AN A.S. PRATT PUBLICATION
MAY 2023
VOL. 9 NO. 4

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 9 **NUMBER 4** **May 2023**

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Alexandra Jefferies at ..... (937) 560-3067
Email: ..... alexandra.jefferies@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3385
Fax Number ..... (800) 828-8341
Customer Service Web site ..... http://www.lexisnexis.com/custserv/
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (937) 247-0293

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY &CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [1] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [82] (LexisNexis A.S. Pratt)

An A.S. Pratt Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2023–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report*, LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

The EU Stance on Dark Patterns

By Daniel P. Cooper, Sam Jungyun Choi, Jiayen Ong, Diane Valat and Anna Sophia Oberschelp de Meneses*

In this article, the authors provide a snapshot of the current EU legislation that regulates dark patterns as well as upcoming legislative updates that will regulate dark patterns alongside the current legal framework.

The European Commissioner for Justice and Consumer Protection, Didier Reynders, recently announced[1] that the European Commission will focus its next 2023 mandate on regulating dark patterns, alongside transparency in the online advertising market and cookie fatigue. As part of this mandate, the EU's Consumer Protection Cooperation (CPC) Network,[2] conducted a sweep of 399 retail websites and apps for dark patterns, and found[3] that nearly 40% of online shopping websites rely on manipulative practices to exploit consumers' vulnerabilities or trick them. In order to enforce these issues, the EU does not have a single legislation that regulates dark patterns, but there are multiple regulations that discuss dark patterns and that may be used as a tool to protect consumers from dark patterns. This includes the General Data Protection Regulation (GDPR), the Digital Services Act (DSA), the Digital Markets Act (DMA), and the Unfair Commercial Practices Directive (UCPD), as well as proposed regulations such as the AI Act and Data Act.

As a result, there are several regulations and guidelines that organizations must consider when assessing whether their practices may be deemed as a dark pattern. This article provides a snapshot of the current EU legislation that regulates dark patterns as well as upcoming legislative updates that will regulate dark patterns alongside the current legal framework.

LEGAL FRAMEWORK ON DARK PATTERNS

There is not a single definition of the term "dark patterns," however, it touches upon manipulative or deceptive practices that causes consumers to do something that they did not intend or want to do, especially where this leads to a negative consequence. For example:

- The European Data Protection Board (EDPB) defines "dark patterns" as "interfaces and user experiences implemented on social media platforms

* The authors, attorneys with Covington & Burling LLP, may be contacted at dcooper@cov.com, jchoi@cov.com, jong@cov.com and aoberschelpdemeneses@cov.com, respectively.

[1] https://www.euractiv.com/section/digital/interview/dark-patterns-online-ads-will-be-potential-targets-for-the-next-commission-reynders-says/.

[2] https://commission.europa.eu/live-work-travel-eu/consumer-rights-and-complaints/enforcement-consumer-protection/consumer-protection-cooperation-network_en.

[3] https://ec.europa.eu/commission/presscorner/detail/en/ip_23_418.

that lead users into making unintended, unwilling and potentially harmful decisions in regards to their personal data with the aim of influencing users' behaviours." The EDPB also defines 6 categories of dark patterns; (1) overloading; (2) skipping; (3) stirring; (4) hindering; (5) fickle; and (6) left in the dark.

- The proposed Data Act similarly describes dark patterns as a "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."

Despite the varying descriptions, the common features of a "dark pattern" are the (i) manipulative or deceptive nature, and the (ii) resulting negative or harmful outcome on the consumer.

This dark patterns language is pervasive across EU legislation, and can be found within different rules, guidelines and principles. Therefore, when organizations seek to consider what a "dark pattern" is and how this affects their practices, it is important to consider a multitude of regulations, for example:

- *GDPR and ePrivacy Directive*. While the GDPR and the ePrivacy Directive do not explicitly mention dark patterns, they form part of the current legal framework that regulate dark patterns. For example, where organizations rely on consent as the legal basis for processing personal data under the GDPR or obtain consent for cookies or marketing communications under the ePrivacy Directive, it may be possible that they engaged in dark patterns when collecting such consent.
    - EDPB Guidelines 03/2022 on Dark patterns in social media platform interfaces: How to recognize and avoid them (Guidelines)[4] offer practical recommendations on assessing dark patterns in social media platforms. The Guidelines note that dark patterns may have the potential to hinder users' ability to provide their "freely given, specific, informed and unambiguous consent," in turn violating their right to privacy from a data protection and consumer protection perspective. As a practical example, an organization may engage in dark patterns when: the use of words or visuals convey information to users in either (a) a highly positive outlook, making users feel good or safe, or (b) a highly negative one, making users feel anxious

[4] https://edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf.

or guilty, particularly in a way to nudge users towards sharing more data as the default option.

- CPC - EDPB Joint Principles for Fair Advertising to Children. On June 14, 2022, representatives of the EU's CPC Network, together with several national data protection authorities in the EU and the secretariat of the EDPB, endorsed five key principles for fair advertising to children.[5] These include, for example, taking into account the specific vulnerability of children when designing advertising or marketing techniques that are likely to target children (in particular, it must not deceive or unduly influence children) and not to target, urge or prompt children to purchase in-app or in-game content. This requires organizations to take better care to avoid dark patterns when creating online interfaces that are targeted at children.

- *UCPD*. The Unfair Commercial Practices Directive prohibits unfair commercial practices affecting consumers' economic interests before, during and after the conclusion of a contract. On December 29, 2021, the European Commission published guidance[6] on the UCPD that confirms that the UCPD covers dark patterns and dedicates a section (4.2.7) to explain how the relevant provisions of the UCPD can apply to data-driven business-to-consumer commercial practices.

  - The UCPD covers commercial practices such as capturing the consumer's attention, which results in transactional decisions such as continuing to using the service (e.g., scrolling through a feed), to view advertising content or to click on a link. To the extent that these practices include dark patterns and are therefore misleading, they would violate the UCPD. For example, dark patterns have the potential of materially distorting the economic behavior of the average consumer in the context of online advertising, and therefore potentially fall under the UCPD.

- *DSA*. The DSA specifically prohibits deceptive or nudging techniques, including dark patterns, that could distort or impair a user's free choice, such as giving more visual prominence to a consent option or repetitively requesting or urging users to make a decision. Additionally, under the

[5] Press release, https://commission.europa.eu/live-work-travel-eu/consumer-rights-and-complaints/enforcement-consumer-protection/cooperation-between-consumer-and-data-protection-authorities_en.

[6] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021XC1229(05)&from=EN.

DSA, the European Commission is also empowered to adopt delegated acts to define additional practices that may fall within the scope of dark patterns.

- *DMA*. The DMA does not explicitly mention dark patterns, but it imposes obligations on gatekeepers that is described in a similar manner to dark patterns. For example, with respect to free user choice and consent withdrawal, gatekeepers "should not design, organize or operate their online interfaces in a way that deceives, manipulates or otherwise materially distorts or impairs the ability of end users to freely give consent." To this end, the DMA provides for the ability of users' to withdraw their consent as easily as it was to give it, and therefore avoid additional burdens. Failure to provide users with an easy mechanism to withdraw their consent would likely be deemed as a dark pattern, and would be considered as a contravention under the DMA.

PROPOSED LEGISLATION

The regulation around dark patterns is continuously evolving and being incorporated into new legislation, particularly as more studies and investigations shed light on the negative effects that dark patterns have on consumers. The following upcoming rules will also regulate the use of dark patterns:

- *The Proposed AI Act*. The proposed AI Act sets out rules on the development, placing on the market, and use of artificial intelligence systems (AI systems) across the EU. While the AI Act is still undergoing the legislative process, the current proposal prohibits the use of dark patterns within AI systems. Namely, the proposal explicitly prohibits "the placing on the market, putting into service or use of an AI system that deploys subliminal techniques beyond a person's consciousness in order to materially distort a person's behavior in a manner that causes or is likely to cause that person or another person physical or psychological harm." Therefore, manufacturers of AI systems would be prohibited from using deceptive techniques like dark patterns and will need to take into consideration the general data protection principles promoted by the GDPR, namely transparency, accountability, data minimization, among others, to avoid the use of dark patterns within its AI system.

- *The Proposed Data Act*. The proposed Data Act aims to facilitate greater access to and use of data, such as allowing users to access and port to third parties the data generated through their use of connected products and services. As part of this, the third party that receives this data is under an obligation not to "coerce, deceive or manipulate the user in any way, by subverting or impairing the autonomy, decision-making or choices of the user, including by means of a digital interface with the user." Recital

34 explains that this means that third parties should not rely on dark patterns when designing their digital interfaces, particularly in a way that manipulates consumers to disclose more data – the third party should therefore comply with the data minimization principle as defined in the GDPR to ensure that they do not employ dark pattern practices in their interfaces.

- *Digital Fairness Consultation*. On November 28, 2022, the European Commission published a digital fairness public consultation,[7] which was open until February 20, 2023. The aim of the consultation is to determine whether it is necessary to update existing consumer protection legislation (i.e., the Unfair Commercial Practices Directive, Consumer Rights Directive, and Unfair Contract Terms Directive) in order to adapt to the digital transformation of the online world. In particular, the European Commission will consider whether existing consumer protection legislation is adequate to protect consumers against novel consumer protection issues, such as online deceptive and nudging techniques, including dark patterns, among other consumer protection concerns (personalization practices, influencer marketing, marketing of virtual items etc.).

Following the consultation, the European Commission will publish a Staff Working Document, which will address these issues and potentially recommend a new legislative proposal that will regulate dark patterns further. In the meantime, the EU has already pursued dark pattern enforcement, for example:

- As part of the European Commission's New Consumer Agenda[8] (which encompasses the dark patterns mandate), in April 2022, the European Commission released its Behavioural study on unfair commercial practices in the digital environment,[9] which examines the use of dark patterns and manipulative personalization and identifies the potential gaps in existing consumer protection legislation to tackle concerns relating to dark patterns. The European Commission will contact online traders identified in this study to ask them to rectify the issues identified.

- As mentioned above, the CPC Network has conducted online sweeps to identify the use of dark patterns on websites and apps – the European Commission press release[10] notes that nearly 40% of online shopping

[7] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13413-Digital-fairness-fitness-check-on-EU-consumer-law/public-consultation_en.

[8] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0696.

[9] https://op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1/language-en.

[10] https://ec.europa.eu/commission/presscorner/detail/en/ip_23_418.

websites that they reviewed (148 out of 399) rely on manipulative practices to exploit consumers' vulnerabilities or trick them (e.g., fake countdown timers, hidden information, and web interfaces designed to lead consumers to purchases, subscriptions or other choices). The relevant member state's consumer protection authorities will now contact the relevant traders to rectify their websites and take further action if necessary.

- Enforcement is also likely to be expected on a sectorial basis, such as in the financial sector as evidenced by the statement[11] of the German Federal Financial Supervisory Authority prohibiting dark patterns in trading apps or trading portals, published on November 21, 2022.

CONCLUSION

The EU is taking significant steps to further protect EU consumers' rights, especially in the digital realm, and continue to provide additional recommendations for companies to fulfil such goals. With the adoption of the Digital Markets Act and Digital Services Act, and the negotiation of the upcoming legislative proposals, the European institutions are setting the tone for 2023 for more transparency and accountability in digital markets. The focus on regulating dark patterns will likely have far-reaching effects, as demonstrated by its nexus to a multitude of EU legislation. Additionally, as dark patterns regulation will not be constrained to any single regulation, there will be an increasing number of enforcement into dark patterns. For example, dark patterns is also on the enforcement agenda for EU data protection authorities as they investigate the use of dark patterns and the processing of personal data and digital marketing.

[11] https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Meldung/2022/meldung_2022_11_21_Dark_Patterns_in_TradingApps_Experten.html.