Are you afraid of the dark? Protecting children from the harms of dark patterns

Karishma Brahmbhatt, of Counsel, and Steve Wood, Consultant, with Allen & Overy, consider keeping children safe online — and organisations compliant — in an increasingly digital world

The use of frontier technologies such as artificial intelligence has raised many regulatory and industry challenges, but one of the most pressing issues is the safety of children. Across the globe, regulators have been introducing or updating laws and guidance to protect children from online harms. Such laws include the Australian Online Safety Act 2021, the EU Digital Services Act ('DSA'), the UK Online Safety Act 2023 ('OSA'), and the US Children's Online Privacy and Protection Act.

In the UK, the Information Commissioner's Office ('ICO') recently issued guidance on content moderation, in the first in a series of planned publications on online safety technologies. This guidance builds on the ICO's Children's Code ('the Children's Code'), a statutory code of practice under the Data Protection Act 2018 that applies to online services that are likely to be accessed by children. It also supplements the codes of practice and guidance on the OSA issued by Ofcom, the UK's regulator for the online safety regime.

The protection of children online is a complex and multi-faceted issue that involves several regulators with different roles and remits. For example, the UK Competition and Markets Authority ('CMA') — one of the four regulators alongside the ICO and Ofcom that comprises the UK's Digital Regulation Co-operation Forum — issued a joint paper with the ICO shining a spotlight on the use of dark patterns and practices that distort online choice architecture, and the potential harm they cause to consumers (see 'Harmful design in digital markets — key do's and don'ts', in Volume 23, Issue 8 of *Privacy & Data Protection*).

In and of themselves, dark patterns can cause individuals to make unintended, subconscious, and potentially harmful decisions against their best interests. But when those individuals are children — defined in the Children's Code as anyone under the age of 18 — the effect of dark patterns in user interfaces can exacerbate potential harms. One piece of research found that 80% of popular children's apps contained at least one manipulative design feature. Given the growing multi-regulatory focus on children's safety as well as on deceptive user interfaces, the use of dark patterns in online services for children is not an issue to be taken lightly. In practice, a design mis-step could lead to an organisation facing investigations or sanctions from multiple regulators across multiple jurisdictions.

There are a number of laws that contribute to the protection of children from deceptive user interfaces and journeys, including consumer laws such as the EU Unfair Commercial Practices Directive, and laws that govern online advertisements, such as the EU Audiovisual Media Services Directive ('AVMSD').

In this article, we discuss the interplay between the dark patterns and children's safety, and provide an overview of some of the key EU and UK law regulating these areas, such as the GDPR/UKGDPR, the EU DSA, and the UK OSA.

Shining a light on dark patterns

Discussing the issue in the context of social media, the European Data Protection Board ('EDPB') in its Guidelines 3/2022 on Dark patterns in social media platform interfaces ('EDPB's Guidelines') has defined dark patterns as 'interfaces and user experiences implemented on social media platforms that lead users into making unintended, unwilling and potentially harmful decisions in regard to their personal data'. Most definitions of the concept refer to manipulation, deception, coercion or exploitation in the design and wording of the user interfaces; the exploitation of humans' cognitive biases; and the leading of individuals to make decisions unknowingly against their preferences or against their best efforts. It is unsurprising, therefore, that dark patterns are also commonly referred to as 'deceptive design patterns', and 'manipulative designs'.

A 2022 study carried out by the European Commission ('Commission') on dark patterns shows that, as expected, vulnerable individuals are more susceptible to the effects of dark patterns. In one study, the majority of apps assessed and targeted to children aged 3-5 years were associated with manipulative design features, including parasocial relationship pressure, fabricated time pressure, navigation constraints, and use of attractive lures to encourage longer screen-time or purchases — all in addition to advertising-based pressures. The study also showed that children from lower socio-economic backgrounds played with apps that had more manipulative designs.

A 2022 report from the US Federal Trade Commission ('FTC') highlighted concerns about a rise in dark patterns and how they could 'trick and trap' consumers. The FTC's concerns included misleading consumers through disguising ads, making it difficult to cancel subscriptions or charges, and tricking consumers into sharing data. In one FTC enforcement action, an online gaming company was required to pay $245 million to refund consumers in respect of the FTC's findings about its dark patterns and billing practices.

Under the regulatory spotlight

So, how do key EU and UK laws seek to tackle this issue?

The GDPR itself does not explicitly reference the concept of dark patterns, as the term only rose to prominence after the GDPR text was agreed. However, as noted in the EDPB's Guidelines, there are several provisions in the GDPR that are highly relevant, such as:

- the fairness principle in Article 5 (1)(a), which requires personal data to be processed in a fair and transparent manner. By their very nature, dark patterns are likely to infringe this Article;
- the requirement for data protection by design and default under Article 25, which mandates controllers to implement appropriate technical and organisational measures to ensure and demonstrate compliance with the GDPR;
- Article 12 GDPR, which requires that any information must be provided to data subjects in a concise, transparent, intelligible and easily accessible form, using clear and plain language. Dark patterns that obscure or confuse key information are likely to breach this provision;
- the definition of consent under Article 4, which requires a freely given, specific, informed and unambiguous indication of the data subject's wishes. Design interfaces that coerce, mislead or nudge users into giving consent are likely to invalidate it; and
- the accountability principle under Article 5, which requires controllers to demonstrate how the design of their website interfaces comply with the GDPR, including the provisions above, when they relate to personal data processing.

> ***"... with a number of open investigations and the Information Commissioner John Edwards indicating that children's privacy is an ongoing priority, it will be important for online service providers to remain focused on how their services conform with the Children's Code."***

The EDPB's Guidelines also provide some specific guidance related to children, highlighting the risks of 'emotional steering', that can make children feel obliged to share personal data. The EDPB's Guidelines note that Recital 75 of the GDPR explicitly refers to the risks of processing of children's data and the harms that could occur, including physical, material or non-material damage.

European Supervisory Authorities ('SAs') have also been active in issuing guidance and enforcing the GDPR, with a particular focus on valid consent. In 2019, researchers from a German University found that out of a sample of 1,000 German websites, 57% used a dark pattern known as 'nudging' to obtain consent from the user under the GDPR. In the same year, the French SA, the CNIL, issued a report that discussed the importance of user design related to user empowerment, and stated that "the fact of using and abusing a strategy to divert attention or dark patterns can lead to invalidating consent."

In 2022, the EU Consumer Protection Cooperation Network endorsed five key principles of fair advertising towards children that were established by representatives from both consumer authorities and SAs. These principles highlighted the importance of considering the vulnerability of children when implementing online advertising; how marketing should be appropriate and clear for children; and how children should not be targeted or urged to purchase in-app or in-game content.

In 2023, the Irish Data Protection Commission ('DPC') issued a €345 million fine of TikTok in what was the first major GDPR sanction that had focused on dark patterns and children. The DPC focused on the way in which default settings were presented to children, and how they nudged towards more privacy intrusive options. This case illustrates just how seriously EU SAs take the issue of the effect of dark patterns on children.

In the UK, the Children's Code is built around the concept that online services likely to be used by children should be designed with the best interests of children in mind, taking account of different ages and stages of development of child internet users. The Children's Code also builds on Recital 38 of the UK GDPR, which states that 'children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data'.

Standard 13 in the Children's Code is

(Continued on page 6)

(Continued from page 5)

the key provision related to dark patterns. This standard focuses on nudge techniques and states: 'Do not use nudge techniques to lead or encourage children to provide unnecessary personal data or turn off privacy protections.' Guidance on the standard highlights a number of examples of unfair techniques, such as enlarged buttons to proceed online, and nudges towards accepting personalised content and profiling. Guidance also highlights the importance of pro-privacy nudges such as reminders, warnings or rewards for choosing privacy-friendly settings.

To date, the ICO has not taken any enforcement actions based on the Children's Code but, with a number of open investigations and the Information Commissioner John Edwards indicating that children's privacy is an ongoing priority, it will be important for online service providers to remain focused on how their services conform with it.

The role of the EU Digital Services Act and the UK Online Safety Act

The DSA is one of the newest EU laws that directly addresses the issue of dark patterns. Under Article 25 ('Online interface design and organisation'), the DSA specifically prohibits deceptive or nudging techniques, including dark patterns, that could distort or impair a user's free choice. These include giving more visual prominence to a consent option or repetitively requesting or urging users to make a decision. The DSA also empowers the Commission to adopt guidelines to define additional practices that may fall within the scope of dark patterns.

Recital 81 of the DSA highlights the importance of considering design when assessing risks related to the rights of the child, and links the possible risks of online interfaces that intentionally or unintentionally exploit the weaknesses and inexperience of children to addictive behaviour. Combined with the Article 28 requirement for providers of online platforms accessible to children to use appropriate and proportionate measures to ensure a high level of privacy, safety, and security of minors in relation to their service, this makes a powerful set of provisions to enable the Commission to tackle the risks to children from dark patterns.

In addition, the Commission is working on a draft of its own Age-Appropriate Design Code. This code will build on the regulatory framework provided in the DSA to assist with its implementation and will be in line with the AVMSD and the GDPR. A draft of the EU Age-Appropriate Design Code is expected to be issued for consultation late in 2024. Practitioners will be looking to see what it says about dark patterns.

The Commission has already flexed its investigatory powers: within weeks of the DSA coming into force, it opened formal proceedings against TikTok. The proceedings will consider issues related to the protection of children, and the Commission's press releases references "actual or foreseeable negative effects stemming from the design of TikTok's system." While dark patterns are not explicitly mentioned, it seems possible that the DSA dark pattern provisions will be part of the investigation.

The UK's OSA was passed into law in 2023, and we are now in a transitional phase for the legislation. The OSA requires online platforms that host user-generated content or provide search engine services for such content, and that are likely to be accessed by children, to abide by a 'duty of care' and undertake risk assessments (Section 28). These risk assessments will include considerations of how the design of the service affects the level of risk of harm that might be suffered by children. We await further details of how Ofcom will address these issues in the code of practice it issues in relation to children. The code is expected to be published for consultation late in the Spring of 2024.

We can expect Ofcom to consider dark patterns related to children, particularly in relation to the way in which algorithmic and recommender systems are designed. This could include, for example, the way in which children are presented with options and choices for content feeds that are chronological or algorithmically generated.

Other digital regulation

Over the past few years, we have seen references to the potentially harmful effects of dark patterns in a variety of legislation for which the regulation of dark patterns and children's online safety is neither the focus nor the objective.

For example, Recital 38 of the EU Data Act states that 'third parties or data holders should not rely on so-called 'dark patterns' in designing their digital interfaces', and acknowledges that those manipulative techniques 'can be used to persuade users, in particular vulnerable consumers, to engage in unwanted behaviour, to deceive users by nudging them into decisions on data disclosure transactions or to unreasonably bias the decision-making of the users of the service in such a way as to subvert or impair their autonomy, decision-making and choice.'

Similarly, Recitals 15 and 16 of the EU Artificial Intelligence Act ('AI Act') allude to dark patterns when noting that 'AI-enabled manipulative techniques can be used to persuade persons to engage in unwanted behaviours, or to deceive them by nudging them into decisions in a way that subverts and impairs their autonomy, decision-making and free choices'. There is also acknowledgment in the AI Act that AI systems may also otherwise exploit vulnerabilities of a person or a specific group of persons (such as children) due to their age. Whether this trend of explicitly governing the use of dark patterns through a patchwork of digital regulation continues has yet to be seen. What is clear, however, is that organisations should be taking measures to address potential harms to children that may arise from their use of dark patterns on their online consumer interfaces and journeys.

From 'so what?' to 'now what?'

What can organisations do to guard

against the risks of investigations and enforcement actions related to dark patterns?

A key part of a successful mitigation strategy will be a focus on user experience testing, often known as 'UX'. Objective evidence of user testing and how children and other consumers have understood and engaged with an interface can be important documentation to present to regulators. A process of regularly testing when updating interfaces is also important, as is a clear procedure for receiving complaints from users. This user testing should also consider the different ages of children in core user groups, the region in which child users are based, as well as the limitations and capacities of the child users. These measures are important for a wide range of online services, from social media to gaming and retailers used by children. User testing with groups of children will also need to be conducted in accordance with ethical principles. We are now seeing the emergence of third party services, for example the Fair Patterns service, to provide assessment tools to help with the process.

It will also be important that teams who engineer and design online systems used by children are trained about risks of dark patterns and understand how to test and mitigate the risks. Existing design processes and manuals should also be updated to include steps related to dark pattern mitigation.

We are just at the start of the process of understanding how regulators and courts will interact with the concept of dark patterns. New data protection laws must also be monitored; for example, dark patterns are addressed by the recent Colorado, Connecticut, and California privacy laws. It will be essential that practitioners track the implications of new guidance and enforcement actions as they emerge (this journal will track the developments closely). As indicated in the UK by the work of the ICO and the CMA, we can also expect joined-up approaches by regulators across the domains of data protection, consumer protection, competition and online safety.

Karishma Brahmbhatt and Steve Wood
Allen & Overy
karishma.brahmbhatt@allenovery.com
steve.wood@allenovery.com