Dark Patterns: Light to be found in Europe's Consumer Protection Regime

Leiser, M.R.; Caruana, M.

Dark Patterns – Light to be found in Europe's Consumer Protection Regime

Abstract

Need to add

Introduction

Defined as 'tricks used in websites and apps that make you do things that you did not mean to, like buying or signing up for something',[1] much of the academic scholarship on the regulation of 'dark patterns' has focussed on privacy and data protection legislation.[2] The term has been deployed to describe 'deceptive' and 'manipulative' design techniques implemented in a way that led to a user behaviour that would not have happened without the dark pattern.[3] The term is used both broadly and informally: 'tricks used in websites and apps that make you do things that you didn't mean to, like buying or signing up for something'[4]. They are also defined broadly and formally; for example, Gray *et al* state dark patterns are 'interface designs that try to guide end-users into desired behaviour through malicious interaction flows';[5] and narrowly and specific to a discipline of information technology law: for example, Santos *et al* refer to dark patterns as a nudge to getting consent from users to begin processing personal data.[6] Luguri and Strahilevitz, bypassing how dark patterns can be embedded in system architecture, limit their definition of dark patterns to "*user interfaces* whose designers knowingly confuse users, make it difficult for users to express their actual preferences, or manipulate users into taking certain actions" [Emphasis Added].[7]

As defaults are easy to implement and constitute one of the most widely deployed tools in user interfaces, the EU Data Protection Supervisor refers to 'privacy intrusive default settings', 'hiding away privacy-friendly choices that require more effort from the user to select', 'illusory' or 'take-it-or-leave-it choices' as dark pattens in advisory documents.[8] The French data protection regulator, the Commission Nationale de L'informatique et des Libertés (CNIL) stated that 'the architect of choice decides (intentionally or unintentionally) the social, technical and political environment in which individuals exercise their power to choose (or not to choose)'.[9] Accordingly, users are more likely to select options with a pre-selected default option chosen for them by designers who deploy dark patterns

---

[1] <darkpatterns.org> accessed 9 April 2020.

[2] Christoph Bösch, Benjamin Erb, Frank Kargl, Henning Kopp, and Stefan Pfattheicher, 'Tales from the dark side: Privacy dark strategies and privacy dark patterns' (2016) 4 Proceedings on Privacy Enhancing Technologies 237-254; Lothar Fritsch and others (eds.) 'Privacy dark patterns in identity management' In *Open Identity Summit (OID) 2017,* Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2017, 93-104; Lior Strahilevitz and others, Subcommittee report: 'Privacy and data protection' (2019) Stigler Center Committee for the Study of Digital Platforms, 22-23; Midas Nouwens, Ilaria Liccardi, Michael Veale, David Karger, and Lalana Kagal (2020) 'Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence' *ArXiv preprint ArXiv:2001.02479*; Damian Clifford, 'Citizen-consumers in a personalised galaxy: Emotion influenced decision-making, a true path to the dark side?' (2017) CiTiP Working Paper Series, 31/2017, accessed <https://ssrn.com/abstract=3037425> or <http://dx.doi.org/10.2139/ssrn.3037425> 17 May 2021.

[3] Colin M Gray, Yubo Kou, Bryan Battles, Joseph Hoggatt, and Austin L Toombs, 'The dark (patterns) side of UX design' (2018) Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, Paper 534, Pages 1 – 14 <https://dl.acm.org/doi/10.1145/3173574.3174108> accessed 25 May 2021 (pp. 1-14); Christoph Bösch, Benjamin Erb, Frank Kargl, Henning Kopp and Stefan Pfattheicher, 'Tales from the dark side: Privacy dark strategies and privacy dark patterns' (2016) 4 Proceedings on Privacy Enhancing Technologies 237-254

[4] Harry Brignell, 'What are dark patterns?' (2018) <https://darkpatterns.org> accessed 9 March 2020.

[5] Gray and others (n 3) 12.

[6] Cristiana Santos, Nataliia Bielova, and Celestin Matte, 'Are cookie banners indeed compliant with the law? Deciphering EU legal requirements on consent and technical means to verify compliance of cookie banners' [2019] *ArXiv preprint ArXiv:1912.07144*.

[7] Jamie Luguri and Lior Strahilevitz, Lior, 'Shining a Light on Dark Patterns' (2021) 13 Journal of Legal Analysis 43, University of Chicago Coase-Sandor Institute for Law & Economics Research Paper No. 879, U of Chicago, Public Law Working Paper No. 719 <https://ssrn.com/abstract=3431205> or <http://dx.doi.org/10.2139/ssrn.3431205> accessed 25 May 2021.

[8] European Data Protection Supervisor, 'Preliminary Opinion of the European Data Protection Supervisor, Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy' (March 2014) <https://edps.europa.eu/sites/edp/files/publication/14-03-26_competitition_law_big_data_en.pdf> accessed 10 April 2020.

[9] Commission Nationale de L'informatique et des Libertés (CNIL), 'Shaping Choices in the Digital World. From dark patterns to data protection: the influence of UX/UI Design on user empowerment' (IP Reports Innovation and Foresight No. 06, 16 April 2019) 41 <https://linc.cnil.fr/fr/ip-report-shaping-choices-digital-world> accessed 10 April 2020.

to weaponize the design of user interfaces and infrastructures for their own benefit, often at the expense of protecting consumers and ensuring the rights of data subjects.

Researchers have begun to study the deployment of dark patterns at scale. Noewens *et al*[10] refer to recent moves by data protection authorities to provide greater oversight over 'certain common dark patterns as non-compliant examples of the European Union's General Data Protection Regulation (GDPR).[11] However dark patterns are not just a privacy issue or a problem for the data protection regulators to solve. Mathur *et al* examined over 11k shopping websites to determine the deployment of dark patterns at scale to influence users into making more purchases or disclosing more information than they would otherwise.[12]

The Norwegian Consumer Council has been very active in this area; first, issuing a report on deceptive design[13] and recently challenging Amazon's use of 'dark patterns' that make it appreciably harder for users to cancel out of its paid-for-subscription service.[14] Luguri and Strahilevitz's study into how effective dark patterns are at convincing consumers to 'choose' options they might not prefer revealed that certain patterns have a clear impact on altering users' behaviour.[15]

Dark Patterns are also getting attention from lawmakers outside of Europe. A new California law defines dark patterns 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",[16] effectively outlawing some dark patterns that steer people into giving companies more data than intended.[17] The US Federal Trade Commission has not only adopted the term 'dark patterns' but began a series of workshops and consultations on the problem.[18] Furthermore, In R*e Age of Learning*, the FTC even embraced the lingo from dark patterns literature, referring to 'obfuscation', 'obstruction', 'forced continuity', interface interference ('hidden information'), and confusing cancellation prompts.[19]

Consumer protection is aimed at fostering user empowerment: The European Data Protection Supervisor stated: 'EU approaches to data protection [. . .] and consumer protection share common goals, including the promotion of growth, innovation and the welfare of individual consumers'.[20] Thus, this article analyses to what extent the current EU Consumer Protection acquis is placed to make a substantial and complementary contribution towards curtailing the use of dark patterns.[21] We do so through the lens of the European Commission's adoption of a 'New Deal for Consumers' which strengthens enforcement mechanisms of EU consumer law and modernises the EU's consumer

[10] Midas Nouwens, Ilaria Liccardi, Michael Veale, David Karger, and Lalana Kagal (2020) 'Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence' *ArXiv preprint ArXiv:2001.02479*

[11] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1

[12] Mathur, A., Acar, G., Friedman, M. J., Lucherini, E., Mayer, J., Chetty, M., & Narayanan, A. (2019). Dark patterns at scale: Findings from a crawl of 11K shopping websites. Proceedings of the ACM on Human-Computer Interaction, 3(CSCW), 1-32.

[13] Norwegian Consumer Council (Forbrukerrådet) report on how Google uses dark patterns to discourage users from exercising their rights, 'Deceived by Design. How Tech Companies use dark patterns to discourage us from exercising our rights to privacy' (27 June 2018) 19 <https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/deceived-by-design/> accessed 10 April 2020

[14] Amazon faces legal challenge over Prime cancellation policy <https://www.bbc.co.uk/news/technology-55637140> accessed 25 May 2021

[15] Luguri, J., & Strahilevitz, L. J. (2021). Shining a light on dark patterns. Journal of Legal Analysis, 13(1), 43-109.

[16] Section 1798.140 (l) of the Civil Code (Definitions)

[17] The California Privacy Rights and Enforcement Act of 2020

[18] See <https://www.ftc.gov/news-events/events-calendar/bringing-dark-patterns-light-ftc-workshop> accessed 25 May 2021.

[19] Case 2:20-cv-07996 <https://www.ftc.gov/system/files/documents/cases/1723086abcmousestipulation.pdf> accessed 25 May 2021.

[20] European Data Protection Supervisor, 'Preliminary Opinion of the European Data Protection Supervisor, Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy' (March 2014) <https://edps.europa.eu/sites/edp/files/publication/14-03-26_competitition_law_big_data_en.pdf> accessed 10 April 2020

[21] Throughout this paper we have referred to the position at law as amended by Directive 2019/2161 on better enforcement and modernisation of Union consumer protection rules, part of the 'Review of EU consumer law – New Deal for Consumers'. It has to be transposed by 28 November 2021 and applied from 28 May 2022

protection rules in view of market developments.[22] Alongside the Unfair Commercial Practices Directive[23], the Consumer Rights Directive[24], the Unfair Contract Terms Directive[25], the Directive on certain aspects concerning contracts for the Supply of Digital Content and Digital Services[26] and other legal instruments,[27] we assess the application and fitness for purpose of the EU Consumer Law acquis to act as an effective deterrent and/or sanctioning mechanism against manipulative design techniques like dark patterns. We analyse these legislative acts as those that could be applied effectively to regulate and suppress the use and deployment of dark patterns. We also consider the legislative amendments introduced to the consumer acquis to strengthen deterrence and enforcement, stopping short of engaging in any empirical analysis of whether these amendments deliver on their promise in practice.

Because common elements of consumer protection legislation include requirements of clarity and comprehensibility of information and commercial communications on-line, rules on truthful advertising, and deterrents against misleading and aggressive commercial practices, as well as other rules aimed at the substance of the consumer contract, Part One of this paper identifies the common elements of dark patterns typically used on digital platforms (e.g., manipulation, deception, forced registration, hidden legalese stipulations, etc.). Parts two and three assess the patchwork of legislative instruments that make up the EU consumer protection regime, and the related mechanisms of redress and enforcement. In these sections, we also consider to what extent the application of Directive 2019/2161[28] will strengthen the tools made available by the Consumer Protection acquis to combat the use of dark patterns. We conclude that consumer protection law should be utilised to maximum effect to ensure a trusted environment essential to the continued development and success of the digital single market. This will ensure design processes and user interfaces are developed for digital environments that respect and uphold the interests of consumers interacting therewith.

Part I: Dark Patterns

What are dark patterns? Much of the regulatory and academic emphasis on dark patterns has focused on the purposeful use of deception and manipulation to modify user behaviour; for example, Harris channels the deceptive nature of magic to describe how design techniques can be used to manipulate users:

> *We ignore how… choices are manipulated upstream by menus we didn't choose in the first place...This is exactly what magicians do. They give people the illusion of free choice while architecting the menu so that they win, no matter what you choose… By shaping the menu, we*

[22] Review of EU consumer law - New Deal for Consumers <https://ec.europa.eu/info/law/law-topic/consumers/review-eu-consumer-law-new-deal-consumers_en> accessed 7 April 2020; See also EC. (2007). EU consumer policy strategy 2007–2013, COM (2007) 99 final. Brussels: European Commission; EC. *Single Market Act —Twelve levers to boost growth and strengthen confidence. (Communication). COM (2011) 206 final*. European Commission. Commission Staff Working Paper. Consumer Empowerment in the EU <https://ec.europa.eu/info/departments/justice-and-consumers_en> accessed 7 April 2020)

[23] Directive 2005/29/EC of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC, and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council [2005] OJ L149/22 ('Unfair Commercial Practices Directive')

[24] Directive 2011/83/EU of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council [2011] OJ L304/64 ('Consumer Rights Directive')

[25] Council Directive 93/13/EEC of 5 April 1993 on Unfair Terms in Consumer Contracts [1993] OJ L95/29 ('Unfair Contract Terms Directive')

[26] Directive (EU) 2019/770 of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services [2019] OJ L136/1 ('Digital Content Directive')

[27] e.g., Directive (EU) 2019/2161 of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC, and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules [2019] OJ L 328/7 ('Directive on Better Enforcement and Modernisation of Union Consumer Protection Rules')

[28] Directive on Better Enforcement and Modernisation of Union Consumer Protection Rules

pick from, technology hijacks the way we perceive our choices and replaces them with new ones.[29]

The design literature has also deployed colourful metaphors to describe dark patterns. Phrases like 'Privacy Zuckering' (named after Facebook CEO Mark Zuckerberg, this dark pattern tricks users into sharing more information about themselves than they wanted to), 'roach motel' (a design technique that makes signing up easy but buries the ability to leave in another part of the site) and 'confirm shaming' (framing and nudging users towards a choice by presenting the alternative as ethically questionable or risky) have entered the lexicon of regulators.[30]

Category	Variant	Description	Source
Nagging		Repeated requests to do something firm prefers	Gray[31]
Social Proof	Activity messages	Misleading notice about other consumers' actions	Mathur[32]
	Testimonials	The website displays recommendations and praises of other users for the products or services, while the source or origin of these customer testimonials is not clearly specified	Mathur
Obstruction	Roach Motel	Design that makes it easy for users to get into certain situations such as subscribing to a paid membership, but then find it difficult to get out of it. This is also called 'Hard to Cancel' or 'Obstruction' in some studies.[33]	Gray, Mathur
	Price Comparison Prevention	The designed interface prevents users from making an informed decision by making it hard for users to compare the prices of an item with another item. For example, two different brands of apples are displayed side by side, while one is sold in units and the other is sold in kilograms	Brignull[34], Gray, Mathur
	Intermediate Currency	Purchases in virtual currency to obscure cost	Brignull
Sneaking	Sneak into Basket	In the purchasing journey, the site adds additional products into the customers' basket without their consent through, for example, an opt-out radio button or checkbox on a prior page. The Sneak into Basket dark pattern "exploits the default effect cognitive bias in users" to trick consumers to stick with the products it adds to basket[35]	Brignull, Gray, Mathur

[29] Triston Harris, 'How technology is hijacking your mind—from a magician and Google design ethicist' (Medium, 6 January 2016) <https://observer.com/2016/06/how-technology-hijacks-peoples-minds%E2%80%8A-%E2%80%8Afrom-a-magician-and-googles-design-ethicist/> accessed 10 April 2020
[30] Note 13 at Page 4.
[31] Gray and others (n 3)
[32] Mathur et al (n 12)
[33] Mathur et al (n 12) 102.
[34] Harry Brignull. 2018. Dark Patterns. <https://darkpatterns.org/> accessed 24 May 2021
[35] Mathur et al (n 12) 93

	Hidden Costs	When the consumers get to the last step of the checkout process, some new additional charges such as delivery fee or tax have suddenly appeared. The Hidden Costs dark pattern exploits "sunk cost fallacy cognitive bias" of consumers; they may hesitate to cancel the purchase as that means all efforts invested in the process of shopping are wasted[36]	Brignull, Gray, Mathur
	Hidden subscription / forced continuity	After a free trial or a one-time purchase comes to an end, the service silently starts getting charged from the user's credit card without any warning. In some cases, the users even find it difficult to cancel the paid membership.	Brignull, Gray, Mathur
	Bait & Switch	Customer sold something other than what's originally advertised	Gray
Interface Interference	Hidden information/ aesthetic manipulation/false hierarchy	Important information visually obscured	Gray, Mathur
	Preselection	Firm-friendly default is preselected	Bösch[37], Gray
	Toying with emotion	Emotionally manipulative framing	Gray
	Trick questions	At first glance, the question seems to ask one thing, while it asks another thing if read carefully, namely the question aims to trick users into giving a certain answer.	Gray, Mathur
	Disguised Ad	Advertisement disguises itself as other kinds of content or navigation, to trick users to click on them	Brignull, Gray
	Confirmshaming	Making users feel guilty for choosing the option to decline by wording the option in a way as to shame users into compliance. For example, 'No thanks, I don't care about my cat'	Brignull, Mathur
Forced Action	Forced Registration	The Forced Action dark pattern requires users to complete certain actions, otherwise the services will not be available. 'Forced enrolment' is a typical Forced Action; users are coerced to creates accounts and surrender their personal information, in order to access the services. 'Pay to skip' can also be an example of the Forced Action dark patterns	Bösch

[36] Mathur et al (n 12) 93
[37] Bösch, C., Erb, B., Kargl, F., Kopp, H., & Pfattheicher, S. (2016). Tales from the dark side: Privacy dark strategies and privacy dark patterns. Proceedings on Privacy Enhancing Technologies, 2016(4), 237-254.

Urgency	Low stock / high-demand message	A static urgency message without an accompanying deadline or stock numbers." For example, stating a sale will be end soon but without mention of the specific time	Mathur
	Countdown timer / Limited time message	Dynamic indicator of deadlines which count down until the deadline expires. But in many cases, the sale deadline does not really exist, and the countdown timer is set to create urgency to sales	Mathur

Taken together, there are some common characteristics that define dark patterns. Mathur *et al* criticise the coercion, steering, and deceptive design choices platforms use to keep the data flowing. These 'interface design choices that benefit an online service by coercing, steering, or deceiving users into making decisions that, if fully informed and capable of selecting alternatives, they might not make'.[38] Dark patterns 'make disclosure 'irresistible' by connecting information sharing to in-app benefits. In these and other ways, designers intentionally make it difficult for users to effectuate their preferences'.[39] Others have argued that dark patterns are subtle and sneaky: hidden influences manipulate users in a way that infringes autonomy, bypass rational capacities, and subvert decision-making; for example, Susser *et al* argue that 'the manipulator infiltrates our decision-making, disposing us to their ends, which may or may not be our own'.[40] Dark patterns would not be approved of by Sunstein, who argues that manipulative actions are intentional measures that do not sufficiently engage or appeal to users' capacity for reflection and deliberation.[41]As new technologies have radically altered the landscape for electronic commerce, the variety and extent of dark patterns can frustrate even the savviest consumers.

Unsurprisingly, the following harms have been associated with the use of dark patterns: lower autonomy[42] a reduction in overall social and consumer welfare; an erosion of trust; increased insecurity; and unfair treatment among consumers,[43], while risking anticompetitive effects (if a sufficient market power exists). Furthermore, if unjust data-driven discrimination persists as a result of a data-grabbing dark pattern, individuals and groups can suffer persistent disadvantages; for example, the unjust consequences associated with algorithmic discrimination, and reinforcement of the social advantages of one to the disadvantage of another. Thus, dark patterns distract from two of the central objectives of the European Union's digital single market: creating the right conditions and a level playing field for digital networks and innovative services to flourish and maximise the growth potential of the digital economy.[44]

To balance clarity for e-commerce businesses with stronger consumer protection measures for users, the European Commission brought into effect a new Directive on Contracts for online and other distance

[38] Arunesh Mathur, Gunes Acar, Micheal J Friedman, Elena Lucherini, Jonathan Mayer, Marshini Chetty, and Arvind Narayanan, 'Dark patterns at scale: findings from a crawl of 11K shopping websites' [2019] ACM Conf. Comp.-Supported Cooperative Work.

[39] Ari Ezra Waldman, 'Cognitive Biases, Dark Patterns, and the 'Privacy Paradox' (2020) 31 Current Opinion in Psychology 105, 107 <https://doi.org/10.1016/j.copsyc.2019.08.025> accessed10 March 2020.

[40] Daniel Susser, Beate Roessler and Helen Nissenbaum, 'Technology, autonomy, and manipulation' (2019) 8(2) Internet Policy Review https://doi.org/10.14763/2019.2.1410 accessed 17 May 2021..

[41] Cass R Sunstein, 'Fifty Shades of Manipulation' (2016) 1 J. Marketing Behav. 213, 218.

[42] Paul Bernal, 'Internet Privacy Rights: Rights to Protect Autonomy' (CUP 2014) 26; See also Antoinette Rouvroy, 'Privacy, Data Protection and the unprecedented challenges of Ambient Intelligence' (2008) 2(1) Studies in Ethics, Law, and Technology 7.

[43] Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy <https://edps.europa.eu/sites/edp/files/publication/10-03-19_trust_information_society_en.pdf> accessed 18 April 2020.

[44] European Parliament, 'The ubiquitous digital single market' <https://www.europarl.europa.eu/factsheets/en/sheet/43/the-ubiquitous-digital-single-market> accessed 8 April 2020.

sales of goods[45], a new Directive regulating contracts for the supply of digital content[46], and a new Directive on better enforcement and modernisation of Union consumer protection rules[47]. The measures mirror upgrades by the Commission to the framework for protecting the processing of personal data. Citizens of the European Union are said to have a 'strong, comprehensive and enforceable privacy protection framework'[48] flowing from the Charter of Fundamental Rights of the European Union[49] and consisting of a general regulation on data protection, the General Data Protection Regulation (GDPR),[50] and the e-Privacy Directive.[51] Further protection comes from the European Convention on Human Rights[52] and laws of the member states, including national constitutions.

Part II: Dark Patterns and the Consumer Protection Regime

If a data subject (in terms of data protection law) is also a consumer (as defined in consumer protection law), the European Union offers a 'high level of consumer protection' for her economic activities.[53] In fact, both consumer and data protection laws aim, at least in part, to protect the autonomy of the natural person[54] In other instances, autonomy is overridden by the interests of protecting the weaker party in an imbalanced relationship).[55] However, protection as a *concept* for consumers is clearer. While privacy and data protection law involve complex balancing of interests in a variety of contexts, consumer protection aims to address power differentials based *inter alia* on information asymmetries and/or bargaining power.[56]

First, as we will discuss throughout this paper, the concept of *fairness* is wider in consumer protection than data protection law and would be more suitable to holding data controllers that deploy dark patterns to account.[57] For example, The Unfair Contract Terms Directive ('UCTD') considers a non-negotiated term in a contract or consent statement unfair if 'contrary to the requirement of good faith, it causes a significant imbalance in the parties' rights and obligations arising under the contract, to the detriment of the consumer'[58], while the GDPR does not contain a similar provision. The Unfair Commercial Practices Directive will consider a dark pattern unfair if it is 'contrary to the requirements of

[45] Directive (EU) 2019/771 of 20 May 2019 on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC [2019] OJ L136/28 ('Sale of Goods Directive')

[46] Directive (EU) 2019/770 of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services [2019] OJ L136/1 ('Digital Content Directive')

[47] Directive on Better Enforcement and Modernisation of Union Consumer Protection Rules

[48] EDRI. (2013, April 10). EU: The global standard setter for privacy and data protection (EU Data P series, Issue 2). EDRI. <http://edri.org/files/eudatap-02.pdf> accessed11 March 2020

[49] The protection of personal data is a fundamental right under Art 8 of the EU Charter of Fundamental Rights. Art 8(2) of the Charter contains key data protection principles (fair processing, consent or legitimate aim prescribed by law, right to access and rectification). Art 8(3) of the Charter requires that compliance with data protection rules be subject to control by an independent authority.

[50] Regulation (EU) 2016/679 of 27 April 2016on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (2016) OJ L119/1

[51] Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) OJ L201/37

[52] Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR)

[53] Charter of Fundamental Rights of the European Union (2012) OJ C326/391, Art 38.

[54] Our concept of autonomy is rooted in Gerald Dworkin's definition of the concept: 'the ability to make informed decisions regarding one's life, while choosing between several reasonable options' Dworkin, G. (1988). The theory and practice of autonomy. Cambridge University Press as cited by Zarsky, T. Z. (2019). Privacy and Manipulation in the Digital Age. Theoretical Inquiries in Law, 20(1), 157-188 at 174.

[55] Stephen Weatherill, *EU Consumer Law and Policy* (2nd edition, Edward Elgar, Cheltenham, UK, 2013).

[56] W. David Slawson, 'Standard Form Contracts and Democratic Control of Lawmaking Power' (1971) 84 Harvard Law Review, 529.

[57] 'Fairness' is explicitly mentioned in Art 8(2) of the Charter of Fundamental Rights and referred to as a 'core principle' by the European Data Protection Supervisor 'Opinion on Coherent Enforcement of Fundamental Rights in the Age of Big Data' (EDPS 2016) Opinion 8/2016 8, at Opinion 8/2016 EDPS Opinion on coherent enforcement of fundamental rights in the age of big data, (last visited 9 April 2020).

[58] Unfair Contract Terms Directive, Art 3; See also Common position of national authorities within the CPC Network concerning the commercial practices and the terms of service of Airbnb, Ireland, at Common position of national authorities within the CPC Network concerning the commercial practices and the terms of service of A, at 10, (last visited 10 April 2020).

professional diligence and materially distorts or is likely materially to distort the economic behaviour of the average consumer with regard to the product'.[59] In turn, 'to materially distort the economic behaviour of consumers' is defined as 'using a commercial practice to appreciably impair the consumer's ability to make an informed decision, thereby causing the consumer to take a transactional decision that he would not have taken otherwise'.[60]

Second, consumer law provides better participation opportunities when seeking a judicial or administrative remedy. The GDPR does not require member states to allow complaints by advocacy groups independently of a data subject's mandate; it merely permits them to do so.[61] Conversely, Article 11(1) of the Unfair Commercial Practices Directive and Article 7(2) of the Unfair Contract Terms Directive requires member states to ensure consumer rights organizations can bring an action before the national courts and/or administrative authorities. These provisions allow the collectivization of resources and building on previous organizational efforts, reducing participating costs. Finally, the consumer protection regime provides more opportunities and remedies (i.e., damages, enforcement measures, including discontinued use of unfair terms) than the regime for the protection of personal data. As this article will discuss, this provides consumers with greater participation rights and more opportunities to shape consumer protection at national level than at EU level.

How does one bring dark patterns, a genre of practices normally associated with the data protection regime, within the scope of consumer protection law? First, the EU consumer protection regime sees personal data as having economic value but does so without resorting to the bestowment of property rights to data subjects over their personal data.[62] The Digital Content and Services Directive is not clear whether a situation 'where the trader supplies or undertakes to supply digital content or a digital service to the consumer, and the consumer provides or undertakes to provide personal data to the trader'[63] constitutes a contract. They are merely 'within the scope' of the Directive. A contract remains 'where the trader supplies or undertakes to supply digital content or a digital service to the consumer and the consumer pays or undertakes to pay a price',[64] where ''price' means money or a digital representation of value that is due in exchange for the supply of digital content or a digital service'.[65] Therefore one would need to look towards national legal frameworks in order to determine whether a contract has been formed; whether in particular the requisite element of 'causa' or 'lawful consideration' (for example, the term used in section 966 of the Maltese Civil Code) is present. This legal point is relevant where the application of consumer protection is dependent on the existence of a contract, such as in the Unfair Consumer Terms Directive (UCTD). Recital 25 clarifies that '(...) This Directive should also not apply to situations where the trader only collects metadata, such as information concerning the consumer's device or browsing history, except where this situation is considered to be a contract under national law. It should also not apply to situations where the consumer, without having concluded a contract with the trader, is exposed to advertisements exclusively in order to gain access to digital content or a digital service. However, Member States should remain free to extend the application of this Directive to such situations, or to otherwise regulate such situations, which are excluded from the scope of this Directive.'

Paragraph to data protection to the consumer protection regime. Symbiosis between the two regimes. Dark patterns for the purpose of getting consumers to agree to data processing are not solely under the scope of the data protection regulation; in fact, this is also a consumer protection issue. The Guidance on the UCPD's application recognizes that 'Personal data, consumer preferences and other user

[59] Unfair Commercial Practices Directive, Art 5(2)(a) and (b)
[60] Unfair Commercial Practices Directive, Art 2(e)
[61] General Data Protection Regulation, Art 80(2)
[62] Recital 24, European Parliament and Council Directive (EU) 2019/770 of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services [2019] OJ L136/1; See also Jacopo Ciano, 'A Competition-Law-Oriented Look at the Application of Data Protection and IP Law to the Internet of Things: Towards a Wider 'Holistic Approach'' in Mor Bakhoum and others (eds), Personal Data in Competition, Consumer Protection, and Intellectual Property Law. Towards a Holistic Approach? (Springer 2018) 223-224.
[63] Digital Content Directive, Art 3(1) paragraph 2
[64] Digital Content Directive, Art 3(1) paragraph 1
[65] Digital Content Directive, Art 2(7)

generated content, have a '*de facto'* economic value and are being sold to third parties.'[66] A German court upheld complaints from the Federal Consumer Association (vzbv) that issues relating to the processing of personal data come within the scope of consumer protection law.[67] In an investigation by the Autorità Garante della Concorrenza e del Mercato (AGCM)[68], it was determined that commercial practice rules could be extended to data processing, as data had economic value.[69] In the European Union, the Competition Commission stated that 'the vast majority of social networking services are provided free of monetary charges. They can however be monetized through other means, such as advertising or charges for premium services.'[70] By merging the personal data of WhatsApp with Facebook, the economic value of data collected from WhatsApp users could strengthen Facebook's position as a leader in online advertising:

> 'the merged entity could introduce targeted advertising on WhatsApp by analysing user data collected from WhatsApp's users (and/or from Facebook users who are also WhatsApp users). This would have the effect of reinforcing Facebook's position in the online advertising market or sub-segments thereof'.[71]

And later in the same judgment:

> 'The merged entity could start collecting data from WhatsApp users with a view to improving the accuracy of the targeted ads served on Facebook's social networking platform to WhatsApp users that are also Facebook users'.[72]

Second, having established personal data has economic value, some dark patterns could be brought under the remit of consumer protection authorities. In the first of two AGCM investigations into whether Facebook violated Italian consumer protection regulations, the social network was charged with aggressively forcing users to accept terms and conditions.[73] First, Facebook was charged with using an in-app procedure for obtaining user acceptance of new terms and conditions. This was characterized as excessively emphasizing the need to accept 'within the following 30 days or lose the opportunity to use the service at all'. Second, the new terms and conditions were followed with inadequate information about the ability to deny consent to sharing personal data from users' WhatsApp accounts with Facebook. Third, consumers were denied the opportunity to refuse consent to sharing their personal data with Facebook. Finally, users found it difficult to opt-out.[74] Zingales points out that not only did the Italian Competition Authority conclude that the practices under review did not affect the competences of the Italian Data Protection Authority, the Communication Authority, Autorità per le Garanzie nelle Comunicazioni (AGCOM), issued an preliminary opinion warning that the use of

---

[66] Guidance on the implementation/application of directive 2005/29/EC on unfair commercial practices SWD/2016/0163 final, at <52016SC0163 - EN - EUR-Lex>, at Section 1.4.10; See also Section 5.2.9, 'Social media', about the application of UCPD to specific sectors: 'Social media such as Facebook, Twitter, YouTube, WhatsApp, Instagram and blogs enable users to create profiles and communicate with each other, including sharing information and content, such as text, images and sound files. […] social media platforms can qualify as 'traders' in their own right, under the UCPD. […] National enforcement authorities have identified a number of issues in relation to social media and EU consumer and marketing law, such as: […] possibly unfair standard contract terms used by social media platforms.'

[67] VZBV vs WhatsApp, Judgment of the Chamber Court of 20.12.2019, Az. 5 U 9/18, at https://www.vzbv.de/sites/default/files/whatsapp_kg_berlin_urteil.pdf, (last visited 09 April 2020).

[68] The AGCM is an independent administrative authority of Italy. It has powers to investigate unfair commercial practices, misleading and unlawful comparative advertising, and the application of conflict of interest's laws to government-office holders.

[69] Case No. CV154: WhatsApp - Unfair Terms; full decision in Italian accessed here <https://www.agcm.it/dotcmsDOC/allegati-news/CV154_vessestratto_omi.pdf> on 18 April 2020; A second case concerned sharing personal data between Facebook and WhatsApp – Case No. PS10601: WhatsApp - Sharing personal data with Facebook; full decision in Italian accessed at <https://www.agcm.it/dotcmsDOC/allegati-news/PS10601_scorrsanz_omi.pdf> on 18 April 2020. Both cases started 27 October 2016 and decided on 11 May 2017.

[70] Case No COMP/M.7217 - Facebook/WhatsApp, at Para 47, at Case No COMP/M.7217 - FACEBOOK/ WHATSAPP REGULATION (EC) No 139/2004 MERGER PROCEDURE Art 6(1)(b) NON-OPPOSITION Date: 03/10, (last visited 09 April 2020).

[71] ibid paragraph 168

[72] ibid paragraph 180

[73] Articles 20 (i.e., Unfair Commercial Practice), 24 (i.e., Aggressive Commercial Practice) and 25 (i.e., Resort to harassment, coercion, or undue influence) of the ICC.

[74] Case No. PS10601: WhatsApp - Sharing personal data with Facebook; above, n.60.

smartphones and the growth of the Internet has increased the effects of unsavoury commercial practices, like undue influence, on consumers.[75] The AGCM also responded to WhatsApp's argument that the transfer of communications data would not constitute a commercial practice by pointing out that the use of data as counter-performance in social media is well recognized in antitrust and consumer protection law. Facebook was found in violation of Articles 24 and 25 of the Consumer Code, for carrying out an aggressive practice, as it exerted undue influence on registered consumers, who suffer, without express and prior consent, and therefore unconsciously and automatically, the transmission of their data from Facebook to third-party websites/apps for commercial purposes, and vice versa. The undue influence was caused by the pre-selection (a type of dark pattern) by Facebook of the broadest possible consent to data sharing. By pre-selecting the 'Active Platform' functionality Facebook set defaults (a dark pattern) that enabled the transmission of personal data to single website/apps without any express consent. Facebook then reiterated the opt-out pre-selection mechanism (a dark pattern) whenever users access third-party websites/apps using their Facebook accounts. In this case, users could only deselect the pre-setting operated by Facebook (a dark pattern), without being able to make a free, informed choice. When users wanted to limit their consent, they were faced with significant restrictions on the use of the social network and third-party websites/apps (a dark pattern), which induced users to maintain a pre-selected choice.[76]

The Unfair Contract Terms Directive

The consumer protection regime envisages transparency and protection against unfairness.[77] The UCTD aims to address situations of imbalance between the parties in relation to contract terms, which can be due to an asymmetry of information or expertise[78] or bargaining power[79] in relation to the contract terms. In the words of the Court:

> the weaker position of the consumer vis-à-vis the seller or supplier, which the system of protection implemented by Directive 93/13 is intended to remedy, relates both to the consumer's level of knowledge and to his bargaining power under terms drawn up in advance by the seller or supplier the content of which that consumer is unable to influence.[80]

Fairness is the substantive test for the legality of contract terms. Thus, under Article 3(1): 'A contractual term which has not been individually negotiated shall be regarded as unfair if, contrary to the requirement of good faith, it causes a significant imbalance in the parties' rights and obligations arising under the contract, to the detriment of the consumer.' The application of this Directive (and relative national transposing legislation) is dependent on the formation and existence of a contract. In the context of dark patterns, this may be limiting as, in analysing the website design and consequent consumer behaviour, the availability of any solution under the UCTD will be dependent on the ability to identify a contractual relationship between a trader and a consumer. Nevertheless, under Article 4, 'the unfairness of a contractual term shall be assessed, considering the nature of the goods or services for which the contract was concluded and *by referring, at the time of conclusion of the contract, to all the circumstances attending the conclusion of the contract* and to all the other terms of the contract or of another contract on which it is dependent' (our emphasis). Such circumstances would clearly include aspects of website design intended to deceive or manipulate the consumer's behaviour.

---

[75] Nicolo Zingales, 'Between a rock and two hard places: WhatsApp at the crossroad of competition, data protection and consumer law' (2017) 33(4) Computer Law & Security Review, 553, 556.

[76] Autorita' Garante della Concorrenza e del Mercato, 'Facebook fined 10 million Euros by the ICA for unfair commercial practices for using its subscribers' data for commercial purposes' 2019) <https://en.agcm.it/en/media/press-releases/2018/12/Facebook-fined-10-million-Euros-by-the-ICA-for-unfair-commercial-practices-for-using-its-subscribers'-data-for-commercial-purposes> accessed 9 April 2020

[77] Transparency requirements are also laid down in other laws which do not strictly form part of the consumer protection acquis; in particular, the e-Commerce Directive (discussed below).

[78] Case C-147/16 *Karel de Grote – Hogeschool Katholieke Hogeschool Antwerpen VZW v Susan Romy Jozef Kuijpers*, ECLI:EU:C:2018:320, paragraph 59.

[79] Case C-110/14 *Horațiu Ovidiu Costea v SC Volksbank România SA*, ECLI:EU:C:2015:538, paragraph 27.

[80] ibid para 27

It is instructive to note that the UCTD does not require that the consumer has to provide monetary consideration for a good or service:

> The Court has not considered monetary consideration to be necessary. (....) Therefore, contracts between consumers and providers of social media services must be considered to be covered by the UCTD regardless of whether consumers have to pay certain amounts of money or whether the consideration for the services consists in consumer generated content and profiling.[81]

Assuming this interpretation is correct,[82] the consideration does not have to be monetary. Nevertheless, a consideration is essential for a court of law to find the existence of a contractual relationship. This is relevant because dark patterns normally do involve a 'consideration' which is not normally monetary, but rather could take the form of sharing of personal data for tracking and profiling consumers. Thus, the regulatory strategy utilized by the UCTD is broadly different from the regulatory strategy utilized by other parts of the EU consumer protection law. Rather than focus on the contractual environment, it focuses on the substance of the agreement. On the other hand, the Consumer Rights Directive tackles any lack of transparency in the pre-contractual environment head on.

The Consumer Rights Directive

The Consumer Rights Directive (CRD) utilizes a regulatory strategy that does not concern itself with the substance of contractual terms, but rather with the environment in which contracting takes place. It is a horizontal instrument affecting all non-sectoral domestic and cross-border, consumer contracts, and also a 'maximum harmonisation' measure.[83] A prevalent form of dark pattern is one that results in *hidden costs* to the consumer. Hidden costs are clearly in breach of the Consumer Rights Directive. Articles 8(2) and 22 protect against inferring of consumer consent to additional charges through pre-checked boxes and the unintended conclusion of online contracts resulting from uninformed clicks.

Article 22 is particularly instructive here:

> Before the consumer is bound by the contract or offer, the trader shall seek the express consent of the consumer to any extra payment in addition to the remuneration agreed upon for the trader's main contractual obligation. If the trader has not obtained the consumer's express consent but has inferred it by using default options which the consumer is required to reject in order to avoid the additional payment, the consumer shall be entitled to reimbursement of this payment.

This article could be interpreted to mean that it cannot be inferred that a consumer has consented to providing personal data to the trader. This mirrors equivalent provisions of data protection legislation.[84] Rather, the trader must ensure that the consumer explicitly acknowledges an obligation to provide personal data; this interpretation is bolstered by the amendment to Article 3 CRD introduced by Directive 2019/261, discussed below.

The focus on transparency is also found in the CRD's pre-contractual information requirements.[85] Transparency militates against deceptive or manipulative practices. The CRD provides more detailed precontractual information requirements than the information requirements in Article 7(4) of the UCPD. For example, an invitation to purchase under the UCPD refers to both the information provided at the marketing stage (advertising) and before the contract is signed. In the latter case, there is an overlap between the information requirements under the UCPD and the more exhaustive pre-contractual

[81] Commission notice — Guidance on the interpretation and application of Council Directive 93/13/EEC on unfair terms in consumer contracts (Text with EEA relevance.) OJ C 323, 27.9.2019, p. 4–92.
[82] It is confirmed by the common position of national authorities within the network of enforcement authorities created under Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws [2004] OJ L 364/1, concerning the protection of consumers on social networks at http://europa.eu/rapid/press-release_IP-17-631_en.htm (November 2016) [Reg. 2006/2004 is repealed with effect from 17 January 2020, and replaced by Reg. 2017/2394.]
[83] For a detailed analysis of this Directive, see Christiana Markou, 'Directive 2011/83/EU on Consumer Rights' in Arno R. Lodder and Andrew D. Murray (eds.) *EU Regulation of E-Commerce: A Commentary* (Edward Elgar Publishing, 2017).
[84] General Data Protection Regulation, Art 4(11), generally and Art 7, specifically
[85] Consumer Rights Directive, Art 6

information requirements under the Consumer Rights Directive. As far as the content of the information is concerned, a trader that complies with the requirements laid down by the CRD for the pre-contractual stage will usually ensure compliance with Article 7(4) of the UCPD. However, information requirements in consumer protection law suffer from a similar malady found in data protection law. A trader may provide all the information, possibly even overload the consumer with information, complying with the letter of the law, while presenting this information in a manner that the consumer is likely to miss or ignore or misunderstand. This leads the consumer to take an action which he would not have otherwise taken and is not in her best interests.

A significant amendment to the Consumer Rights Directive introduced by Directive 2019/2161 is that the pre-contractual information requirements for distance contracts under Article 6 now include 'where applicable, that the price was personalised on the basis of automated decision-making'. Therefore, any price discrimination can no longer (once the new Directive applies) be hidden. The personal data on the basis of which the price is personalised may have been collected through a dark pattern mechanism. Awareness of the fact that a price is personalised may thus promote the uncovering of the use of dark patterns.

Article 3 CRD on the scope of the Directive has been amended by Directive 2019/2161 on better enforcement and modernisation of Union consumer protection rules: The Directive applies 'to any contract concluded between a trader and a consumer where the consumer pays or undertakes to pay the price'; the scope is extended to include 'payment' with personal data (but the term 'payment' is judiciously avoided). Article 4(2) Directive 2019/2161 provides that Article 3 CRD is amended, *inter alia*, by inserting a new paragraph 1a:

> This Directive shall also apply where the trader supplies or undertakes to supply digital content which is not supplied on a tangible medium or a digital service to the consumer and the consumer provides or undertakes to provide personal data to the trader, except where the personal data provided by the consumer are exclusively processed by the trader for the purpose of supplying the digital content which is not supplied on a tangible medium or digital service in accordance with this Directive or for allowing the trader to comply with legal requirements to which the trader is subject, and the trader does not process those data for any other purpose.

This wording reflects the wording already found in Article 3 Digital Content Directive. Thus, nominally 'free' services are brought within the reach of existing EU consumer protection laws and, in this instance, benefit from the right of withdrawal provided in Article 9 CRD.

Certain dark patterns will be directly regulated by amendments introduced to the CRD by Directive 2019/2161. A newly inserted Article 6a makes it an obligation for online marketplace providers to provide, before a consumer is bound by a distance contract or any corresponding offer, and without prejudice to the UCPD, the consumer with general information in a clear and comprehensible manner 'in a specific section of the online interface that is directly and easily accessible from the page where the offers are presented, on the main parameters determining ranking, as defined in point (m) of Art 2(1) of Directive 2005/29/EC, of offers presented to the consumer as a result of the search query and the relative importance of those parameters as opposed to other parameters'. For example, 'ranking' means the relative prominence given to products, as presented, organised, or communicated by the trader, irrespective of the technological means used for such presentation, organisation or communication'.[86] One could be deceived into believing that the ranking is organic, for example, as opposed to biased/influenced by paid advertising, and manipulated towards purchasing certain products, as a result of lack of transparency in this area. Other additional information requirements for contracts concluded on online marketplaces include 'whether the third party offering the goods, services or digital content is a trader or not, on the basis of the declaration of that third party to the provider of the online marketplace'.[87] This is important because the consumer is only protected under consumer protection laws when engaging in B2C transactions (and not if the consumer is transacting with another consumer,

[86] Unfair Commercial Practices Directive, Art 2(1)(m)
[87] Consumer Rights Directive, new Art 6a(1)(b)

C2C), which information must also be provided to the consumer.[88] With regard to these information requirements, the relevant provisions are of minimum (not maximum) harmonisation, as Member States are free to impose additional information requirements for providers of online marketplaces provided such provisions are proportionate, non-discriminatory, and justified on grounds of consumer protection.[89] These provisions, in promoting transparency, militate against deceptive and/or manipulative commercial practices.

The Unfair Commercial Practices Directive

The UCPD is an ambitious act of secondary legislation adopted with maximum harmonization in the field of consumer protection and applies to 'business-to-consumer commercial practices', which are defined as 'any act, omission, course of conduct or representation, commercial communication including advertising and marketing, by a trader, directly connected with the promotion, sale or supply of a product to consumers'.[90] It can be distinguished by its horizontal character (its rules apply to all types of products and services and to all methods of marketing and selling, whether online or offline[91]), and a combination of principle-based rules and specific prohibitions for certain practices. The fairness of a commercial practice is tested against a general prohibition of unfair commercial practices[92], elaborated with a prohibition of misleading and aggressive practices,[93] and a blacklist of practices which are unfair in every circumstance.[94]Commercial practices which do not affect the consumer's economic interests fall outside the scope of the UCPD.[95]

Certain dark patterns will amount to unfair commercial practices and will be prohibited under the UCPD. A newly inserted Article 6a makes it an obligation for online marketplace providers[96] to provide, before a consumer is bound by a distance contract or any corresponding offer, and without prejudice to the UCPD, the consumer with general information in a clear and comprehensible manner 'in a specific section of the online interface that is directly and easily accessible from the page where the offers are presented, on the main parameters determining ranking, as defined in point (m) of Art 2(1) of Directive 2005/29/EC, of offers presented to the consumer as a result of the search query and the relative importance of those parameters as opposed to other parameters'.[97] Ranking' means the relative prominence given to products, as presented, organised or communicated by the trader, irrespective of the technological means used for such presentation, organisation or communication'.[98] Some dark patterns affect consumers' economic interests; other instances may be less obvious. For example, by using online personal data acquired through a dark pattern to profile consumer behaviour, a consumers' economic interests are affected. Under the Directive, unfair commercial practices are those that are either contrary to the requirements of professional diligence, and will materially distort or are likely to materially distort the economic behaviour with regard to the product of the average consumer whom they reach or to whom they are addressed, or of the average member of the group when such commercial practices are directed to a particular group of consumers.[99] If a platform, webpage, or app is designed in a way that the dark pattern 'appreciably impairs the consumer's ability to make an informed decision, thereby causing the consumer to take a transactional decision that he would not have

[88] Consumer Rights Directive, new Art 6a(1)(c)
[89] Consumer Rights Directive, new Art 6a (2)
[90] Unfair Commercial Practices Directive, Art 2(d)
[91] European Parliamentary Research Service, 'Combating unfair commercial practices' (2013) <https://www.europarl.europa.eu/RegData/etudes/BRIE/2013/130533/LDM_BRI%282013%29130533_REV1_EN.pdf> accessed 11 April 2020
[92] Unfair Commercial Practices Directive, Art 5, Recitals 11 and 13
[93] Unfair Commercial Practices Directive, Art 6-7 and 8-9
[94] Unfair Commercial Practices Directive, Annex 1
[95] Unfair Commercial Practices Directive, Art 1
[96] Defined as 'a service using software, including a website, part of a website or an application, operated by or on behalf of a trader which allows consumers to conclude distance contracts with other traders or consumers.' Directive on Better Enforcement and Modernisation of Union Consumer Protection Rules, Article 3, Amendments to Directive 2005/29/EC Article 2.
[97] This information is regarded as material and its omission would also constitute a misleading omission in terms of the UCPD Article 7 new sub-article(4a) inserted by the Directive on Better Enforcement and Modernisation of Union Consumer Protection Rules.
[98] Unfair Commercial Practices Directive, Art 2(1)(m)
[99] Unfair Commercial Practices Directive, Art 5(2)(b)

taken otherwise'.[100] Some dark patterns will materially distort the economic behaviour of users. The term 'transactional decision' is defined under the Directive as 'any decision taken by a consumer concerning whether, how and on what terms to purchase, make payment in whole or in part for, retain or dispose of a product or to exercise a contractual right in relation to the product, whether the consumer decides to act or to refrain from acting.'[101] Taken together with 'commercial practice' in Article 2(d), dark patterns that materially distort, or are likely to materially distort the economic behaviour of a user, will fall under the scope of the Directive. When specific design features are created and implemented for the purpose of engaging users, the practice will be deemed unfair if the user enters into a transaction *or is likely to* make a decision that they would not have made without the use of the dark pattern.

The Directive is applicable to unfair B2C commercial practices[102] before, during, and after a commercial transaction in relation to a product.[103] A product is defined as any goods or service including immovable property, rights and obligations.[104] Consumer activities, therefore, are not restricted to 'products' in the literal sense, as the Directive defines 'products' very broadly.[105] A recent amendment expanded the definition of 'product' to include 'immovable property, digital service, and digital content, as well as rights and obligations'.[106] The scope and application of this Directive, therefore, is clearly different than, for example, that of the Unfair Contract Terms Directive and is more relevant in combating dark patterns. In particular, unfair commercial practices are those which are misleading[107] or aggressive.[108] As regards aggressive commercial practices, these are those which, in their factual context, taking account of all their features and circumstances, by harassment, coercion, including the use of physical force, or undue influence, significantly impair or are likely to significantly impair the average consumer's freedom of choice or conduct with regard to the product.'[109] Therefore, some dark patterns will amount to coercive practices which are a subset of aggressive commercial practices, which are themselves a subset of unfair commercial practices. The language of 'undue influence' may also be interpreted to encompass those dark patterns which are manipulative.

A misleading commercial practice may 'contain false information or is untruthful, or in any way, including *overall presentation*, deceives or is likely to deceive the average consumer, even if the information is factually correct' [Emphasis added].[110] Therefore, in the legal sense, deception, or a deceptive practice, is a subset of misleading commercial practices, which are themselves a subset of unfair commercial practices. A commercial practice will be misleading if it omits the material information that the average consumer needs to make an informed decision about whether to enter a transaction.[111] If the design causes a transactional decision that is based on inaccurate *material* information or is likely to cause the average consumer to take *a transactional decision that he would not have taken otherwise* [*italics* added], then the dark pattern will be misleading. The right to information is a basic consumer right; accordingly, any dark pattern that compromises the truthfulness, accuracy, or timeliness of information about the characteristics, price, and key conditions would amount to an unfair practice.

The commercial practices of an online platform must avoid any misleading actions[112] and omissions[113] whenever engaging in the promotion, sale, or supply of a product to consumers. Only those acts, omissions, course of conduct, representations or commercial communications can be considered as

[100] Unfair Commercial Practices Directive, Art 2(e)
[101] Unfair Commercial Practices Directive, Art 2(k)
[102] Unfair Commercial Practices Directive, as defined in Art 5
[103] Unfair Commercial Practices Directive, Art3(1)
[104] Unfair Commercial Practices Directive, Art 2(c)
[105]Geraint Howells, Hans-W. Micklitz and Thomas Wilhelmsson, *European Fair-Trading Law: The Unfair Commercial Practices Directive* (Routledge 2006) 66.
[106] Article 3 (Amendments to Directive 2005/29/EC) of the Directive on Better Enforcement and Modernisation of Union Consumer Protection Rules
[107] Unfair Commercial Practices Directive, Art 6 and 7
[108] Unfair Commercial Practices Directive, Art 8 and 9
[109] Unfair Commercial Practices Directive, Art 8
[110] Unfair Commercial Practices Directive, Art 6(1), see also Art 5(4)
[111] Unfair Commercial Practices Directive, Art 7
[112] Unfair Commercial Practices Directive, Art 6
[113] Unfair Commercial Practices Directive, Art 7

commercial practices that are directly connected with the promotion, sale, or supply of a product.[114] Failure to comply with these obligations could result in liability for unfair practices by the platform provider.

The average consumer benchmark in the unfair commercial practices law reflects the European Union's emphasis on information obligations and transparency as part of an effective consumer protection regime; however, this is not absolute. Traders engaging in business-to-consumer transactions are able to balance transparency and information obligations imposed by the UCPD against the fictional *average consumer*.[115] The 'average consumer' who is 'reasonably well-informed and reasonably observant and circumspect, considering social, cultural and linguistic factors'[116] is used as the basis for assessing the fairness of a trader's commercial practice. The concept has been developed by the CJEU: The Court has mandated that national courts determine, in light of all the relevant factors, whether the practice materially distorts the economic behaviour of the 'reasonably well-informed and reasonably observant and circumspect average consumer'.[117] There is always a presumption of how an average consumer is expected to behave as a key player in the market. Apart from the definition of 'average consumer' as the benchmark for the assessment of the fairness of a commercial practice, the UCPD provides a further test to protect the 'vulnerable' consumer 'whose characteristics make them particularly vulnerable to unfair commercial practices'[118]. This test is used as a benchmark for assessing the fairness of a commercial practice when it hinders the economic interests of such consumers.[119]

Can the UCPD be applied to dark patterns targeted at vulnerable people? In principle, yes. Art 5(3) specifically refers to 'credulity' as a practice that the trader could reasonably be expected to foresee to materially distort the economic behaviour of users. The term covers groups of consumers who may more readily believe specific claims. The term is neutral and circumstantial, so the effect is to protect members of a group who are for any reason particularly open to be influenced by a specific commercial practice. Any consumer can qualify as a member of this group. Recital 19 provides a non-exhaustive list of characteristics that make a consumer 'particularly susceptible'. A dark pattern designed to take advantage of credulity could see the practice qualify consumers as vulnerable, especially if proven that the user behaviour was foreseeable. A study by the European Commission into consumer vulnerability across key markets defined 'vulnerable consumer' as 'a consumer who as a result of…the market environment...is more susceptible to marketing practices'.[120] Accordingly, they should be adequately protected by assessing the practice from the perspective of the average member of that group.

Can the UCPD be applied to dark patterns generally? Again, yes. The first issue to be considered concerns the transparency of the commercial practice. Dark patterns can facilitate transactions whereby personal data is sold to third parties; data-driven commercial practices which harm consumers' economic interests will fall under the scope of the UCPD. For example, personal data is lawfully processed *inter alia* if consent has been given by the consumer or if the processing is necessary for the performance of the contract, or for the purposes of the legitimate interests pursued by the data controller.[121] If a data controller seeks to rely on consent as a ground for processing, it must be obtained prior to the processing of personal data.[122] Otherwise 'the processing carried out during the period of time from the moment the processing had started until consent is obtained would be unlawful'.[123] Under the UCPD, if a trader fails to disclose, or fails to disclose in a clear, intelligible and timely manner, that

[114] Unfair Commercial Practices Directive, Art 2(d)
[115] Art 6 and Art 7. In addition, furthermore, the Unfair Contract Terms Directive protects consumers against unfair standard contract terms imposed by traders. It applies to all kinds of contracts on the purchase of goods and services; for example, online or off-line-purchases of consumer goods, gym subscriptions or contracts on financial services, such as loans.
[116] Unfair Commercial Practices Directive, Recital 18
[117] For example, Case C-210/96 *Gut Springenheide GmbH and Rudolf Tusky v Oberkreisdirektor des Kreises Steinfurt - Amt für Lebensmittelüberwachung*,, ECLI:EU:C:1998:369 and Case C-220/98 *Estée Lauder Cosmetics GmbH v Lancaster Group GmbH*, ECLI:EU:C:2000:8.
[118] Unfair Commercial Practices Directive, Recital 18.
[119] Unfair Commercial Practices Directive, Art 5(3).
[120] Study on consumer vulnerability in key markets across the European Union (EACH/2013/CP/08) - see: <http://ec.europa.eu/consumers/consumer_evidence/market_studies/vulnerability/index_en.htm> accessed 10 April 2020.
[121] General Data Protection Regulation, Art 6(1).
[122] Article 29 Working Party, 'Guidelines on consent under Regulation 2016/679', (WP259, rev.01, 10 April 2018) 4
[123] Article 29 Working Party, 'Opinion 15/2011 on the definition of consent', (WP187, 13 July 2011) 31

personal data provided by the consumer will be processed and used for commercial activities of the trader, this would be a misleading *omission* and a violation of data protection law.

A trader that does not inform a consumer that their data will be sold to third parties could be committing a misleading omission of material information. More specifically, any dark pattern that hides the *commercial intent* behind a commercial practice could violate Article 7(2) and Point 22 of the blacklist found in Annex I. Information requirements are not just applicable to commercial communications: violations of transparency obligations under data protection legislation will be considered 'material' information in terms of the UCPD.[124] This could also be considered a violation of the EU data protection requirements to provide the required information to the individual concerned as to the purposes of the processing of the personal data.[125] By focussing on the decision-making capacity of the average consumer *ex-ante*, the UCPD rules can mitigate the effects of dark patterns and support the *ex-post* processing protections provided by the GDPR. Similarly, Riefa and Markou argue that businesses that fail to provide necessary information on the use of tracking technologies or disrespect the requirement to obtain any relevant consent would be committing an unfair commercial practice under the UCPD.[126] Furthermore, Article 7(1)'s prohibition on misleading omissions can be used to hold advertisers to account for insufficient advert labelling, protecting consumers from the risks associated with behavioural advertising.

Under the UCPD, a 'commercial practice shall be regarded as misleading if…it omits material information that the average consumer needs … to take an informed transactional decision...'. With regard to the dark pattern 'testimonials of uncertain origin' (identified at number (16) above) an amendment introduced to the UCPD by Directive 2019/2161provides that

> 6. Where a trader provides access to consumer reviews of products, information about whether and how the trader ensures that the published reviews originate from consumers who have actually used or purchased the product shall be regarded as material.

Thus, the absence of such information would constitute a misleading omission in terms of the UCPD.

Can the UCPD be applied to dark patterns in a strict liability sense, without consideration of any defences from the designer? Yes, the intention of the designer will not be considered. Article 8 provides an outright prohibition on several forms of dark patterns techniques. One way to establish a dark pattern is an aggressive practice is to show that there is 'coercion or harassment' that leads to an actual or likely 'significant restriction' on the average consumer's 'freedom of choice or conduct'.[127] Otherwise, it must be shown that there is 'undue influence', for which there must be 'exploitation' of a 'position of power' through 'pressure', which 'significantly' impairs (or is likely to so impair) the average consumer's 'freedom of choice or conduct', by 'significantly' limiting the ability of this average consumer to take an 'informed decision'. The wording used in Article 2(k), coupled with the language of the article, encourages the regulator to consider the entirety of circumstances in which a dark pattern operates. Because many dark patterns use a specific method to harass, coerce, or unduly influence users, they satisfy the requirement to show active conduct by the trader.[128] These all apply in the same way as strict liability offences – there is no *mens rea* requirement for regulators to consider. In the case of any practice claimed to be aggressive under the UCPD provisions, it must be shown that the result of the coercion, harassment or undue influence would be (or be likely to be) that consumers would take a transactional decision different to the one they would have taken otherwise.[129] Articles 8 and 9 also work in synchronicity with other consumer protection instruments. For example, Article 22 of the Consumer Rights Directive prohibits traders from using default options (that a consumer must uncheck)

[124]Unfair Commercial Practices Directive, Art 7(5)
[125] General Data Protection Regulation, Art 5 and Arts 12-14, Recital 58
[126] Christine Riefa and Christiana Markou, 'Online marketing: advertisers know you are a dog on the Internet!' in A Savin and J Trzaskowski (eds), *Research Handbook of EU Internet Law* (Edward Elgar Publishing Limited 2014) ch16.
[127] Unfair Commercial Practices Directive, Arts 8 And 2(j)
[128] State Council, Plenary Meeting – Judgment T 11 May 2012, N.14 - Pres. Courage - Est. Greek Judgment at <https://www.neldiritto.it/appgiurisprudenza.asp?id=8032&id=8032#.XpasjFMzZhE> accessed15 April 2020.
[129] Unfair Commercial Practices Directive, Art 8

to avoid additional payments. In a decision by the Latvian Consumer Protection Authority, the use of pre-ticked boxes was considered aggressive and not in compliance with professional diligence.[130]

The Gray *et al* typology of dark patterns (nagging, obstruction, sneaking, interface interference, and forced action) is reminiscent of aggressive commercial practices.[131] Designers have used dark patterns to persistently nag users into agreeing to various types of data-sharing, while others make withdrawing from a contract or their consent onerous. 'Persistence'[132] and 'making withdrawal from a contract onerous'[133] are both practices specifically referred to in Article 9 as examples of an aggressive commercial practice. Google's constant reminders to activate location services, Instagram's lack of a 'no' option, and unsolicited 'reminder' pop-ups from apps are characterized as 'persistent' dark patterns. Traders that nag consumers into providing consent through their apps' interface could be participating in an aggressive commercial practice. Hidden ad tracking and hard-to-cancel subscriptions amount to aggressive practices under Article 9(d). Making it appreciably harder to delay or impede a legal right like withdrawal from a contract or cancel consent to the processing of personal data could amount to an aggressive commercial practice.[134] 'Sneaking' dark patterns that force continuity, where one free month passes then morphs into a paid service[135]; default subscriptions, where something free is promised while hiding consequences of entering into the arrangement is buried in the fine print; and manipulative dropdown lists[136] could all amount to coercive practices. In *Wiltshire County Councils Trading Standards Department v. Jimmy Stockwell & Shane Stockwell*(unreported)[137], the presentation of information in a manner that is likely to deceive the customer amounted to an aggressive commercial practice under the United Kingdom's consumer protection regulations. Even requiring users to perform a certain action like subscribing to a newsletter to create an account to access certain functionality could amount to a coercive, aggressive commercial practice under certain circumstances if amounting to an onerous or disproportionate non-contractual barrier.

Can the UCPD be applied to traders using dark patterns irresponsibly? The UCPD can also be used in symbiosis with the industries it regulates. Article 10 encourages professional organizations to develop codes of conduct to hold members to account and apply the principles of the Directive effectively.[138] Several professional and industry codes can hold designers to account for the manipulative and unfair practices they build into user interfaces. For example, The Model Code of Professional Conduct for Designers requires members work to 'act in the client's interests within the limits of professional duties'.[139] The Institute of Electrical and Electronics Engineers (IEEE) Code of Conduct makes general reference to respecting 'the privacy of others and the protection of their personal information and data' and 'treating people fairly', and a more specific reference to 'avoid injuring others, their property, data,

[130] Decision of the Latvian Consumer Protection Authority, E03-PTU-K115-39 CRPC decision No. E03-PTU-K115-39 of 23.10.2012 against Air Baltic, at <http://www.ptac.gov.lv/sites/default/files/lieta_air_baltic_keksi_lemums_izraksts_23_10_12_2_.pdf> accessed 18 April 2020.

[131] Gray and others (n 3)

[132] Unfair Commercial Practices Directive, Art 9(a).

[133] Unfair Commercial Practices Directive, Art 9(d).

[134] PS8215, decision no 24117 of 12 December 2012; See also Supreme Court of Bulgaria, 3 November 2011, 15182/2011, VII d: http://www.sac.government.bg/court22.nsf/d6397429a99ee2afc225661e00383a86/4ade3b5386f5ef2cc225793b003048b3?OpenDocument and PS8215, decision no 24117 of 12 December 2012.

[135] Subscription traps' could also be a violation of the Unfair Commercial Practices Directive's Blacklist Point 29 of Annex I; See also Misleading « free » trials and subscription traps for consumers in the EU, at Misleading « free » trials and subscription traps for consumers in the EU: final report., (last visited 09 April 2020).

[136] Natalie Paris, 'Ryanair finally realizes "Don't Insure me" isn't a country' *The Telegraph* (London, 3 March 2015) <https://www.telegraph.co.uk/travel/news/ryanair/Ryanair-finally-realises-Dont-Insure-Me-isnt-a-country/> accessed 14 April 2020.

[137] Guidance on the Implementation/Application of Directive 2005/29/EC on Unfair Commercial Practices <https://e-justice.europa.eu/caseDetails.do?idTaxonomy=6518&idCountry=28&plang=en> accessed 18 April 2020

[138] See also Unfair Commercial Practices Directive, Recital 20

[139] International Council of Design, 'Best practice paper: model code of professional conduct for designers' <https://www.ico-d.org/database/files/library/icoD_BP_CodeofConduct.pdf> accessed 14 April 2020

reputation, or employment by false or malicious action'.[140] The Association for Computing Machinery's (ACM) Code of Ethics and Professional Conduct encourages members to 'Avoid harm'[141], "be transparent and provide full disclosure of all pertinent system capabilities, limitations, and potential problems to the appropriate parties"[142], and 'respect privacy' by establishing 'transparent policies and procedures that allow individuals to understand what data is collected and how it is being used, to give informed consent for automated data collection, and to review, obtain, correct inaccuracies in, and delete their personal data'.[143] This symbiosis is not just between the UCPD and industry codes of conduct. As more designers join these types of professional organizations, they become instrumental in setting the sector standard and evidential value of what amounts to professional diligence.[144] The UCPD will deem a dark pattern unfair if that commercial practice contradicts any code of conduct that serves as a specific mandatory requirement regulating the behaviour of traders.[145] Article 6(2)(b) states that a commercial practice will be misleading if 'in its factual context, taking account of all its features and circumstances, it causes or is likely to cause the average consumer to take a transactional decision that he would not have taken otherwise and…non-compliance by the trader with commitments contained in codes of conduct by which the trader has undertaken to be bound', if it is a firm, verifiable commitment.[146]

Dark patterns have brought renewed interest in the UCPD's role in regulating the entirety of the transactional process. Its tried, tested principles and three-tier structure to determine whether a commercial practice is unfair are well-documented and, as part of the old guard of consumer protection, the Directive certainly has a role to play in the regulation of dark patterns. Many of its provisions look ripe for reinterpreting and development for the appropriate regulation of commercial practices in the digital era. Other new consumer protection instruments seemed destined to have a more subtle and indirect effect on the inappropriate use of dark patterns.

E-Commerce Directive (2000/31/EC)

Like the Consumer Rights Directive, the E-Commerce Directive, while strictly not a consumer protection instrument but specific to digital environments, also contains transparency/information requirements.[147] Even if their effectiveness is limited, these are relevant in the context of the fight against dark patterns. Article 5(2), for example, provides that, 'In addition to other information requirements established by Community law, Member States shall at least ensure that, where information society services refer to prices, these are to be indicated clearly and unambiguously and, in particular, must indicate whether they are inclusive of tax and delivery costs.'

According to Article 14 of the e-Commerce Directive, intermediaries such as online marketplace operators may not benefit from the immunity cover provided by Article 14 and may be liable, not only for primary infringement of consumer protection law provisions, but also for secondary (contributory, vicarious) infringement for the activities of the users of their platform.[148] A hosting service provider is not liable for the information stored at the request of a user of the service, on condition that the provider does not have actual knowledge of illegal activity or information and is not aware of facts or circumstances from which the illegal activity is apparent[149] or, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.[150] However, Article

[140] IEEE Code of Conduct <https://www.ieee.org/content/dam/ieeeorg/ieee/web/org/about/ieee_code_of_conduct.pdf> accessed 14 April 2020
[141] Section 1.2
[142] Section 1.3
[143] Section 1.6
[144] Unfair Commercial Practices Directive, Art 5(2)
[145] Unfair Commercial Practices Directive, Recital 20
[146] Unfair Commercial Practices Directive, Art 6(2)(b)(i)
[147] e-Commerce Directive, Art 5 ('general information to be provided'); 6 ('information to be provided') within section 2 on commercial communications; and 10 ('information to be provided') within section 3 on contracts concluded by electronic means.
[148] Cf. Judgment of 12 July 2011, *L'Oréal SA and Others v eBay International AG and Others*, Case C-324/09, ECLI:EU:C:2011:474.
[149] e-Commerce Directive Art 14(1)(a)
[150] e-Commerce Directive Art 14(1)(b).

14(3) states that a court or administrative authority may nevertheless require the service provider to terminate or prevent an infringement. Recital 40 further clarifies: 'service providers have a duty to act, under certain circumstances, with a view to preventing or stopping illegal activities'. Riefa has argued that online auction platforms' liability can feasibly be extended to encompass consumer law, concluding that:

> 'It is possible to envisage an even wider liability regime, forcing intermediaries to also ensure against the use of unfair commercial practices or unfair terms on their platforms. This is not yet possible and some amendments to legislation are necessary to make it a reality, but it could provide a viable solution in the future.'[151]

However, this proposition is not unproblematic or uncontroversial. It is uncertain whether consumer protection law could be enforced against secondary infringers. Moreover, unlike in instances of intellectual property infringement where the Directive on the Enforcement of Intellectual Property Rights provides for the possibility of an injunction against intermediaries whose services are used by a third party to infringe an intellectual property right, EU consumer protection law does not provide for the possibility of an injunction against intermediaries whose services are used by a third party to infringe consumer protection law.[152] Therefore, if a dark pattern is deployed by a trader operating on an intermediary platform, it is uncertain whether the intermediary platform may be held responsible and/or an injunction issued against it.

Nevertheless, in the wake of the COVID-19 public health crisis, online intermediary service providers such as social media, search engines, and marketplaces were called upon by the European Commission and the Consumer Protection Cooperation (CPC) network (discussed further below) to better identify scams and unfair practices happening on their platforms, to take them down, and prevent similar ones reappearing.[153] While the action taken was not specifically directed at dark patterns, it was directed as deceptive marketing techniques on online platforms deployed to exploit consumers' fears to sell products associated with the prevention and/or cure of an infection from the COVID-19 virus. The provisions of Article 14, in conjunction with the requirement of 'professional diligence' laid down in Article 5 UCPD and the proscription of misleading commercial practices under Articles 6-7 and of aggressive commercial practices under Articles 8-9, were brought to bear as additional tools in the hands of the consumer protection authorities. Taken together, this suggests that the UCPD and the e-Commerce Directive can be used to ensure online platforms provide a fair marketplace environment for consumers.

Furthermore, as noted by the CJEU, advertising transparency comes under the remit of Article 6 of the e-Commerce Directive.[154] Riefa and Markou opine that it is also possible to venture and spread beyond trademark law into unfair commercial practices territory to find adequate protection for consumers against misleading keyword advertising.[155]However, the role of the UCPD in this context remains untested and may only have limited impact. If the conditions in Article 14, as interpreted in the *Google France* preliminary ruling are not met, the platform provider could be held liable for the activity of traders on its platform. As noted, a limitation of this argument is that once the safe harbour provided by Article 14 is lost, primary or secondary liability on the part of the platform provider would need to be established. To be successful, one would need to make out a case on contributory or vicarious liability

---

[151] Christine Riefa, *Consumer Protection and Online Auction Platforms: Towards a Safer Legal Environment* (Ashgate 2015) 221.

[152] Art 11, Directive 2004/48/EC of 29 April 2004 on the enforcement of intellectual property rights OJ L 157/45; see also Art 8(3), Directive 2001/29/EC of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, OJ L167/10

[153] European Commission/ Consumer Protection Cooperation (CPC) Network, 'Common Position of CPC Authorities: Stopping scams and tackling unfair business practices on online platforms in the context of the Coronavirus outbreak in the EU' (2020) <https://ec.europa.eu/info/sites/info/files/live_work_travel_in_the_eu/consumers/documents/cpc_common_position_covid19.pdf> accessed 2 June 2020

[154] *Google France SARL and Google Inc. v Louis Vuitton Malletier SA* (C-236/08), *Google France SARL v Viaticum SA and Luteciel SARL* (C-237/08) and *Google France SARL v Centre national de recherche en relations humaines (CNRRH) SARL and Others* (C-238/08) ECLI:EU:C:2010:159

[155] Riefa and Markou (n 126)

of the platform provider for the activities of the traders using the platform. Vicarious liability could theoretically be argued on the basis that the platform is able to control the activities of its traders by 'pulling the plug'; for example, removing an infringing advertisement. Platforms such as Amazon AWS, could be held liable/responsible as a primary infringer, or as secondary (contributory or vicarious) infringer for the activities of traders using the marketplace platform.

Part III: Redress and Enforcement Against Dark Patterns

Under the EU Directives discussed above, there is a general obligation for Member States to ensure that 'adequate and effective means exist' in order to ensure compliance with the Directives in the interests of consumers.[156]Collectively, the Consumer Rights Directive, the Unfair Contract Terms Directive, and the Unfair Commercial Practices Directive could play a substantial part in the regulation of dark patterns. However, the application of consumer protection law without increasing the ability to enforce the regime will only lead to frustration and disappointment. The limitations of extant enforcement mechanisms have long been identified as compromising the effectiveness of the consumer protection regime.[157] Accordingly, this section will discuss how further development and interpretation of the enforcement regime could inhibit the deployment, use of, and/or stop abusive dark patterns.

The Unfair Contract Terms Directive

In the context of dark patterns, the UCTD's first remedy may not be helpful: Under Article 6(1) 'unfair terms used in a contract concluded with a consumer by a seller or supplier shall, as provided for under their national law, not be binding on the consumer and the contract shall continue to bind the parties upon those terms if it is capable of continuing in existence without the unfair terms.' Moreover, Member States must take the 'necessary measures' to ensure that a consumer in the Union does not lose the protection granted by this Directive as a result of a choice of law clause in the contract, where the contract has a close connection with the territory of the Member States.[158] While the unfair clauses in contracts entered into by a consumer as a result of a dark pattern will not be binding on the consumer (irrespective of the existence of a dark pattern or otherwise), very often this is not the remedy a consumer needs; for example in the case of the dark patterns termed 'privacy zuckering' or 'forced continuity' and others, because although the unfair clauses may not be binding, enforcement will not be a simple matter.

However, more importantly, the UCTD aims to deter sellers or suppliers from using unfair terms in the future: 'the objective is to restore the balance between the parties and have a future dissuasive effect on the seller or supplier'.[159] Under Article 7(1) 'in the interests of consumers and of competitors, adequate and effective means exist to prevent the continued use of unfair terms in contracts concluded with consumers by sellers or suppliers.' The means 'shall include provisions whereby persons or organizations, having a legitimate interest under national law in protecting consumers, may take action according to the national law concerned before the courts or before competent administrative bodies for a decision as to whether contractual terms drawn up for general use are unfair, so that they can apply appropriate and effective means to prevent the continued use of such terms.'[160] 'With due regard for national laws', the legal remedies may be directed separately or jointly against a number of sellers or suppliers from the same economic sector or their associations which use or recommend the use of the

[156] Unfair Contract Terms Directive Article 7, Unfair Commercial Practices Directive Article 11; Consumer Rights Directive Article 23.
[157] European Commission (2012). Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and The Committee of the Regions: A European Consumer Agenda - Boosting Confidence and Growth (No. COM (2012) 225 final). Brussels: European Union at Section 3.4; See also Inge Graef, Damian Clifford, Peggy Valcke, 'Fairness and enforcement: bridging competition, data protection, and consumer law' (2018) International Data Privacy Law 8(3) 200-223 at 223.
[158] Unfair Contract Terms Directive, Article 6(1).
[159] Opinion of Advocate General Petronella in Case C-260/18 *Kamil Dziubak, Justyna Dziubak v Raiffeisen Bank International AG z sidebar w Wiedniu, prowadzacy działalność w Polsce w formie oddziału pod nazwą Raiffeisen Bank International AG Oddział w Polsce*, formerly *Raiffeisen Bank Polska SA z siedzibą w Warszawie*, paragraph 53.
[160] Unfair Contract Terms Directive, Art 7(2)

same general contractual terms or similar terms.[161] Prior to the amendments introduced by Directive 2019/2161 discussed below, the UCTD contained no provision for penalties.

The Unfair Commercial Practices Directive

Under Article 11 of the UCPD, the means to combat unfair commercial practices must include legal provisions under which persons or organisations regarded under national law as having a legitimate interest in combating unfair commercial practices, including competitors, may: take legal action against such unfair commercial practices; and/or bring such unfair commercial practices before an administrative authority competent either to decide on complaints or to initiate appropriate legal proceedings (our emphasis). The UCPD explicitly states that competitors can play a role in enforcement as the Directive acknowledges that 'legitimate competitors' may also be indirectly harmed by unfair commercial practices aimed at consumers.[162] It demonstrates that competitors can also play a role in enforcing EU law that is primarily aimed at the protection of other parties from dark patterns. However, the facilities in terms of enforcement action are not fully harmonised and can vary between Member States.[163] The Member States may for example require prior recourse to other established means of dealing with complaints, including control bodies of codes of conduct.[164] As with the UCTD, it is for the Member States to decide whether these legal facilities may be directed separately or jointly against a number of traders from the same economic sector; and whether they may be directed against a code owner where the relevant code promotes non-compliance with legal requirements.[165]

The remedy provided for under the UCPD is for a court or administrative authority to order the cessation, or to institute legal proceedings for an order for the cessation, of unfair commercial practices; or if the unfair commercial practice has not yet been carried out but is imminent, to order the prohibition of, or to institute legal proceedings for an order for the prohibition of, the practice, even without proof of actual loss or damage or of intention or negligence on the part of the trader.[166] These remedies are important in the context of prohibiting or stopping dark patterns which harm or pose a threat of harm to consumers even before any contractual transaction may have been entered into. The amendments introduced by Directive 2019/2161 include a new Article 11a inserted into the UCPD that will provide consumers harmed by unfair commercial practices with access to 'proportionate and effective remedies, including compensation for damage suffered by the consumer and, where relevant, a price reduction or the termination of the contract'. It remains to be seen how and to what extent these new remedies would be applied by national courts and/or administrative authorities in situations where the consumer is harmed by dark patterns. With regard to damage suffered by the consumer, the damage suffered by any individual consumer may be minimal, which highlights the importance of the availability of class actions, something the EU is poised to legislate for, as discussed below.

The Consumer Rights Directive

Under the Consumer Rights Directive the means to ensure compliance with the Directive must include provisions whereby public bodies or their representatives and/or consumer organisations having a legitimate interest in protection consumers and/or professional organisations having a legitimate interest in acting, as determined by national law, may take action under national law before the courts or competent administrative bodies to ensure that the national provisions transposing the Directive are applied.[167]

Penalties

The UCTD, the CRD and the UCPD have been amended by Directive 2019/2161 on better enforcement and modernisation of Union consumer protection rules. The reform introduces an obligation for Member States under all three Directive to provide for 'effective, proportionate and dissuasive'

[161] Unfair Contract Terms Directive, Article 7(3)
[162] Unfair Commercial Practices Directive, Recitals 6 and 8
[163] Unfair Commercial Practices Directive, Art 11(1)
[164] Unfair Commercial Practices Directive, Art 11(1)
[165] Unfair Commercial Practices Directive, Art 11(1)
[166] Unfair Commercial Practices Directive, Art 11(2)
[167] Consumer Rights Directive, Article 23

penalties in case of infringements;[168] under the UCTD, such penalties may be restricted 'to situations where the contractual terms are expressly defined as unfair in all circumstances in national law or where a seller or supplier continues to use contractual terms that have been found to be unfair in a final decision taken in accordance with Article 7(2)'.[169] Furthermore, the reform provides for increased financial sanctions for non-compliance. When penalties are to be imposed in accordance with Article 21 of Regulation 2017/2394, the maximum fine must be at least 4% of the seller's or supplier's annual turnover in the Member State(s) concerned. If information on maximum turnover is not available, the maximum amount of the fine must be at least €2 million.[170] The teeth of the consumer protection regime are not any less sharp than those of the GDPR; however, it should be noted that the GDPR-like penalties apply only if there is a coordinated enforcement action by the network on national consumer authorities which, BEUC notes, reduces the likelihood of these higher penalties being imposed.[171] Nevertheless, the reform does generally give authorities and courts more teeth to protect consumers and deter traders from bad behaviour.

The Directive on injunctions for the protection of consumers interests

The scope of the Directive on injunctions for the protection of consumers interests,[172] ('Injunctions Directive') covers actions for an injunction 'aimed at the protection of the collective interests of consumers included in the Directives listed in Annex I.'[173] The Annex includes the Unfair Terms in Consumer Contracts Directive, the e-Commerce Directive, the Unfair Commercial Practices Directive, the Consumer Rights Directive, and others. Injunctions are important in the enforcement of consumer protection law as they provide an effective tool to consumer protection authorities and organisations to stop unlawful practices. Nevertheless, this 'closed list' can be problematic, because injunctions may not be available when, for example, the consumer interest concerned is protected under data protection legislation.[174] Therefore, in some EU countries, breaches of data protection law may not be the subject of injunctions issued by consumer protection authorities or associations (the German legislature amended the law to specifically allow for this.[175]) This is possible because the Directive does not prevent Member States from adopting or maintaining in force provisions designed to grant qualified entities and any other person concerned more extensive rights to bring action at national level.[176]

Assuming that a dark pattern has been identified as an act contrary to the Directives listed in Annex 1 as transposed into the internal legal order of the Member States, and which harms the collective interests of consumers, the Injunctions Directive allows a consumer authority or association to file for an injunction prohibiting the continued use of the dark pattern.

According to Article 2 of the Injunction Directive, 'qualified entities' (essentially consumer authorities and associations[177]) may commence proceedings before a court or administrative authority (as designated by the Member States) seeking: (a) an order with all due expediency requiring the cessation or prohibition of any infringement; (b) where appropriate, measures such as the publication of the decision and/or the publication of a corrective statement with a view to eliminating the continuing effects of the infringement; and (c) in so far as the legal system of the Member State concerned so permits, an order against the losing defendant for payments into the public purse or to any beneficiary designated in or under national legislation, in the event of failure to comply with the decision within a

[168] Unfair Contract Terms Directive, New Article 8b; Unfair Commercial Practices Directive, New Article 13; Consumer Rights Directive, new Article 24
[169] Unfair Contract Terms Directive, New Art 8b (2)
[170] Unfair Contract Terms Directive, new Article 8b (4) and (5); Unfair Commercial Practices Directive, new Article 13(3) and (4); Consumer Rights Directive, new Article 24(3) and (4)
[171] Deal reached to improve enforcement of consumer law, <https://www.beuc.eu/publications/deal-reached-improve-enforcement-consumer-law/html> accessed 25 May 2021.
[172] Directive 2009/22/EC of the European Parliament and of the Council of 23 April 2009 on injunctions for the protection of consumers' interests (Codified version) Text with EEA relevance OJ L 110/30 ('Injunctions Directive')
[173] Injunctions Directive, Art 1(1).
[174] Peter Rott and Axel Halfmeier, 'Reform of the Injunctions Directive and Compensation for Consumers: Study commissioned by BEUC' (2018) <https://www.beuc.eu/publications/beuc-x-2018-022_reform_of_the_injunctions_directive_and_compensation_for_consumers.pdf>, accessed 10 April 2020
[175] Ibid, referencing § 2 para. 2 sentence 1 no. 11 Injunctions Act.
[176] Injunctions Directive, Art 7
[177] Injunctions Directive, Art 3

time limit specified by the courts or administrative authorities, with a view to ensuring compliance with the decisions.[178] It is noticeable that this Directive does not provide for a mechanism for damages to be paid to consumers on account of the period during which the dark pattern was in operation:

> 'This 'enforcement gap' works not only to the detriment of the affected consumers who are not compensated for their losses, but it may also have negative social consequences as the deterrence potential of an injunction procedure is very limited, while in contrast the threat of a possible payment of damages to a large number of affected consumers may serve as a stronger deterrent against unlawful behaviour by businesses'.[179]

To effectively combat dark patterns, consumers who have been affected by the relevant infringement should have a right to compensation, an approach favoured by a recent study in the context of the EU law 'Fitness Check'.[180] As we have seen, the possibility of compensation for damage as a remedy has been provided for in the new Article 11a of the UCPD.

The provisions of the Injunctions Directive are without prejudice to 'the rules of private international law with respect to the applicable law; that is, normally, either the law of the Member State where the infringement originated or the law of the Member State where the infringement has its effects.'[181] This provision is especially relevant when the trader operating a particular website is outside of the EU, so that the laws of the EU may still be enforceable against that trader.

The Regulation on cooperation between national authorities responsible for the enforcement of consumer protection laws

The Regulation on cooperation between national authorities responsible for the enforcement of consumer protection laws[182] ('CPC Regulation') lays down a cooperation framework for national authorities to be able to effectively deal with breaches of consumer protection legislation in situations in which the trader and the consumer are established in different countries of the European Economic Area. Collectively the authorities form a European enforcement network, the 'CPC Network', coordinated by the European Commission. The latter can alert the CPC network and coordinate EU-wide enforcement against a trader responsible for 'widespread infringement' (defined in article 3(3)) or 'widespread infringement with a Union dimension'[183], to bring about the cessation or prohibition of that infringement.[184] Where appropriate, the competent authorities will impose penalties; with the entry into application of the Directive on Enforcement and Modernisation of Consumer Law[185] the maximum amount of fines will be at least 4% of the turnover of the businesses in the Member States concerned or at least EUR 2 million where information on the trader's annual turnover is not available, where penalties are imposed in accordance with Article 21 of this Regulation: these include sanctions for breaches of the Unfair Terms in Consumer Contracts Directive,[186] the Unfair Commercial Practices Directive,[187] and the Consumer Rights Directive.[188] The importance of this cooperation framework is for national authorities to be able to deal effectively with instances of data patterns which have a cross-border or Union dimension, including EU-wide enforcement against a trader responsible for the deployment of a dark pattern.

[178] Injunctions Directive, Art 2(1)
[179] Reform of the Injunctions Directive and Compensation for Consumers: Study commissioned by BEUC, p.4.
[180] Civic Consulting, Study for the Fitness Check of EU consumer and marketing law – Final report Part 1 (May 2017), at 286, referenced also in the Study commissioned by BEUC.
[181] Injunctions Directive, Art 2(2)
[182] Regulation (EU) 2017/2394 of the European Parliament and of the Council of 12 December 2017 on cooperation between national authorities responsible for the enforcement of consumer protection laws and repealing Regulation (EC) No 2006/2004 (Text with EEA relevance) OJ L 345/1
[183] As defined in Art 3(4).
[184] *Ibid*, Art 21.
[185] Directive on Better Enforcement and Modernisation of Union Consumer Protection Rules
[186] ibid Art 1 (new Art 8b to be inserted in Directive 93/13/EEC).
[187] ibid Art 3 (Art 13 of Directive 2005/29/EC to be replaced by a new Art 13 - Penalties).
[188] ibid Art 4 (Art 24 of Directive 2011/83/EU to be replaced by a new Art 24 - Penalties).

The Directive on representative actions for the protection of the collective interests of consumers, and repealing Directive 2009/22/EC

The Directive on representative actions for the protection of the collective interests of consumers[189]('Collective Redress Directive') introduces 'class action' style litigation for consumers across the EU. The overall aim of the Directive is to strengthen enforcement of EU consumer law. A detailed analysis of this proposal is beyond the scope of this paper. Suffice to say that, when applicable, this law will represent a stronger enforcement mechanism against dark patterns than that available under Article 80 of the GDPR, which only provides for the right of the data subject to mandate a not-for-profit body, organisation, or association to exercise the right to receive compensation referred to in Article 82 on his or her behalf *as provided for by Member State law* (our emphasis).

Conclusion

By purposely moving away from terms commonly found in the design literature to describe dark patterns, this article has put these and other techniques into the language of consumer protection regulators. The analysis reveals that, when used appropriately, the regime could have significant potential restraining the deployment of manipulative design features that affect users across the pre-contractual, contractual, and post-contractual environments found embedded in user interfaces and system architectures. Most of the academic scholarship in this area has focused on the data protection regime; however, it is not only clear that consumer protection legislation is perfectly capable of standing on its own as a powerful enforcer against dark patterns but, in some instances, offers even more protection and enforcement opportunities than the GDPR.

In some cases, the proscription of the dark pattern will be clear cut; others will require further development of the law. Some will need creative interpretations by regulators in order to stop the abusive practice. With enhanced harmonisation, a new right to individual remedies when they are harmed by unfair commercial practices, and enhanced protection of consumers using 'free' digital services, the consumer protection regime is set to remove its reputational shackles as 'ineffective' and become an important enforcer against the use of abusive dark patterns. Fortunately, the flexibility in adopting specific additional measures to respond to 'rapid technological developments concerning online marketplaces' is likely to be written into the modernization of the consumer protection rules.[190] Any future upgrade should incorporate recognition that the technological environment for transacting, generally, and the user interface, specifically, is central to the examination of whether a commercial practice is unfair.

The long-needed modernisation reflects recognition and concern that online marketplaces and interfaces are increasingly using data as the quantum for access to the 'free' good and/or service. With the prohibitive structure of the data protection regime arguably contributing to the rise of dark patterns, emphasis should shift onto interactions between traders/data controllers and consumers to assess the *process* of obtaining a legal ground of data processing and/or how pre-contractual arrangements were influenced by technological tricks and design techniques. Consumer protection is uniquely qualified and in a better position to do so than the data protection regime.

Possibly the most challenging aspect of consumer protection law is to remedy how poorly it has been enforced to date. The ongoing reform of the consumer protection regime, and of the Directives on unfair contract terms, unfair commercial practices, and consumer rights in particular, is welcomed. It represents the introduction of much needed and stronger remedies and enforcement capabilities into the digital single market. The toughness of the sanctions regime may also provide a significant and immeasurable deterrent effect on the use of abusive dark patterns. Aimed at the protection of the collective interests of consumers, the availability of injunctions is an important element of the enforcement regime. It provides consumer protection authorities and organisations with an effective tool to stop the continued use of dark patterns. As websites that deploy dark patterns will likely be accessible from anywhere in the Union, with the possibility of harmful consequences in several or all Member States, cooperation between national authorities responsible for the enforcement of consumer

[189] Directive 2020/1828 of 25 November 2020 on representative actions for the protection of the collective interests of consumers, and repealing Directive 2009/22/EC, OJ L 409/1

[190] Directive on Better Enforcement and Modernisation of Union Consumer Protection Rules, Recital 29

protection laws across the EU, as provided by the CPC Regulation, is another important enforcement tool. Finally, the Collective Redress Directive, which will introduce ‘class action’ style litigation for consumers across the EU, will constitute a markedly more appropriate procedure to combat dark patterns than the limited possibilities for representation of data subjects provided for under Article 80 of the GDPR.