particular promoting transparency and genuine, informed choices. The CMA enforces a range of consumer protection law[75] but, for the purposes of this joint position paper, the most relevant regulations are the Consumer Protection from Unfair Trading Regulations 2008 (SI 2008/1277) (CPRs) and Part 2 of the Consumer Rights Act 2015 (CRA),[76] which implement the Unfair Commercial Practices Directive[77] (UCPD) and Unfair Contract Terms Directive[78] (UCTD) respectively, and the Consumer Contracts (Information, Cancellation and Additional Charges) Regulations 2013 (CCRs).

CPRs

Broadly speaking, the CPRs prevent firms (described as "traders" in the CPRs) from treating consumers unfairly. A commercial practice is governed by the CPRs if it is directly connected with the promotion, sale or supply of goods or services (both described as 'products' in the CPRs) to consumers. As such, they apply to a wide range of commercial practices such as advertising, marketing, sales, supplies and after-sales services.

The CPRs apply not just to "paid for" services but may also apply to services provided in exchange for consumers' personal data, just as if they had paid a monetary price. This may particularly apply where a firm processes consumer data in breach of data protection rules for direct marketing purposes or any other commercial purposes such as profiling, personal pricing or as part of data collection practices to support its commercial operations.[79]

Regulations 3, and 5 to 7 of the CPRs prohibit unfair practices which have, or are likely to have, an effect on the transactional decisions of the average

[75] See CMA guidance Consumer protection enforcement guidance: CMA58.
[76] Businesses may also need to comply with the requirements of other parts of the CRA.
[77] See Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business -to-consumer practices in the internal market.
[78] See Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts.
[79] See also the European Commission, Commission Staff Working Document: Guidance on the implementation / application of Directive 2005/29/EC on Unfair Commercial Practices, p. 25 and SWD (2016) 163 final p. 24.

consumer.[80] The average consumer is generally assumed to be reasonably well informed and reasonably observant and circumspect. Average does not mean a statistically average consumer. Where a commercial practice is targeted at a particular group or it is reasonably foreseeable that a group of consumers will be particularly vulnerable to that practice, then the average consumer refers to the average member of that group.

Regulation 3 contains a general prohibition on unfair commercial practices. This prohibits practices that contravene the requirements of professional diligence (meaning honest market practice and good faith) and materially distort or are likely to materially distort the economic behaviour of the average consumer. Failure to comply with data protection legislation could contravene the requirements of professional diligence.

Regulation 5 prohibits misleading actions, which occur when a business gives consumers false information (about a wide range of things listed in the CPRs) or is deceptive in the presentation of that information even if it is factually correct, and causes or is likely to cause the average consumer to take a different decision.

Regulation 6 prohibits misleading omissions, which occur when businesses fail to give consumers the information that they need to make an informed choice in relation to a product. This includes practices which omit or hide 'material information', or provide it in an unclear, unintelligible, ambiguous or untimely manner, and the average consumer takes, or is likely to take, a different decision as a result.

Regulation 7 prohibits aggressive commercial practices. These are practices that, in the context of the particular circumstances, put unfair pressure on consumers, restricting their ability to make free or informed decisions.

The CMA has examined a number of OCA practices in different sectors which involved concerns that these commercial practices may breach the CPRs and has an ongoing programme of OCA enforcement work.[81] Past cases include hotel bookings (concerns included misleading default ranking); secondary ticket sellers (presentation of choice information); online gambling (concerns included 'sludge' practices); cloud computing (default settings); and anti-virus

[80] In addition, there are 31 practices listed in Schedule 1 to the CPRs, which because of their inherently unfair nature, are prohibited in all circumstances.
[81] CMA Online Choice Architecture work.

and online video gaming sectors (concerns around the use of defaults auto-renewals in subscription contracts).[82, 83]

Cases decided under the UCPD from which the CPRs derive, and which may be relevant to OCA practices include:

- WhatsApp – in 2017 the Italian competition authority (the AGCM) fined WhatsApp €3,000,000 for the use of aggressive commercial practices, in particular putting unfair pressure on consumers to accept WhatsApp's new terms of use (which included pre-selected consent to share personal data with Facebook for commercial and advertising purposes). [PS10601, dated 11 May 2017]

- In 2018 the AGCM fined Facebook a further €5,000,000 for the use of aggressive commercial practices, in particular sharing existing user's data with third party websites and Apps for commercial practice without express and prior consent. [PS11112, 29 November 2018]

A breach of data protection law will not automatically constitute a breach of consumer law. However, the CMA will take this into account when assessing the overall unfairness of commercial practices under the CPRs.

Part 2 of the CRA

Part 2 of the CRA applies to both consumer contracts and consumer notices[84] and requires the terms in consumer contracts and consumer notices to be fair and, if written, transparent.

A term in a consumer contract or consumer notice is unfair if, contrary to the requirement of good faith, it causes a significant imbalance in the parties' rights and obligations under the contract, to the detriment of the consumer (the "fairness test").

[82] For further details see section 2.4 of CMA discussion paper Online Choice Architecture - How digital design can harm competition and consumers.
[83] In addition, the CMA has initiated a programme of work tackling harmful online selling practices such as misleading urgency and price reduction claims.
[84] A consumer notice is wording that may not form part of a contract but which relates to the same kind of issues that would be dealt with in a contract – for instance the rights or obligations between a business and a consumer.

Generally, contract terms or notices are unfair if they put the consumer at an unfair disadvantage. The "fairness test" starts by asking whether the wording used tilts the rights and responsibilities between the consumer and business too much in favour of the business. The test is applied by looking at the words and how they could be used. It takes into consideration what is being provided, how a term relates to other terms in the contract and all the circumstances at the time the term was agreed.

The CRA illustrates what "unfairness" means by listing some types of terms that may be unfair in Schedule 2 to the CRA (known as the "Grey List"). Terms like those included in the Grey List are not necessarily unfair, but concerns about the fairness of a term are likely to arise where it has the same purpose, or can produce the same result, as the types of terms listed in the Grey List. The Grey List is not exhaustive, which means that terms that do not appear on it may still be unfair.

Examples of cases decided in relation to the UCTD which involved consumer data include:

- WhatsApp – in 2017 the Italian competition authority (the AGCM) found a number of WhatsApp's terms of use unfair. These included terms which gave WhatsApp the right to introduce changes without reason and without informing the consumer and the tacit approval to obtain consent through consumer inertia. [CV154, dated 11 May 2017]

- Facebook – in 2019 a French court fined Facebook €30,000 for using unfair terms. These included terms which allowed Facebook to retain, use and resell user's data, even after their account had been closed, and to unilaterally change the terms and conditions without informing users. [Paris TGI judgment, 9 April 2019]

CCRs

Among other matters, the CCRs set out the information that should be provided to consumers before entering into a "distance contract" (which includes contracts entered into online) and the confirmations that should be provided after the contract is entered into. In addition, the CCRs set out requirements that apply in other situations in which contracts are entered into (such as "off-premises" and "on-premises"), as well as rules regarding consumers' cancellation rights.

The CCRs require the consumer's express consent to additional payments, and specifically provide that using pre-ticked boxes on a website for additional payments do not meet this requirement. The CCRs also include certain requirements to make consumers aware when there is an obligation to pay.

Competition law

Competition Act 1998

The CMA enforces competition law under rules set out in the Competition Act 1998 (CA98). Competition law protects businesses and consumers against anti-competitive agreements or behaviours under Chapter I of the CA98, and against abuse of dominance under Chapter II of the CA98.[85] These prohibitions mirror the provisions of Article 101 and 102 of the Treaty on the Functioning of the European Union (TFEU) respectively which is enforced by the European Commission.[86]

For example, in Google Search (Shopping), the European Commission found that "the more favourable positioning and display by Google in its general search results pages of its own comparison shopping service compared to competing comparison shopping services, was an abuse of dominance".[87] The CMA also identified concerns with OCA practices in both its Online Platforms and Digital Advertising Market Study[88] and its Mobile Ecosystems Market Study[89].

Digital Markets, Competition and Consumers (DMCC) Bill

The DMCC Bill was introduced to Parliament on 25 April 2023.[90] It proposes a new, targeted regime enforced by the CMA, to enhance competition in digital markets.

As part of the DMCC Bill, the DMU will be able to designate firms which meet statutory criteria as having "Strategic Market Status" in respect of a particular digital activity. Among other things, this designation will enable the DMU to:

[85] See CMA guidance The CMA's investigation procedures in Competition Act 1998 cases: CMA8.
[86] The CMA performs a range of other competition functions, including merger control, market studies and market investigations.
[87] See European Commission Decision in case AT.39740 Google Search (Shopping).
[88] CMA Online platforms and digital advertising market study.
[89] CMA Mobile ecosystems market study.
[90] See Digital Markets, Competition and Consumers Bill.

- Step in to set tailored rules on how SMS firms behave and operate in relation to the activity that is the focus of its SMS designation. These rules (or "conduct requirements") will seek to manage the effects of market power and ensure the firm doesn't take advantage of its position to harm competition and consumers. The CMA can impose conduct requirements to promote objectives of fair trading, open choices and trust and transparency.

- Make pro-competitive interventions, for example to seek to address the source of an SMS firm's market power in the relevant digital activity, and to open up greater competition and innovation in the markets in question. Prior to the DMCC Bill's introduction, the Final Report of the CMA's Online Platforms and Digital Advertising Market Study[91] (published in July 2020) recommended potential principles of "fairness by design" that the DMU could require designated businesses to apply when presenting choices to consumers about sharing their data for personalised advertising.

The DMCC Bill also proposes changes to how consumer law may be enforced and to certain aspects of substantive consumer law, including proposals in respect of unfair commercial practices which would replace the CPRs, and makes certain procedural changes to the CMA's existing competition powers.

CMA Online choice architecture publications

This paper should also be read in conjunction with other publications the CMA has released separately that set out its positions on OCA practices and interface design:

- Online Choice Architecture: How digital design can harm competition and consumers
- Guidance for business on using urgency and price reduction claims online
- Online platforms and digital advertising market study
- Mobile ecosystems market study, including Appendix J: Apple's and Google's privacy changes and Appendix K: consumer experiences of app purchases and auto-renewing subscriptions to apps sold through the app stores.

[91] CMA "Online platforms and digital advertising market study" final report.