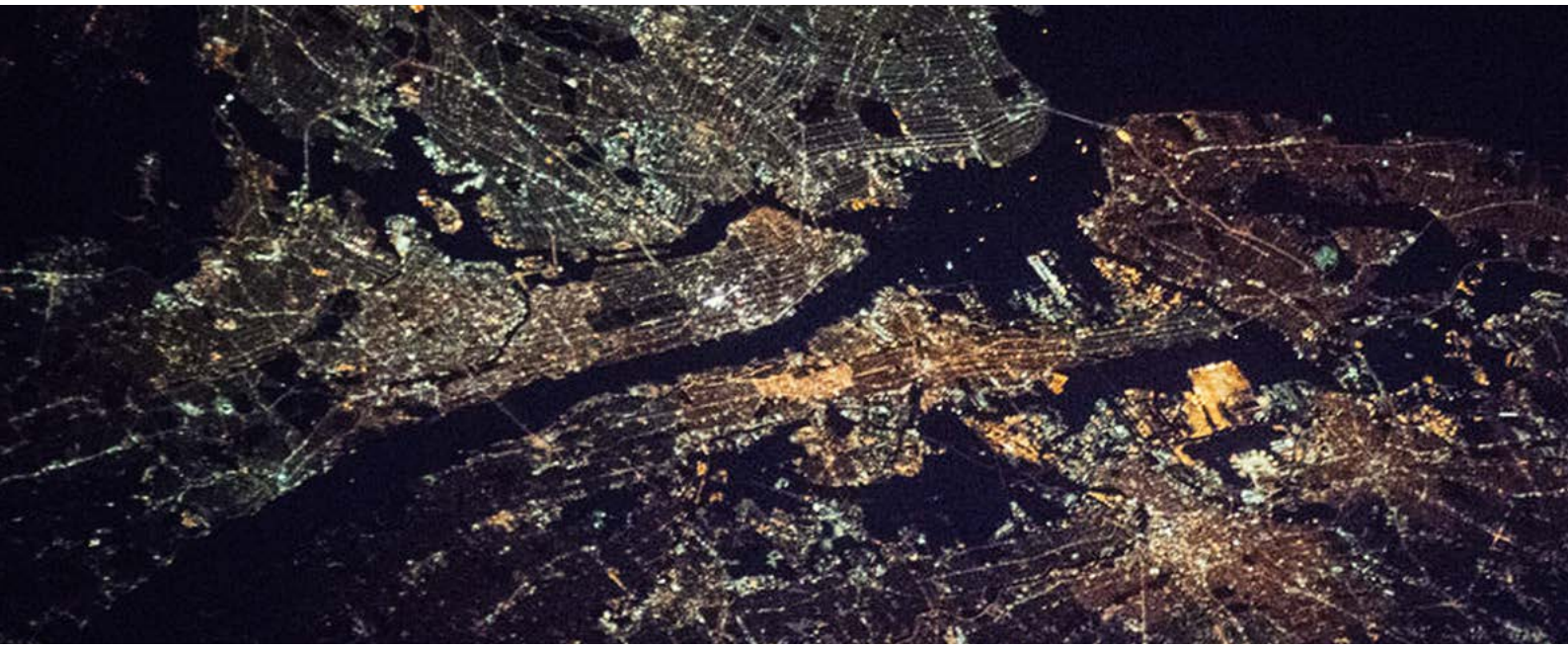
WOMBLE BOND DICKINSON

A regulatory deep dive into ‘dark patterns’

June 2023

GROWING GLOBAL

Contents



What is a ‘dark pattern’?

The term dark patterns was coined in 2010 by UX specialist Harry Brignall. To put it simply, dark patterns are user interfaces designed to ‘trick’, ‘encourage’ or ‘compel’ users into taking certain actions, potentially against users’ wishes.

The information in this publication is accurate as of June 2023.

Increased regulatory scrutiny globally

Increased regulatory scrutiny globally

There has been an increasing focus on dark patterns by the advertising and consumer regulators, including in the UK, EU and US. Recent areas of investigation / focus include:

UK: CMA’s new phase of ‘Online Rip-Off Tip-Off’ campaign. The campaign aims to encourage consumers to “spot and avoid misleading online sales tactics” and to report organisations involved. The CMA’s new poll revealed that 1 in 4 of UK respondents said they had “fallen victim to sneaky online sales tactics”. There are concerns that the cost of living crisis is compounding this problem, with 67% of UK consumers saying that this makes them “more desperate to find a deal”.

UK: CMA’s investigation into Emma Sleep for its pressure-selling tactics through false ‘limited time offers,’ including a countdown timer.

UK: ASA’s decision relating to the use of a ‘flash sale’ timer. The ASA upheld its decision that a ‘flash sale’ timer that was swiftly followed by an additional sale breached the UK Code of Non-broadcast Advertising and Direct and Promotional Marketing.

EU: Screening exercise. The European Commission and Consumer Protection Cooperation Network [1] conducted a screening exercise of 399 online shops of retail traders selling products across a wide range of industries, including apps of 102 of the sites screened. This screening exercise revealed that **“nearly 40% of the online shopping websites rely on manipulative practice to exploit consumers’ vulnerabilities or trick them”**. This highlights the extent of the problem, which is only likely to be further compounded by the use of AI to create more advanced dark pattern practices.

EU: The French data protection authority investigated and fined a big tech company €150million for its use of dark patterns. The dark pattern concerned allowed users to accept cookies easily whilst they were unable to refuse such cookies without difficulty (with several steps) encouraging acceptance out of frustration.

US: The FTC entered into **settlements for more than $245 million** for dark patterns practices that falsely manipulate consumers. The $245m will be used to provide refunds to consumers affected.

Examples of dark patterns

We have included some examples of dark patterns below, some of which were also identified as part of the European Commission and Consumer Protection Cooperation Network's sweeping exercise.

Type	How it operates
 Roach motel	This design provides an easy/straightforward path to get 'in' but a difficult path to get 'out'. For example, the user journey for signing up for online newsletters or subscription services can be much more straightforward than to unsubscribe, pause or cancel. The sweeping exercise identified that there were 54 websites that used language / visual design to encourage consumers towards a particular choice, including subscriptions.
 Misdirection	Arguably the most simple and universal trick when it comes to dark patterns: a website will focus your attention on one thing in order to distract your attention from another. For example, a user feeling inclined to accept 'all cookies' due to flashy bright visuals. The sweeping exercise identified that there were 70 websites found to be "hiding information or making it less visible for consumers".
 Sneaking	Have you ever gone to check out and noticed an additional item in there you didn't add? This may be as a result of the site having 'sneaked' an additional item into your basket.
 Hidden costs	In this instance the price stipulated when viewing an item is much lower than the price when you get to checkout. This is because at the final stage additional costs have been added on top, such as tax and delivery. Companies should always make clear the costs to customers that are additional to the item price (e.g. delivery will be added at checkout) from the outset.
 Pressure	Examples include countdown clocks, repeated notifications encouraging users to do something in the site's interest or 'low stock' alerts.
 Friend spam	When signing up to a new website, for example LinkedIn, individuals are asked to invite friends to the new service. This could be an example of friend spam. A user is asked for the personal details of others (inviting friends via their email) under false pretences – then the website sends spam messages to contacts of the user claiming to be them. As well as causing challenges from a consumer perspective, this also breaches data privacy laws and contravenes the relevant ICO guidance on 'refer a friend' and 'tell a friend campaigns.

Navigating the regulation of dark patterns

The overview above shows that there are numerous types of dark patterns, which you would expect to be heavily regulated. However, surprisingly, regulation has not quite caught up with putting a stop to these practices. Aside from ‘sneak into basket’ (which is now illegal), the only way to regulate other dark patterns is applying certain regulation indirectly.

We have summarised the key elements of the UK and EU regulatory landscapes below.

United Kingdom

Under current UK law there are no laws that specifically reference dark patterns. However certain consumer laws could be breached indirectly, including:

- **UK GDPR and DPA 2018** (in force) – data protection laws are intrinsically interlinked to the use of dark patterns where personal data is involved, for example, where dark patterns are potentially used to capture users’ consent. Core data protection principles, like data protection by design, are key when considering the impact of technologies and whether they are capable of manipulating individuals.
- **ICO’s Guidance** – specific guidance on ‘nudge techniques’, including in relation to children the possibility of using ‘pro-privacy nudges’ where appropriate.
- **Consumer Rights Act 2015** (in force) – where dark patterns are principally used to encourage/make consumers enter into contracts for goods and / or services, they are at risk of falling foul of the CRA 2015.
- **Consumer Protection from Unfair Trading Regulations 2008** (in force) – again, these apply where the actions taken by the organisation are likely to result in an unfair outcome for the individual. These will apply when the aim of the dark pattern is to influence the customer’s financial decisions in some way (e.g. sneak into basket, hidden costs).
- **Consumer Contracts (Information, Cancellation and Additional Charges) Regulations 2013** (in force) – these provide customers with a cooling off period of 14 days after purchase.

The CMA is taking a hard-line approach to dark patterns, including conducting the Online Rip-Off Tip-Off campaigns and launching its first investigation into dark patterns. These actions are likely to be the starting point for further investigation into and enforcement against dark patterns in the UK.

European Union

The EDPB has defined 6 categories of dark patterns: (1) overloading; (2) skipping; (3) stirring; (4) hindering; (5) fickle; and (6) left in the dark.

- **GDPR** (in force) – as above, data protection laws are intrinsically interlinked to the use of dark patterns where personal data is involved.
- **EDPB's Guidelines** – specific guidelines on **dark patterns in social media platform interfaces**. These guidelines highlight the importance of adopting a data protection by design and default approach before launching interface design.
- **Digital Services Act (DSA)** (in force) – from 17 February 2024 (earlier for the largest of online platforms), the Digital Services Act (DSA) has set out an express ban on dark patterns. More specifically, Article 25 of the DSA states: "Providers of online platforms shall not design, organise or operate their online interfaces in a way that deceives or manipulates the recipients of their service or in a way that otherwise materially distorts or impairs the ability of the recipients of their service to make free and informed decisions".
- **AI Act (proposed)** – the proposed AI Act prohibits the use of dark patterns within AI systems.
- **Data Act (proposed)** – the proposed Data Act describes dark patterns as design technique or mechanism that: "push or deceive consumers into decisions that have negative consequences for them. These manipulative techniques can be used to persuade users, particularly vulnerable consumers, to engage in unwanted behaviours, and 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 a way that subverts and impairs their autonomy, decision-making and choice." **Important – the prohibition in the DSA only applies to practices that are not already covered by the UCPD or GDPR.**

United States

The FTC's April 2021 workshop **'bringing dark patterns to light'** investigated manipulative user interface designs on websites and Apps. Dark patterns continues to remain an enforcement priority for the FTC:

- The FTC released its 'Bringing Dark Patterns to Light' report in September 2022 illustrating that organisations are increasingly using sophisticated design practices to trick or manipulate consumers into buying products or services or giving up their privacy. The FTC's report identified what it considered to be four of the most common uses of dark patterns: (1) misleading consumers / disguising adverts (2) burying key terms; (3) subscription cancellation barriers / charges; and (4) tricking / manipulating users into providing data.
- The FTC entered into settlements for more than $245 million in December 2022 for dark patterns practices that falsely manipulate consumers.

In recent months, multiple states have also begun to legislate directly and consider more widely the impact of dark patterns. Most notably:

- **California Privacy Rights Act (CPRA)** (in effect since January 2023) – The CPRA has redefined consumer consent, stipulating that "agreement obtained through the use of dark patterns does not constitute consent". The CPRA defines a 'dark pattern' as "a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice, as further defined by regulation." Furthermore, the legislation directs that regulations regarding the sale or sharing of personal information must ensure that a business obtaining consumer consent to such sale or sharing "does not make use of any dark patterns".
- **The Colorado Privacy Act** (will have effect from July 2024) – This Act outlines that a consumer's consent is not valid if obtained through the use of 'dark patterns'.
- **The Ninth Circuit Court of Appeals decision** also questioned whether placement and linking to a company's privacy policy or website terms and conditions could be considered an unlawful dark pattern.

Dark patterns and AI – a double edged sword

- **Development of dark patterns.** AI can be used to develop complex dark patterns that are difficult to detect. AI developed with embedded dark patterns (where the AI's learning capabilities involve dark patterns) intend to alter the user's behaviour over time to make them think the dark pattern-related decisions are their own, rather than influenced by the AI. The added layers of complexity might mean AI dark patterns require a different legislative framework and it will be interesting to see how regulating the use of AI dark patterns is considered in the future.
- **Development of new technologies to counter dark patterns.** Whilst in its infancy, academic research is ongoing into machine learning technology capable of detecting and alerting users on the presence of dark patterns. For example, a team at Heidelberg University, Germany, developed and trained a prediction model to spot dark patterns in cookies. Evidently, there will be a market for dark pattern-spotting tools to help both users and enforcement agencies crackdown on such behaviour against breaching organisations.

The proposed EU's proposed AI Act, considered further in our AI Roadmap, expressly prohibits the use of dark patterns within AI systems. Consequently, developers, manufacturers and organisations deploying AI systems would be prohibited from utilising dark patterns once the proposed AI Act comes into force.

Key takeaways

Regulatory bodies are taking action on the use of dark patterns globally. This trend is likely to continue as further guidance is published and laws come into force

Adopting a ‘privacy by design’ approach from the outset of projects, with a particular focus to the end-user’s journey is likely to be key to avoiding regulatory investigations and penalties

The impact of the new Digital Service Act (DSA) is yet to be seen in the dark patterns space, however, there are concerns that this could be limited given that it only bites in situations where the General Data Protection Regulation and Unfair Commercial Practices Directive do not apply. Our prediction is that this will place greater pressure on the data protection and consumer regulators to enforce the existing rules and issue more granular guidance.

AI is being used as a double-edged sword in the dark patterns space: on the one hand, it is being used as a key tool to spot and control dark pattern behaviour, on the other, it is being used to develop new dark patterns that are much harder to spot.

Footnotes:

[1] Formed of the national consumer protection authorities of 23 EU Member States, Norway and Iceland.

[2] There is no ‘one way’ of categorising ‘dark patterns’ and there are several taxonomies.

Timeline

EU / US/ UK

February 2022
CMA launched its Online Rip-Off Tip-Off Campaign.

April 2022
CMA issued its discussion paper on Online Choice Architecture.

April 2022
FTC held a workshop on bringing dark patterns to light.

April 2022
European Commission issued its 'behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation'.

15 September 2022
The FTC released its report illustrating that organisations are increasingly using sophisticated design practices to trick or manipulate consumers into buying products or services or giving up their privacy.

4 October 2022
The EU adopted the DSA.

19 May 2022
FTC issued proposed revisions to Guidelines Concerning the Use of Endorsements and Testimonials in Advertising.

16 November 2022
The DSA came into force.

November 2022
CMA launched investigation into Emma Sleep into the use of "urgency claims" by the Emma Group.

December 2022
FTC entered into settlements for more than $245 million for dark patterns practices that falsely manipulate consumers.

January 2023
The California Privacy Act came into force.

17 February 2023
Online platforms must have published the number of active users by this date under the DSA.

29 March 2023
CMA launched a new phase of its Online Rip-Off Tip-Off Campaign.

2023/2024
AI expected to become EU law but with a two - three year grace period before fully enforceable.

17 February 2024
DSA rules apply for all regulated entities in scope.

July 2024
The Colorado Privacy Act will come into effect.

Key contacts

Alastair Mitton
Partner

T: +44 (0)117 989 6837
E: alastair.mitton@wbd-uk.com

Caroline Churchill
Partner

T: +44 (0)191 279 9069
E: caroline.churchill@wbd-uk.com

Andrew Parsons
Partner

T: +44 (0)238 020 8115
E: andrew.parsons@wbd-uk.com

Ted Claypoole (US)
Partner

T: +1 404-879-2410
E: ted.claypoole@wbd-us.com

Katie Simmonds
Managing Associate

T: +44 (0)207 788 2415
E: katie.simmonds@wbd-uk.com

Will Hall (UK)
Solicitor

T: +44 (0)117 989 6563
E: will.hall@wbd-uk.com

Lucy Reeve (UK)
Apprentice Solicitor

T: +44 (0)117 989 6817
E: lucy.reeve@wbd-uk.com

GROWING
GLOBAL

womblebonddickinson.com