'Dark Patterns': The Case for Regulatory Pluralism between the European Union's Consumer and Data Protection Regimes

Dr M.R. Leiser

Abstract

"Dark patterns" is a generic term used by the design community and an increasing number of data protection academics to describe a variety of manipulative design techniques that compromise legal requirements like consent and privacy-by-design and legal principles like fairness and transparency. To assess the regulation of dark patterns, two legal frameworks of the European Union are compared and critiqued: first, an examination of relevant rules and principles of the General Data Protection Regulation (GDPR) leads to the conclusion that the principle of data-protection-by-design could be useful, but the lack of clarity about what constitutes fairness undermines the GDPR's ability to regulate dark patterns. Second, an examination of the 'fairness' principle in the EU's consumer protection acquis reveals a significantly further developed regime. After examination of the various enforcement mechanisms across both regimes, the Chapter concludes that a pluralistic approach that mixes the strengths of one regulatory regime while compensating for the weaknesses of the other is needed to harness manipulative design techniques like dark patterns.

Keywords: dark patterns, consumer protection, data protection, law, regulation

Introduction

'Dark patterns' is a term commonly used by the web collective to describe a user interface that exploits users into doing something that they would not normally do. It is a coercive and manipulative design technique typically used by web designers when some sort of action is needed from a user; for example, to begin the processing of personal data or indicate agreement to a contract. Via specific design choices, many e-commerce and social media platforms prioritize capturing user attention while obfuscating information that might help them make more informed decisions. These techniques, including unbalanced design, information overload, fine-tuned personalization, and distorted social cues, pave the way for the manipulation of users and compromise rational decision-making. Scholarship from the fields of computer science, consumer law, and data protection have categorized the different ways users are tricked, dazzled, and decoyed into everything from providing consent to the processing of personal data to entering transactions to making purchases that they would not undertake without the use of a dark pattern.[1]

By adopting creative metaphors like 'roach motel', 'misdirection', 'confirm-shaming', 'bait-and-switch' and so on to describe tricks of the trade, scholarship from design ethics is largely responsible for increased awareness about the kinds of dark patterns used to manipulate users.[2] However, the adoption of these terms by European regulators is inappropriate for several reasons. First, term inflation risks amalgamating all forms of manipulative design under the scope of one regulatory regime. Second, the

[1] Christoph Bösch and others, 'Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns' [2016] 4(4) Proceedings on Privacy Enhancing Technologies <https://petsymposium.org/2016/files/papers/Tales_from_the_Dark_Side__Privacy_Dark_Strategies_and_Privacy_Dark_Patterns.pdf> accessed 2 July 2021; Lothar Fritsch and others, 'Privacy dark patterns in identity management' [2017] 0(0) Lecture Notes in Informatics (LNI) 93-104 On data protection: Midas Nouwens and others, 'Dark Patterns After The GDPR: Scraping Consent Pop-Ups And Demonstrating Their Influence', Association for Computing Machinery (ACM 2020)<https://dl.acm.org/doi/pdf/10.1145/3313831.3376321?casa_token=fDsPakcJwQUAAAAA%3A5p2usbRAr38SO8uMnfoX5xBE9-hh_JVVsak59KKRzVdhBZpmrjh2hY5Ac_vouC447mtHvU6UcxDj> accessed 2 July 2021.; Clifford, D. (2017). On Consumer Protection: Gesellschaft für Informatik; Lior Strahilevitz et al., Subcommittee report: Privacy and data protection, Stigler Center Committee for the Study of Digital Platforms 22-23 (2019).

[2] 'Dark Patterns: Submission By Design?' (Medium, 2021) <https://uxdesign.cc/dark-patterns-submission-by-design-6f61b04e1c92> accessed 2 July 2021

term ‘dark patterns’ runs the risk of getting overused to describe features of websites that we simply do not like or are a matter of poor UX design. Third, the design literature is very precise - dark patterns are deceptive and manipulative *choices* made by designers to get users to do something; however, both the consumer and data protection frameworks are clear - one does not have to prove *intent* to hold a data controller or a trader accountable for failing to live up to their respective obligations under either framework. Accordingly, this paper moves away from terminology of the design community and adopts the vernacular of European regulators for data and consumer protection.

The preventative nature of the regulatory framework for the protection of personal data requires data controllers to satisfy one of legitimate grounds for processing.[3] For example, users are required to provide positive indication of their consent to processing[4] or that they agree to enter a contract.[5] Unsurprisingly, dark patterns have emerged a manipulative means of nudging users toward satisfying the legal conditions required to process personal data. Because it is seen as regulating data controllers’ behaviour directly, the GDPR is increasingly, and arguably erroneously, seen as applicable to the entirety of the user experience.[6] This is not necessarily a shortcoming of the regime: Regulating controllers is one way of ensuring the GDPR is enforceable, effective, and relevant as technology progresses. But these formal requirements contain complex standards enforced by specialised government agencies.[7] The GDPR may contain virtues of dependability and predictability (if adequately enforced), it often proves to be inflexible and inefficient, and its proponents are left to resort to having to delve into creative interpretations of its provisions to get the ‘right’ outcome. Against this backdrop, this paper critiques the ability of the regulatory frameworks (consumer and data protection) of the European Union to constrain design techniques embedded in websites that facilitate the practice of both anti-privacy functionality and the entering into a contractual agreement that would not have happened without the use or influence of the dark pattern.

What are ‘dark patterns’?

‘Dark patterns’ are ‘interface design choices that benefit an online service by coercing, steering, and/or deceiving users into making decisions that, if fully informed and capable of selecting alternatives, they might not make’.[8] Most dark patterns have been categorized into those that obfuscate interface elements that could be theoretically used to protect user privacy, and those that hide disclosures that, had they been known and understood, might affect whether a typical user would enter into a transaction. However, dark patterns can be any manipulative design technique. Unbalanced accept/reject buttons, or even sensory overload could also be a dark pattern - if the design does something that causes the user to do something that the user would not have done without the design technique. Why are dark patterns so problematic? One aspect of the digital single market is to provide a competitive environment for data-driven businesses. Dark patterns contribute to a new kind of 'race to the bottom' as businesses become more willing to forgo other obligations to capture user consent and/or agreement.

---

[3] 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), O.J. L 119 of 4.5.2016 (hereafter General Data Protection Regulation), art 6(1)

[4] General Data Protection Regulation, art 6(1)(a)

[5] General Data Protection Regulation, art 6(1)(b)

[6] de Hert, P., & Gutwirth, S. (2009). Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action. In Serge Gutwirth, Yves Poullet and Paul de Hert, Reinventing Data Protection? (Springer Netherlands 2009; For further criticism see B.-J. Koops, 'The Trouble With European Data Protection Law' (2014) 4(4) International Data Privacy Law, 250-261.; N. Purtova, 'The Law Of Everything. Broad Concept Of Personal Data And Future Of EU Data Protection Law' (2018) 10 Law, Innovation, and Technology.

[7] Michiel Rhoen, 'Beyond Consent: Improving Data Protection Through Consumer Protection Law' (2016) 5 Internet Policy Review

[8] Arunesh Mathur and others, 'Dark Patterns At Scale: Findings From A Crawl Of 11K Shopping Websites: Proceedings Of The ACM On Human-Computer Interaction: Vol 3, No CSCW' (Dl.acm.org, 2021) <https://dl.acm.org/doi/10.1145/3359183> accessed 2 July 2021. 81; See also 'Report: Deceived By Design' (Forbrukerrådet, 2021) <https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/deceived-by-design/> accessed 2 July 2021

Most dark patterns manifest themselves in user interfaces, but some can be found at system level. The risks arising from this type of system architecture design are amplified when its sources and intentions remain hidden: when users are subjected to customized architecture and dark pattern tactics, they cease to be subject to not only regulatory scrutiny, but make decisions that go against their interest, and, on occasion, harm the entire digital ecosystem. Other more nefarious dark patterns exist within system architecture and are used to push users in certain directions. Some use design to deflect users away from making rational decisions about the use of their personal data (e.g., persistent pop-ups, attention grabbing graphics, and insights from eye-tracking and neuromarketing) to nag users into accepting terms and conditions or grant consent. Others will use information overload to overwhelm users with complex and confusing offers or choices. Some dark patterns brazenly place goods into e-commerce baskets, hide information away from users, or make it appreciably harder to find how to exercise one's rights against the data controller or trader. By creating manipulative menus, hiding costs to users away, using pre-checked boxes and specific colouring and graphics in the UI, users can find it disparately harder to withdraw from something than they did to accept. These are used to benefit the trader's interest, rather than the user's.[9] Even more specific typologies of dark patterns have emerged from the fields of design ethics[10] and psychology[11]. According to a classification system proposed by Claude Castelluccia of INRIA, those dark patterns which undermine the privacy of users fall into the category of 'execution attacks', or actions which make things so complicated that they lead the user to give up on opposing them.[12] Other work has focussed on a singular aspect of data protection law; for example, Nouwens *et al's* research into consent management platforms, albeit with questionable methodology, concluded that only 11.8% of websites met the minimum threshold for consent under EU law.[13]

The 'ubiquitous, invisible, and proactive'[14] nature of dark patterns preclude 'scenarios in which users choose whether they authorize to record [or have access to] data'.[15] As users lose control over what information they consent to processing by third parties, their individual autonomy, agency, and control

---

[9] For comprehensive discussions about how architecture can be used to nudge users into behaviour modification, see Karen Yeung, ''Hypernudge': Big Data as A Mode Of Regulation By Design' (2016) 20 Information, Communication & Society, 118-136 at 120; See also Tal Z. Zarsky, 'Privacy And Manipulation In The Digital Age' (2019) 20 Theoretical Inquiries in Law; Daniel Susser, Beate Roessler and Helen Nissenbaum, 'Technology, Autonomy, And Manipulation' (2019) 8 Internet Policy Review.); M. Ryan Calo, 'Digital Market Manipulation' (2014) 82 The George Washington Law Review

[10] 'The Dark (Patterns) Side Of UX Design | Proceedings Of The 2018 CHI Conference On Human Factors In Computing Systems' (Dl.acm.org, 2021) <https://dl.acm.org/doi/10.1145/3173574.3174108> accessed 2 July 2021.; 'Dark Patterns In UX: How Designers Should Be Responsible For Their Actions' (Medium, 2021) <https://uxdesign.cc/dark-patterns-in-ux-design-7009a83b233c> accessed 2 July 2021; *Harry Brignull and others, 'Dark Patterns: Deception Vs. Honesty In UI Design' (2021) <https://alistapart.com/issue/338/> accessed 2 July 2021.*; Harry Brignull, 'Dark Patterns: Inside The Interfaces Designed To Trick You' (The Verge, 2021) <https://www.theverge.com/2013/8/29/4640308/dark-patterns-inside-the-interfaces-designed-to-trick-you> accessed 2 July 2021

[11] Jachimowicz, J. M., Duncan, S., Weber, E. U., & Johnson, E. J. (2019). When and why defaults influence decisions: A meta-analysis of default effects. Behavioural Public Policy, 3(2), 159-186 at 159. For an example of the integration of cognitive psychology into regulatory policy, see Commission Nationale de L'informatique et des Libertés (CNIL), the French data protection authority, '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, at IP Report: Shaping Choices in the Digital World, (last visited 10 April 2020); See also Damian Clifford (2017) Citizen-consumers in a personalised galaxy: Emotion influenced decision-making, a true path to the dark side?; Bösch, C., Erb, B., Kargl, F., Kopp, H., & Pfattheicher, S. (2016) Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns; Draper, N. A., & Turow, J. (2019). The corporate cultivation of digital resignation. *New Media & Society*, *21*(8), 1824-1839

[12] https://voxeurop.eu/en/2019/privacy-5124014, (visited 18 April 2020)

[13] Midas Nouwens and others, 'Dark Patterns After The GDPR: Scraping Consent Pop-Ups And Demonstrating Their Influence', Association for Computing Machinery (ACM 2020)<https://dl.acm.org/doi/pdf/10.1145/3313831.3376321?casa_token=fDsPakcJwQUAAAAA%3A5p2usbRAr38SO8uMnfoX5xBE9-hh_JVVsak59KKRzVdhBZpmrjh2hY5Ac_vouC447mtHvU6UcxDj> accessed 2 July 2021.

[14] Loke, S. (2006). Context-aware pervasive systems: architectures for a new breed of applications. CRC Press citing Weiser, M. (1993). Hot topics-ubiquitous computing. *Computer*, *26*(10), 71-72, Norman, D. A. (1999). *The invisible computer: why good products can fail, the personal computer is so complex, and information appliances are the solution*. MIT press and Tennenhouse, D. (2000). Proactive computing. *Communications of the ACM*, *43*(5), 43-50

[15] Philip Brey, 'Freedom and Privacy In Ambient Intelligence' (2005) 7 Ethics and Information Technology, at 164

is reduced.[16] Regulatory emphasis in the GDPR remains rooted in the prohibition of processing unless data controllers satisfy one of six legitimate grounds for processing and compliance with the GDPR's principles.[17] Some dark patterns manipulate users to 'use a facility and give away one's privacy, or not to get to use the facility at all'.[18] Viewed in this light, the deployment means 'privacy has become a tradable commodity'.[19] For example, after the implementation of a dark pattern design to obtain user permission to process sensitive personal data, the data controller may have obtained the prerequisite authorisation but 'given on the basis of a limited understanding of what personal information is collected and how it would or could be used'[20], it is 'doubtful that such authorizations are based on *informed* consent' [Emphasis added].[21] Dark patterns, therefore, facilitate some sort of benefit to the data controller at the expense of users who, in return, trade away their fundamental right to data protection. For example, a dark pattern could be deployed in the user interface to make the disclosure of personal data appear 'irresistible' by connecting the data subject's consent to the processing of personal data to in-app benefits. While the EU data protection framework places the principle of transparency at the forefront of data processing, the regime is not balanced with a requirement to be transparent *about* the in-app benefits. Many apps are simply designed for the collection of personal data, rather than providing any meaningful utility. Accordingly, designers use the User Interface (UI) to exaggerate the benefits of the app at the expense of the consequences of data-sharing. There is clearly a symbiotic relationship and a synergy between the consumer and data protection regimes. For example, consumer protection regulators have has concluded that some privacy policies are contracts by nature. Although this position is hotly debated among data protection academics, the fact remains that after the GDPR came into force, many data controllers took the opportunity to update the legitimate ground of processing from consent under Article 6(1)(a) (thanks to the higher benchmark required post implementation of the GDPR) to Article 6(1)(b) – necessary for performance of a contract.[22] This switch from 'consent' to 'contract' is subject to a legal challenge by the Austrian Supreme Court who has asked the CJEU to determine whether Facebook illegally undermined the GDPR by allegedly bypassing consent via contractual provisions.[23]

A recent study examined the effects of different consent management pop-up windows, using a browser extension that displayed different privacy control pop-ups in real websites. The designs were mimicking the consent management pop-ups that we commonly find in the EU following the introduction of the GDPR. The experiment was conducted with U.S. participants (to avoid familiarity with current European consent practice) and measured the effect of pop-up design on the final privacy decisions of participants. In the experiment, the basic layout of the consent notification (a horizontal 'banner' vs. a rectangular 'barrier') had no effect on the final privacy decisions, but other components of the design mattered. Removing the 'reject all' button from the first page of the consent form increased the probability of consent by 22%. The display of granular consent choices on the first page also had effects on consent: Showing a list of granular choices that spelled out the purposes of data use decreased consent by 8%. Showing a list of vendor companies that would access the data decreased consent by 20% and showing the list of both purposes and vendors decreased consent by 11%. These results suggest that design lacking accessible granularity and/or the absence of simple opt-out buttons in consent forms leads users to share more data than they would when given accessible control over their privacy.[24]

---

[16] Philip Brey, 'Freedom and Privacy In Ambient Intelligence' (2005) 7 Ethics and Information Technology, at 164
[17] General data protection regulation, art 6(1)
[18] Philip Brey, 'Freedom and Privacy In Ambient Intelligence' (2005) 7 Ethics and Information Technology at 165
[19] Philip Brey, 'Freedom and Privacy In Ambient Intelligence' (2005) 7 Ethics and Information Technology at 165
[20] Philip Brey, 'Freedom and Privacy In Ambient Intelligence' (2005) 7 Ethics and Information Technology at 165
[21] Philip Brey, 'Freedom and Privacy In Ambient Intelligence' (2005) 7 Ethics and Information Technology at 165
[22] Using Facebook as an example, see https://noyb.eu/en/breaking-austrian-ogh-asks-cjeu-if-facebook-undermines-gdpr-2018, accessed 23 July 2021
[23] https://noyb.eu/sites/default/files/2021-07/Vorlage_sw_EN.pdf at 2, accessed 23 July 2021
[24] Midas Nouwens and others, 'Dark Patterns After the GDPR: Scraping Consent Pop-Ups and Demonstrating Their Influence', Association for Computing Machinery (ACM 2020), <https://dl.acm.org/doi/pdf/10.1145/3313831.3376321?casa_token=fDsPakcJwQUAAAAA%3A5p2usbRAr38SO8uMnfoX5xBE9-hh_JVVsak59KKRzVdhBZpmrjh2hY5Ac_vouC447mtHvU6UcxDj> accessed 2 July 2021.

The protection of personal data is a fundamental right under Article 8 of the EU's Charter of Fundamental Rights (CFR). Article 8(2) CFR contains key data protection principles (fair processing, consent, or legitimate aim prescribed by law, rights of access and rectification, etc.) and under Article 38 'public authorities shall guarantee the protection of consumers and users and shall, by means of effective measures, safeguard their safety, health, and legitimate economic interests'. The EU consumer protection acquis[25] provides for an extensive framework of consumer rights. Recently updated, the "New Deal for Consumers" package aims at strengthening enforcement of EU consumer law and modernising the EU's consumer protection rules in view of market developments.[26] Both regimes stand-alone but can be used to supplement and complement each other. This paper assesses the capabilities and limitations of both -consumer and data protection- regimes to regulate the use of dark patterns.

Dark Patterns & Data Protection

By relying on psychological mechanisms to manipulate users away from rational deliberation and argumentation[27], dark patterns 'ruthlessly nudg[e] consumers to disregard their privacy and to provide more personal data than necessary'.[28] Because dark patterns are 'physically' unobtrusive (otherwise they would not work) and their intentions are not generally transparent, they should be seen as manipulative and not 'fair' to the user. Yet, the first principle of data protection requires processing to be 'fair, lawful, and transparent'.[29] *Fair processing* implies that data has not been obtained nor otherwise processed through unfair means, by deception or without the data subject's knowledge[30]. Furthermore, the data protection regime contains strict obligations to design processing systems with the protection of personal data embedded.[31] Can the fairness principle also apply to data-protection-by-design, and if so, can this work together to regulate dark patterns?

Dark Patterns and the Data-Protection-by-Design requirement

The effectiveness of the EU's rules for the protection of personal data relies on the implementation of and compliance with Article 25 of the GDPR (data-protection-by-design-and-default; herafter DPbDD) by designers and the subsequent enforcement thereof by regulators.[32] DPbDD requires that controllers

[25] Directive 2011/83/EU of the European Parliament and of the Council 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 (The Consumer Rights Directive (CRD)); Directive 2005/29/EC of the European Parliament and of the Council 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 ('Unfair Commercial Practices Directive' (UCPD)); Council Directive 93/13/EEC of 5 April 1993 on Unfair Terms in Consumer Contracts (hereafter, UTCCD); Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services (Supply of Digital Content Directive); Directive (EU) 2019/2161 of the European Parliament and of the Council 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(Enforcement and Modernisation Directive); Directive (EU) 2019/771 of the European Parliament and of the Council 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 (Maximum Harmonization And Higher Protection of Consumers Under The Directive);

[26] 'Communication From the Commission To The European Parliament, The Council And The European Economic And Social Committee: A New Deal For Consumers' (Eur-Lex, 2021) <https://ec.europa.eu/info/sites/default/files/communication_11.4.2018.pdf> accessed 2 July 2021

[27] From an interview with Giovanni Buttarelli, European Data Protection Supervisor (who died on 20 August 2019), 'Dark Patterns in Data Protection - Giovanni Buttarelli' (European Data Protection Supervisor, 2021) <https://edps.europa.eu/data-protection/our-work/publications/speeches-articles/dark-patterns-data-protection-giovanni_en> accessed 2 July 2021

[28] Thomas RV Nys and Bart Engelen, 'Judging Nudging: Answering The Manipulation Objection' (2016) 65 Political Studies

[29] General Data Protection Regulation, art 5(1)(a)

[30] *KH and others v Slovakia* [2009] (App no. 32881/04) (ECtHR, 28 April 2009)

[31] General Data Protection Regulation, art 25

[32] 'Internet Privacy Engineering Network Discusses State Of The Art Technology For Privacy And Data Protection' (European Data Protection Supervisor, 2021) <https://edps.europa.eu/press-publications/press-news/press-releases/2019/internet-privacy-engineering-network-discusses_en> accessed 2 July 2021

implement data protection principles e.g., data minimisation (do not collect more data than necessary)[33], accountability and fairness[34], etc. into the design of data processing systems. It ensures that data protection becomes part and parcel of data processing without users necessarily needing to fully comprehend complex technical practices behind the processing of personal data. It also provides opportunities to integrate individual (control) rights into the data systems operation, increasing transparency.[35]

Koops and Leenes have posed a series of questions about the extent of DPbDD obligations: 'Does it imply, at one end of the spectrum the deployment of straightforward technologies, such as data encryption or role-based access control? Or does it, at the other end of the spectrum, imply hardcoding the data-protection rules into machine-executable code as much as possible?'[36] A narrow interpretation of DPbDD obligation implies that designers must evaluate any possible risks to privacy in the use of their service and take any measures necessary to prevent any threats to users. This would ensure the reasonable technical and organizational measures are taken to protect from breaches of personal data.[37] However, Article 25(1) GDPR requires that data controllers implement technical and organisational measures appropriate for the protection of the data subject rights at the time of processing of personal data. More specifically, controllers are required to implement such measures when determining the means of processing*:*

> '(..) both *at the time of the determination of the means for processing* and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.'[38] [Emphasis Added]

Furthermore, Recital 4 of the GDPR states: '*the processing of personal data should be designed to serve mankind*', suggesting that 'privacy-by-design' should be understood as a broad, overarching concept of technological measures for ensuring privacy. This is very close to the ethos already found in Recital 46 of the Data Protection Directive 95/46/EC: the technical and organisational measures to be taken to protect rights and freedoms of people whose data are processed should be applied '*both at the time of the design of the processing system and at the time of the processing itself …*'

Privacy-by-default, on the other hand, requires pre-checked options for digital services to be always in favour of maximum data protection: no unnecessary data should be collected, unless the user agrees to such data being collected. In contrast, 'data-protection-by-design' and 'data-protection-by-default' designate the specific legal obligations established by Article 25 of the GDPR.[39] Taken together, data protection-by-design-and-default ensures that personal data is 'automatically protected in any given IT system or business practice. If an individual does nothing, their privacy remains intact. No action is required on the part of the individual to protect their privacy — it is built into the system, by default'.[40] This statement is a powerful operational definition of the privacy-by-default principle, where the individual does not bear the burden of striving for protection when using a service or a product but

---

[33] General Data Protection Regulation, art 25(2)
[34] General Data Protection Regulation, art 5
[35] Simone van der Hof and Eva Lievens, 'The Importance Of Privacy By Design And Data Protection Impact Assessments In Strengthening Protection Of Children's Personal Data Under The GDPR' (2018) Communications Law 23
[36] Bert-Jaap Koops and Ronald Leenes, 'Privacy Regulation Cannot Be Hardcoded. A Critical Comment on The 'Privacy By Design' Provision In Data-Protection Law' (2013) 28 International Review of Law, Computers & Technology. 159-171, at 161
[37] General Data Protection Regulation, art 5(1)(f)
[38] General Data Protection Regulation, art 25
[39] European Data Protection Supervisor, 'Preliminary Opinion On Privacy By Design' (2018) https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf, accessed 2 July 2021.
[40] Hoepman, J. H., Leenes, R., & Whitehouse, D. (2014). Privacy and identity management for emerging services and technologies. M. Hansen (Ed.). Springer citing Cavoukian A, "Privacy by Design [Leading Edge]" (2012) 31 IEEE Technology and Society Magazine 18

enjoys 'automatically' (no need for active behaviour) the fundamental right of privacy and personal data protection. [41]

By hard-wiring data-intrusive options by default, obscuring more privacy-friendly settings, threatening the loss of functionality unless users comply, and using persistent pestering to compel users to make certain data-invasive choices, the effects on users echo previous concerns about the regulatory effect of code.[42] For Brownsword who argues that ''using design for regulation impacts users' empowerment and their ability to make choices'[43] and Yeung who argues that design choices remove 'the ability of users to choose to obey or disobey a rule'[44], the integration of dark patterns at system level sets users on the course to choose the parameters that benefit the data controller, and push users to respond to the preconfigured settings of the technology. Not only do dark patterns manipulate users into giving up their data protection rights, but they also create a situation in which individuals are refrained from 'being called upon to explain [their] reasons for actions'[45] as 'technologies are enforcing behaviours without relying on moral reflection'.[46] Furthermore, if dark patterns manipulate users into doing something that they would not have done otherwise, then compliance regimes could operate less than optimally. As Leenes states, when design 'norms are embedded into technology, sanctions do not exist, instead 'enforcement and sanction coincide'.[47]

The DPbDD contains an internal obligation for data controllers to self-assess whether they are complying with their legal obligations at the very conception stages of design. Koops and Leenes argue that energy should be expended on 'fostering the right mindset of those responsible for developing and running data processing systems [as this] may prove to be more productive than trying to achieve rule compliance by techno-regulation'.[48] The focus must not be limited solely to 'data protection compliance, [instead] we must look more holistically to principles of privacy law like protection for autonomy, liberty and human dignity'.[49] DPbD also contains an external obligation to ensure transparency for the processing activities of the controller. The use of dark patterns compromises the *ethos* of Article 25 to ensure data protection-by-design-and-default[50], while persistent pop-ups and nudges violate broader conceptual notions of both the fairness and the transparency principle when integrated at system level. It also creates an important benchmark for determining whether the design was *fair* on data subjects and consumers.

Dark Patterns and the Consent Mechanism

The EDPB has reiterated that the consent mechanism does not legitimise collection of personal data when it is not related to a specified purpose and/or is fundamentally unfair.[51] Although Article 7(3)

[41] Douwe Korff and Marie Georges, "The Data Protection Officer Handbook@, https://www.garanteprivacy.it/documents/10160/0/T4DATA-The+DPO+Handbook.pdf/a5bfc9ba-8a0c-0f88-9874-71be40be6a6d?version=1.0 accessed 2 July 2021

[42] For an example of the 'Code is law' school of thinking, see Lawrence Lessig, Code (Basic Books 2008; For an example from the code is not a standalone regulatory modality, but rather a tool of regulators, Andrew Murray and Colin Scott, 'Controlling the New Media: Hybrid Responses to New Forms of Power' (2002) 65 The Modern Law Review at491-516

[43] Brownsword 'What the World Needs Now: Techno-Regulation, Human Rights and Human Dignity' (ed) Human Rights: Global Governance and the Quest for Justice (Oxford: Hart Publishing 2004), at 211.

[44] Karen Yeung, 'Can We Employ Design-Based Regulation While Avoiding a Brave New World?' (2011) 3 Law, Innovation and Technology.) at 1-29

[45] Karen Yeung, 'Can We Employ Design-Based Regulation While Avoiding a Brave New World?' (2011) 3 Law, Innovation and Technology.) at 1-29 at 5

[46] Karen Yeung, 'Can We Employ Design-Based Regulation While Avoiding a Brave New World?' (2011) 3 Law, Innovation and Technology.) at 1-29 at 15

[47] Ronald Leenes, 'Framing Techno-Regulation: An Exploration of State and Non-State Regulation By Technology' (2011) 5 Legisprudence, 143-169 at 147

[48] Urquhart and Rodden, A Legal Turn in Human Computer Interaction? Towards 'Regulation by Design' for the Internet of Things (Working Paper, March 11, 2016) at 6

[49] J. Savirimuthu, 'Smart Meters and The Information Panopticon: Beyond The Rhetoric Of Compliance' (2013) 27 International Review of Law, Computers & Technology at 161–186

[50] General Data Protection Regulation, recital 78

[51] Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.0 Adopted on 4 May 2020, <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf> at 5 accessed 24 July 2021

provides a legal requirement that consent shall be as easy to withdraw as to give, dark patterns also expose the *consent fallacy* embedded within the text of the GDPR. Long touted to help data subjects steer through privacy trade-offs, whether the consent mechanism makes changes in user behaviour remains largely theoretical and hypothetical. Moreover, the concept is grounded in unrealistic optimism: if individuals are informed about how their data is handled; for example, what is being collected and to whom it is disclosed, then they will be in a better position to decide their preferences regarding privacy protection and disclosure. This claim is, unfortunately, not backed in any actual evidence.

Edwards argues that prior to the GDPR, the consent requirement was a 'magic wand that could be waived by any popular online service to secure itself a revenue stream of personal data whilst remaining legally compliant'.[52] Post the implementation of the GDPR, there is little indication that the situation has improved. The Regulation's unfortunate fixation on the mechanism results in negligible consideration as to whether it provides real protection to users. Consider the following design technique: arrows pointing away from a small grey transparent box to a giant red button signalling to users that 'clicking here will indicate you have agreed to the processing of sensitive personal data which we will sell to third parties and track every instance of your very being' satisfy the legal requirement for 'specific, informed and unambiguous indication of the data subject's wishes', and satisfy the 'a clear affirmative action' which 'signifies agreement' requirement[53], the data controller could also theoretically argue that the transparency principle under Article 5(1)(a) is satisfied. After all, is there anything more transparent than a big red button telling users exactly what they are going to do with a subject's personal data? There are no pre-ticked boxes[54], the data controller can argue they obtained consent[55] using 'intelligible' and 'clear and plain language'. Consent is not bundled within vague terms describing contract performance and is presented in a 'manner clearly distinguishable from other matters'.[56] Dark patterns can be designed in a way that push users to provide the regulatory requirement that a user has provided 'consent'. They can also be implemented in a way that appear to make the mechanism transparent.

Dark Patterns and the Data Protection Principles

A DPbDD compliant system will make data protection principles an integral part of the process of data processing; for example, a UI that provides users with a visual of their settings and allows permissions to be tweaked would not only ensure compliance with Article 25, but also principles of fairness transparency[57], and the proper purpose principle.[58] A DPbDD solution entails making transparency an integral part of the process of data processing practices, e.g. by clearly and instantaneously showing important events or changes in data processing systems to users or by giving them a visualisation of and accessible tools to tweak data processing in a control panel or privacy dashboard.[59] However, the transparency principle is normally associated with either a) rights; for example, the right to information

[52] Lilian Edwards, Law, Policy and The Internet (1st edn, Hart Publishing 2019), at 99
[53] General data protection regulation, art 4(11); cf. Also Article 7(4) GDPR which provides that consent may be considered not free if it is not necessary for the contract that data subject is signing up for ; cf. also the finalized A29 WP Guidelines on Consent under Regulation 2016/679 (wp259rev.01), at A29 WP Guidelines on Consent under Regulation 2016/679, at <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051> accessed 24 July 2021and the Article 29 WP Guidelines on transparency under Regulation 2016/679 <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227> accessed 24 July 2021. In the UK, the ICO issued its final GDPR consent guidance at ICO Consent Guidance <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/>, accessed 24 July 2021
[54] Pre-ticked boxes are specifically banned under General Data Protection Regulation, recital 32
[55] GDPR, art 7(1)
[56] GDPR, art 7(2)
[57] GDPR, art 5(1)(a)
[58] GDPR, art 5(1)(b)
[59] For instance, see the suggestions by the Article 29 Working Party in *Guidelines on Transparency under Regulation 2016/679* (11 April 2018) at ARTICLE 29 Newsroom - Guidelines on Transparency under Regulation 2016/679 (wp260rev.01) < http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227> accessed 12 April 2021

about data processing procedures[60], rights concerned with information and access to data[61], rights to transparency in decisions obtained from an automated process[62] and obligations to communicate data breaches to data controllers[63] and communicate with data subjects if there is risk of harm to privacy or personal data[64], b) ensuring information disclosures are comprehensible by data subjects[65] or c) the processing itself is transparent.[66] There is also scholarly recognition of the transparency principle's shortcomings. Weatherill, for example, argues that regulatory techniques for information disclosure assumes that consumers can grasp the nature of the information provided[67]:

> 'Their efficiency depends on the capacity of the consumer to process the information that is supplied and act rationally in response to it. In so far as consumers fail to behave in an alert and rational manner, regulatory interventions based on information disclosure may not yield the intended benefits.'[68]

In fact, Weatherill argues that 'if a bargaining environment is fundamentally flawed by the imbalance between the parties, then to introduce disclosure requirements may even legitimize a pernicious practice.[69] The transparency principle is a trapdoor in the fight against dark patterns; one might argue that the more transparent a dark pattern, the more likely a user will consent to data processing when there is a significant power imbalance between the two parties. What matters is whether *the process* of processing of personal data is fair. More specifically, is the process designed for satisfying the legal requirements for processing personal data (the lawful principle) transparent and *fair*? On the surface, transparency acts as an important tool for ensuring users are empowered with the capability to determine whether agreeing to processing is in their best interests. Scholarship in this area totes transparency as crucial to help users navigate the privacy trade-offs.[70] But in actuality, there is little evidence to suggest that *transparency* plays a role in reducing the instances where users agree to the processing of personal data or mitigate any individual privacy concerns. On the contrary, increased transparency increases transaction costs. This should be a function of not only accessibility (the time required to access and understand the information), and the complexity of the information provided, but awareness costs. Once the information is made available, then what? Presuming that the imposition of strict transparency requirements onto dark patterns would magically illuminate the risks associated with data processing in a meaningful way could result in the same erroneous assumptions about the mechanism of consent.

---

[60] General Data Protection Regulation, arts 12, 13 and 14.
[61] General Data Protection Regulation, art 15; See also Gutwirth and De Hert, Regulating Profiling in a Democratic Constitutional State (Profiling the European Citizen: Chapter 14) 2008 at290 < https://www.researchgate.net/profile/Paul_Hert/publication/226481037_Regulating_Profiling_in_a_Democratic_Constitutional_State/links/54a3f57d0cf257a6360714b6.pdf> accessed 21 July 2021: 'profiling activities should be ruled by transparency tools that ensure the visibility, controllability and accountability of the profilers and the information, control and participation of those concerned'
[62] General Data Protection Regulation, arts 13, 14, and 22
[63] General Data Protection Regulation, art 33
[64] General Data Protection Regulation, art 34
[65] General Data Protection Regulation, recital 58; art 12(1); On transparency as one of the central principles about processing of personal data, see Spagnuelo, D., Ferreira, A., & Lenzini, G. (2019, March). Accomplishing Transparency within the General Data Protection Regulation. In *ICISSP* at 114-125
[66] General Data Protection Regulation, art 5 (1)(a)
[67] Weatherill, Stephen (2013) EU Consumer Law and Policy (2nd edition), Edward Elgar, Cheltenham, UK at 143
[68] Weatherill, Stephen (2013) EU Consumer Law and Policy (2nd edition), Edward Elgar, Cheltenham, UK at 93
[69] Weatherill, Stephen (2013) EU Consumer Law and Policy (2nd edition), Edward Elgar, Cheltenham, UK at 93.
[70] Acquisti, A., Adjerid, I., & Brandimarte, L. (2013). Gone in 15s: The limits of privacy transparency and control. *IEEE Security Privacy, 11*(4), 72–74 <https://doi.org/10.1109/MSP.2013.86> accessed 24 July 2021; Adjerid, I., Acquisti, A., Brandimarte, L., & Loewenstein, G. (2013). Sleights of privacy: framing, disclosures, and the limits of transparency. In *Proceedings of the ninth symposium on usable privacy and security* at 9:1–9:11. New York, NY: ACM, < https://doi.org/10.1145/2501604.2501613> accessed 26 July 2021; Kaplan, B. (2016). How should health data be used? Privacy, secondary use, and big data sales. *Cambridge Quarterly of Healthcare Ethics, 25*(2), 312–329. <https://doi.org/10.1017/S0963180115000614> accessed 24 July 2021

Fairness is at the core of the fundamental right to data protection. Article 8(2) CFR stipulates that data must be processed fairly.[71] Although Bygrave refers to fairness as 'the cornerstone upon which the other principles are built'[72], a comprehensive understanding of the principle's application remains elusive. Clifford and Ausloos's examination of the 'elusive' principle concluded that, not only it is to be interpreted independent of the 'lawful' and 'transparency' principles; fairness should be viewed as both complementary and supplementary to the other two. However, their analysis contains an admitted, but unfortunate, amalgamation of the fairness and transparency principles:

> '*The express mentioning of fairness and the positioning of fairness, lawfulness, and transparency as 'core' principles is manifested in the recognition of both an explicit and implicit role for fairness. Explicitly in the requirement for fair and transparent processing (i.e., information requirements and thus the application of the inherent transparency principle) and implicitly via the recognition of the need for a 'fair balance' regarding competing fundamental rights and interests*'.[73]

For Clifford and Ausloos, fairness operates with transparency (given the explicit mentioning of the need for fair and transparent processing). Through this explicit operation of the principle of fairness processing becomes 'procedurally' fair and not just transparent. However, providing information also ensures compliance with the transparency principle, *in itself*. One does not need to argue that the data controller must do so to ensure fairness. Any analysis that concludes an implicit requirement for 'fair-balance' between competing rights *and interests* suggests that a data controller has the right to design their UXs and UIs in any manner they see fit, with regulatory oversight of the fairness principle only acting to mitigate the excesses of only the worst dark patterns. Clifford and Ausloos also emphasize enforcement over inquiry as to whether the fairness principle extends to DPbDD as a *legal obligation:*

> '*Without adequate enforcement, businesses will likely take a more utilitarian approach to the weighing of interests and the implementation of architectural operational safeguards, reducing it to a de facto cost–benefit analysis and failing to give due consideration to all data processing risks. In essence therefore, this raises doubts in terms of the effective implementation of the principle of fairness given the reliance of 'new' regulation on effective enforcement and thus the effective operation of the GDPR specific proportionality and necessity notions*.'[74]

Without examination of whether fairness extends to the legal obligation of data-protection-by-design, it remains unclear whether the principle extends to the entirety of the pre-processing environment, not just the act of processing itself. Questions like 'Does the UX and UI operate in a manner that is fair to users?' and 'does its design manipulate, deceive, or take advantage of behavioural insights that would not have resulted in the same outcomes if systems were designed fairly?' remain unanswered by data protection scholarship.

Extending the DPbDD principle to prevent the integration of dark patterns into the design of the system is neither a creative overreach of legislative intention nor requires extensive reinterpretation of the data protection acquis: Recital 78 states that the 'the controller should adopt internal policies and implement measures which meet the principles of data protection by design and data protection by default'. These measures include 'transparency with regard to the *functions* and processing of personal data' [Emphasis added]. Here the term 'functions' is referring to the system architecture and the way the data is processed. Therefore, *data protection-by-design* means that data protection 'should be considered throughout the entire engineering process' while the additional 'by-default' requires fairness should be

[71] Furthermore, the principles found in Directive 95/46/EC, art 6(1)(a) are now in General Data Protection Regulation, art 5(1)(a)
[72] Damian Clifford and Jef Ausloos, '*Data Protection and the Role of Fairness*' in Yearbook of European Law, Vol. 37, No. 1 (2018), pp. 130–187 at 137, citing Lee A Bygrave, Data Protection Law: Approaching Its Rationale, Logic and Limits (The Hague: Kluwer Law International, 2002) at 58
[73] Damian Clifford and Jef Ausloos, 'Data Protection and the Role of Fairness' in Yearbook of European Law, Vol. 37, No. 1 (2018), pp. 130–187, at 138
[74] Damian Clifford and Jef Ausloos, 'Data Protection and the Role of Fairness' in Yearbook of European Law, Vol. 37, No. 1 (2018), pp. 130–187, at 183

embedded 'at the earliest design stages to the operation of the productive system'[75]. Moreover, Article 25 requires controllers to implement 'technical measures' designed to 'implement data-protection principles in an effective manner and to integrate the necessary safeguards *into* the processing' [Emphasis added]. Accordingly, the obligation is not just limited to just explicit and implicit roles in data processing. Fairness should be something to be instilled throughout the design of the system architecture and any user interfaces.

Clifford and Ausloos as well as Malgieri have cited the GDPR's fairness principle as a means of rectifying the imbalances between data subjects and data controllers.[76] For Clifford and Ausloos, the principle targets 'the re-balancing of the asymmetric data subject–controller relationship'.[77] However, Malgieri rightly recognizes the 'proper meaning of the fairness principle in the GDPR is still unclear and vague'[78], and Clifford and Ausloos concur: 'fairness remains somewhat of a mystery' before concluding that the principle's application is limited to 'procedural fairness' and 'fair-balancing' in context dependent circumstances. Their emphasis is limited to discussion whether the fairness principle in the GDPR is strictly *necessary* to solve the problems associated with any identified power imbalances.

How the fairness principle can be applied to the broader principle of privacy-by-design is uncertain. While Article 25 GDPR provides some clarity on what amounts to data-protection-by-design, this amounts to legal rules to ensure transparency is taken into consideration during the design stage for *processing*. Without any clear understanding of the role of the fairness principle, it is helpful to look elsewhere for guidance. As discussed in the next section, the further effectuation of the fairness principle that Clifford and Ausloos call for is not essential for the regulation of dark patterns: the principle is also at the heart of the consumer protection regime, which could be better placed to determine whether the design that led to data processing was a fair *practice*.

Dark Patterns and Consumer Protection

As this section will outline, analysing the overall system architecture, user experience and interfaces for fairness would permit consumer law to gauge whether the totality of the consent process was fair on consumers. This requires moving away from proposals for remedying the consent fallacy that focus on the panacea of consent simplification[79] and reflects recent acknowledgements found in the European Union's 'new deal for consumers' that personal data is increasingly seen as having economic value.[80]

Like the framework for the processing of personal data, the consumer protection regime is aimed at fostering user empowerment.[81] The concept is recognized in the European Commission's adoption of a 'new deal for consumers' which is aimed at strengthening the enforcement of EU consumer law and

[75]For analysis of the concepts of privacy by design, data- protection- by-design-and-by-default read: ENISA, Privacy and Data Protection by Design, 12 January 2015, <https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design/> accessed 21 July 2021

[76] Damian Clifford and Jef Ausloos, 'Data Protection and the Role of Fairness' in Yearbook of European Law, Vol. 37, No. 1 (2018), at 130–187; Gianclaudio Malgieri, 'The concept of fairness in the GDPR: a linguistic and contextual interpretation'. In Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency (2020) at 154-166

[77] Damian Clifford and Jef Ausloos, 'Data Protection and the Role of Fairness' in Yearbook of European Law, Vol. 37, No. 1 (2018), pp. 130–187, at 131

[78] Gianclaudio Malgieri, 'The concept of fairness in the GDPR: a linguistic and contextual interpretation'. In Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency (2020) at 154-166 at 155

[79] For an example of a consent simplification solution, see Custers B.H.M., Dechesne F., Pieters W., Schermer B. & Hof S. van der (2018), Consent and Privacy. In: Müller A., Schaber P.(red.) The Routledge Handbook of the Ethics of Consent. London: Routledge, 247-258 at 254

[80] 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 L 136/1

[81] The European Data Protection Supervisor acknowledges that the '*EU approaches to data protection [. . .] and consumer protection share common goals, including the promotion of growth, innovation and the welfare of individual consumers*'. 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< https://edps.europa.eu/sites/edp/files/publication/14-03-26_competitition_law_big_data_en.pdf> accessed 24 July 2021

modernising the rules in view of market developments.[82] Not only does the European Union offer a 'high level of consumer protection' for her economic activities[83], both consumer and data protection aim, in part, to protect the autonomy of the natural person.[84] In other instances, autonomy is overridden by the interests of protecting the weaker party in an imbalanced relationship.[85] However, protection as a *concept* for consumers is clearer. Where 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.[86]

In the run up to the implementation of the GDPR, some data controllers not only took the opportunity to update their privacy policies and terms and conditions generally, but to update the relevant basis used for the processing of personal data. With perceptions rife that the threshold for proving consent had risen to an unachievable standard, many providers opted to switch their legal basis from consent under Article 6(1)(a) to 'necessary for the performance of a contract' under Article 6(1)(b); in doing so, triggering the consumer protection regime[87]: every data subject that has purchased a service by agreeing to the processing of their personal data is also a consumer[88] with commercial practice rules extending to the processing of personal data.[89] By agreeing to the terms and conditions needed to access a digital service, every natural person becomes a consumer that has bought a service. Consumer law regulates the circumstances surrounding a 'transaction' far more broadly than data protection does regulating the circumstances surrounding processing[90]; for example, consumer law also covers advertising and pre-contractual environments. The decision to enter an e-commerce site can fall under its remit even if a user does not buy a product or a service and can also apply after a transaction has been completed. Accordingly, every user interface that either pushes users into agreeing to terms and conditions or indicating consent could fall under its scope, as would any onerous non-contractual barriers following the conclusion of a contract.

---

[82] For an excellent and in-depth overview of the consumer protection regime's ability to regulate and sanction dark patterns, see Caruana and Leiser, '*Dark Patterns': Light to be found in Europe's consumer protection regime?*' (forthcoming, 2021) citing 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 24 July 2021; 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 < http://ec.europa.eu/consumers/consumer_empowerment/docs/swd_consumer_empowerment_eu_en.pdf> accessed 24 July 2021

[83] CFR, art 38

[84] 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

[85] Weatherill, Stephen (2013) EU Consumer Law and Policy (2nd edition), Edward Elgar, Cheltenham, UK at 143.

[86] Gomez, *Id*. and Slawson, W. D. (1970). Standard Form Contracts and Democratic Control of Lawmaking Power. Harvard Law Review at 84, 529

[87] The consumer protection regime applies whenever the consumer and trader engage in a commercial relationship - this could be the result of consent to data processing. There are also non-contractual consumer relationships, for example, advertising. In other words, the consumer protection regime would also be triggered for any practices related to advertising, even if the consumer has never entered a specific "contract" with the trader.

[88] A German court upheld a complaint from the Federal Consumer Association (vzbv) that issues relating to the processing of personal data come within the scope of consumer protection law; See VZBV vs WhatsApp, Judgment of the Chamber Court of 20.12.2019, Az. 5 U 9/18, at Urteil des KG Berlin vom 08.04.2016, Az. 5 U 156/14.

[89] Case No. CV154: WhatsApp - Unfair Terms; full decision in Italian accessed here <L'autorità Garante Della Concorrenza E Del Mercato Nella Sua Adunanza dell'11 maggio 2017; SENTITO il Relatore Prof. Michel> accessed 21 July 2021; 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 <L'autorità Garante Della Concorrenza E Del Mercato Nella Sua Adunanza dell'11 maggio 2017; Sentito il Relatore Dottoressa G> on 18 April 2020. Both cases started 27 October 2016 and decided on 11 May 2017.

[90] Unfair Commercial Practices Directive, art 2(d)

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.[91] 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'[92] 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',[93] 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'.[94] 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'. 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.'

Any use of a dark pattern designed to get users to indicate agreement to the terms of conditions that processes personal data within can activate both regimes: the user can be both a 'consumer' and a 'data subject'. Second, as the consumer protection regime considers data to have economic value[95], using a dark pattern to influence the agreement of terms and conditions in relation to buying a digital service could amount to an unfair practice under Article 5 of the Unfair Commercial Practice Directive.[96] Importantly, this creates exposure to double liability for traders. Not only will the data controller be liable for up to 4% of their global revenue under the GDPR, recent reform in this area could result in a consumer protection regulator imposing their own fine of *at least* up to 4% of the seller or the supplier's annual turnover in the Member State(s) concerned.[97] The regime also contains provisions for

[91] 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

[92] Digital Content Directive, Art 3(1) paragraph 2

[93] Digital Content Directive, Art 3(1) paragraph 1

[94] Digital Content Directive, Art 2(7)

[95] 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, recital 24; 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) at 223-224; See also 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', 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.'

[96] Directive 2005/29/EC of the European Parliament and of the Council 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 ('Unfair Commercial Practices Directive').

[97] Directive (EU) 2019/2161 as regards the better enforcement and modernisation of Union consumer protection rules, OJ L 328, 18.12.2019, p. 7–28 and 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

competitors to take action against malicious use of dark patterns: under 'level playing field' provisions, a competitor can take an action against another trader for their commercial practices as long as it is 'in the interest of consumers'.

Fairness & The Unfair Commercial Practices Directive

Based on the principle of full harmonisation, the Unfair Commercial Practices Directive is set out as follows: Article 5 of the Directive contains a general unfair practice provision. This requires a breach of 'professional diligence' and a 'material distortion' of a consumer's decision. This is very broad and depends on the national interpretation of 'professional diligence' with the circumstances analysed on a case-by-case basis. Articles 6 and 7 contain provisions about misleading omissions and actions. There must be an omission or misleading presentation of information, and which results in the material distortion of the consumer's decision. For a practice to be considered aggressive under Article 8, there must be an element of an aggressive practice like undue influence and material distortion of the consumer's decision. The Directive also contains an Annex of blacklisted items. Once the practice described in the Annex is proved, there is no need to prove that the practice resulted in a material distortion.

Fairness is at the heart of the UCPD. The development of fair commercial practices within the EU is vital for the promotion of the development of cross-border activities.[98] The determination of fairness requires an 'average consumer' commonly presumed to be a 'reasonably well informed and circumspect observer'.[99] However, this fictional, rational, and utility-maximising agent is presumed to gather information, make decisions in an autonomous manner and is sufficiently knowledgeable to critically assess commercial communication.[100] This implies a right of self-determination within the UCPD with consumers either accepting or rejecting the price asked for a product or service in an economic exchange.[101] Unsurprisingly, the UCPD emphasises the role of fairness in the pre-contractual environment by imposing a mixture of conditions for information transparency and bans on practices that take advantage of the recognized shortcomings of consumers. Case law from the CJEU has determined that cognitive and economic factors can impair decision-making in certain environments.[102] Even when an average consumer knows the risk associated with a behaviour, she can still be induced to do more than should be required. Although out of the scope of this paper, the concept of *inducement* is ripe for development for application in digital environments as an important check on manipulative design techniques. For example, in *Dextro,* an inducement to consume more sugar than was healthy to do so, was deemed to be misleading even to average consumers deemed to know better.[103] While under French law, any form of inducement such as a 'bonus payment' or any kind of 'prize' is prohibited in advertising for consumer credit.[104]

---

consumer protection laws and repealing Regulation (EC) No 2006/2004 (Text with EEA relevance) OJ L 345, 27.12.2017, p. 1–26, art 21

[98] Unfair Commercial Practices Directive, recital 2

[99] Cătălin Gabriel Stănescu, 'The Responsible Consumer in The Digital Age: On the Conceptual Shift From 'Average' To 'Responsible' Consumer and The Inadequacy Of The 'Information Paradigm' In Consumer Financial Protection' (2019) 24 Tilburg Law Review

[100] Bram B Duivenvoorde, Consumer Benchmarks in The Unfair Commercial Practices Directive (Springer International PU 2016), at 166

[101] Jan Trzaskowski, '*Lawful Distortion of Consumers' Economic Behaviour – Collateral Damage under the Unfair Commercial Practices Directive*', 27(1) European Business Law Review 25 (2016).

[102] See Tjon Akon, Melvin, '*Personalized Pricing Using Payment Data: Legality and Limits Under European Union and Luxembourg Law*' (December 1, 2019) at 13, <https://kluwerlawonline.com/journalarticle/European+Business+Law+Review/31.5/EULR2020035>, accessed 21 July 2021, citing Case C-210/96 *Gut Springenheide* [1998] ECR I-04657; Case C-195/14 *Teekanne* [2015] Digital reports (Court Reports - general)at para 40; Case T-363/04 *Koipe Corporación*, [2007] ECR II-03355, at para 109; 81 Joined Cases C-54/17 and C-55/17 *Wind Tre and Vodafone Italia*, [2018] OJ C 408, at paras 52-5; See also Case C-562/15 *Carrefour Hypermarchés SAS* [2017] Digital reports (Court Reports - general), at para 31

[103] Case T-100/15 *Dextro Energy GmbH & Co. KG v European Commission* [2016] Digital reports (Court Reports - general), at para 60

[104] Code de la consummation, art L 311-5(5)

The UCPD permits companies to freely determine that data is the 'price' of entry to the product or service. There is no obligation to set a fair, reasonable, or just 'price'. The UCPD presumes that normal market principles of supply-and-demand will set 'prices' appropriately.[105] As discussed briefly above, there is also an increasing acceptance that data has economic value[106] and the cost of entry to digital content. For example, the Guidance on the application of the UCPD recognizes that 'personal data, consumer preferences, and other user generated content as having economic value and are being sold to third parties'[107], but does so without resorting to the bestowment of property rights to data subjects over their personal data.[108]

If a trader does not inform the consumer that the data, he is required to provide to the trader to access the service will be used for commercial purposes could amount to a misleading omission of material information.[109] On a textual reading of Article 6 and 7 UCPD, it is axiomatic that traders 'should not mislead consumers on aspects that are likely to have an impact on their 'transactional decisions'. Using design to obfuscate the processing of personal data will amount to an omission. A dark pattern used to hide the commercial intent behind a commercial practice not only violates the transparency principle of the GDPR, but Article 7(2) and No 22 of Annex I of the UCPD. This reveals an important distinction between the data and consumer protection regimes - the former contains a different type of protection for pre-processing, while the latter regulates the pre-contractual environment.

Dark patterns can also make it appreciably harder for a consumer/data subject to leave a digital environment. Under Article 9(d) UCPD, any practice that makes it more onerous or uses disproportionate non-contractual barriers following the conclusion of a contract and/or during its execution to withdraw may amount to an unfair commercial practice. It will ultimately depend on the case-by-case assessment and the material distortion to the consumers' decision-making. Any design that makes it particularly burdensome for users to terminate or withdrawal from the service could amount to an aggressive commercial practice.[110] This Article's application is particularly apropos for examining the interplay with data protection rights as theoretically, it could be extended to third parties that make it disproportionately difficult for consumers to exercise their rights.

Increasing recognition of the economic value of information relating to consumers' preferences, personal data, and user-generated content could amount to a misleading practice if the dark pattern nudges consumers away from opportunities to rationalize the 'cost' of providing access to their data. The Federation of German Consumer Organisations (VZBV) sought an injunction against an internet company for claiming that its service is 'for free' or 'without charge'. The VZBV argued that this was a blacklisted practice under Point 20 of Annex I as the company derived its revenues from analysing users'

---

[105] Annette Nordhausen Scholes, '*Behavioral Economics and the Autonomous Consumer*', in: The Cambridge Yearbook of European Legal Studies, Volume 14, 2011-2012 (Hart Publishing, 2012), 297-324; Vanessa Mak, '*The Consumer in European Regulatory Private Law*', 381-400 in: The Images of the Consumer in EU Law. Legislation Free Movement and Competition Law (Hart Publishing, 2016)

[106] For example, see Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services (Supply of Digital Content Directive), where the EU legislator has accepted at least to some extent that you can pay with personal data and have consumer law apply, art 3

[107] Guidance on the implementation/application of directive 2005/29/EC on unfair commercial practices SWD/2016/0163 final, at < https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016SC0163>, 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.'

[108] 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, recital 24; See also Jacopo Ciani, '*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) at 223-224.

[109] Unfair Commercial Practices Directive, art 7(5)

[110] Supreme Court of Bulgaria, PS8215, decision no 24117 of 12 December 2012

private data and selling the information to third party traders for the purposes of advertising.[111] An Italian Internet Service Provider was injuncted from claiming in an advertisement that the services it offered were 'free'. Consumers were subjected to 'onerous' obligations like tracking and receiving commercial communications in return for access to a 'free' service. The authorities examined the entirety of the pre-contractual environment and concluded that the omission of the conditions in the advertisement unduly affected their economic behaviour.[112]

The open-textured concept of 'professional diligence' refers to 'the standard of special skill and care which a trader may reasonably be expected to exercise towards consumers, commensurate with honest market practice and/or the general principle of good faith in the trader's field of activity.[113] It facilitates the integration of a sector's best practices into the determination of fairness. In an American context, 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'[114] while 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, reputation, or employment by false or malicious action'.[115] The Association for Computing Machinery's (ACM) Code of Ethics and Professional Conduct encourages members to 'Avoid harm'[116], 'be transparent and provide full disclosure of all pertinent system capabilities, limitations, and potential problems to the appropriate parties'[117], 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'.[118]

The requirement of professional diligence can be used as an indicator of what amounts to acceptable design techniques. Accordingly, the UCPD's prohibition of practices contrary to the requirements of professional diligence can also be used in symbiosis with the industries it regulates.[119] Article 10 of the UCPD encourages professional organizations to develop codes of conduct to hold members to account and apply the principles of the Directive effectively.[120] This symbiosis is not just between the UCPD and European industry codes of conduct. Professional organizations become instrumental in setting the sector's standards and can provide evidential value of what amounts to professional diligence.[121] The UCPD could 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.[122] Article 6(2)(b) UCPD 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.[123] Industry standards can be used to set the legal benchmark for professional diligence –

---

[111] Case *Verbraucherzentrale Bundesverband/Facebook*, Landgericht Berlin, Az. 16O341/15
[112] Decision PI2671 – *Libero Infostrada* paraa. 6, 5th indent by the AGCM. It was taken in the year 2000 before the adoption of the UCPD and based on the national provisions implementing Directive 84/450/EEC on misleading advertising
[113] Jan Schürnbrand, 'Understanding EU Consumer Law' (2010) 74 Rabels Zeitschrift für ausländisches und internationales Privatrecht
[114] International Council of Design, '1-8' (International Council of Design, 2021) <https://www.ico-d.org/database/files/library/icoD_BP_CodeofConduct.pdf> accessed 4 July 2021
[115] 'Code Of Ethics' (ACM Ethics, 2021) <https://ethics.acm.org/code-of-ethics/> accessed 4 July 2021.
[116] ACM Code of Ethics and Professional Conduct at Section 1.2
[117] ACM Code of Ethics and Professional Conduct at Section 1.3
[118] ACM Code of Ethics and Professional Conduct at Section 1.6
[119] Unfair Commercial Practices Directive, art 5; On the unfairness concept in the UCPD generally, Stephen Weatherill and Ulf Bernitz, The Regulation Of Unfair Commercial Practices Under EC Directive 2005/29 (Hart 2007); H-W Micklitz, '*The General Clause on Unfair Practices*' in GG Howells, H-W Micklitz and T Wilhelmsson (eds), European Fair-Trading Law. The Unfair Commercial Practices Directive (Aldershot: Ashgate, 2006) 83.
[120] See also Unfair Commercial Practices Directive, recital 20
[121] Unfair Commercial Practices Directive, art 5(2)
[122] Unfair Commercial Practices Directive, recital 20
[123] For more on the interplay between professional diligence and codes of conduct, see M.R. Leiser and M. Caruana, "*Dark Patterns': Light to be found in Europe's consumer protection regime?*', (forthcoming 2021); See

even those businesses and traders that have not agreed to the standards set by 'well-behaved' players in the industry.

Sitting at the intersection of freedom of contract, good faith, the freedom to operate a business, and fairness, dark patterns have brought renewed interest in the UCPD's role in regulating the entirety of the transactional process. Its tried and tested principles as well as its approach to determining 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 their regulation. Moreover, many of its provisions look ripe for development and reinterpretation to ensure the appropriate regulation of commercial practices in the digital era in which dark patterns are on the rise. Other consumer protection instruments seemed destined to have more subtle and indirect effects on their inappropriate use.

Good Faith/Unfair Terms/Bad Patterns

As freedom of contract embodies the positive freedom to willingly enter contractual relationships, regulators will not intervene in a contract which is the result of the ordinary interplay of forces; otherwise, uncertainty would undermine the entire contractual process. Furthermore, the CFR provides businesses with the freedom to conduct their affairs in any manner they see fit if it is in accordance with Union and national law.[124] There are exceptions to the general rules of freedom and sanctity of contract. To promote a fairer transaction process or outcome between the parties, courts will intervene in contractual relationships where parties have not met on equal terms. As traders are operating in a professional capacity the law recognises that consumers are in an economically and intellectually weaker position. Unsurprisingly, given the interplay between good faith and fairness, good faith is a key element in statutory unfair terms regimes. By requiring good faith in consumer contracts, the law allows for more contractual freedom between commercial parties of equal bargaining strength and focuses on protecting vulnerable parties from opportunistic behaviour or improper use of contractual terms. The Unfair Contract Terms Directive only applies to "individually non-negotiated contract terms which create an imbalance to the detriment of the consumers" that are contrary to good faith.[125]

Compared to civil law systems, orthodox common law is hostile to good faith. The orthodox sentiment that a general duty of good faith is 'inherently repugnant to the adversarial position of the parties' has been declared by courts.[126] In England and Wales, the weight of judicial opinion suggests there is no recognition in English common law of an overarching and organising principle amounting to a duty to act in good faith in contractual negotiation and performance. However, many of these cases involve commercial contracts where the parties may 'be considered capable of…mak[ing] contracts of their choosing'.[127] Based on a desire to avoid uncertainty and preserve contractual freedom, the common law approach to good faith is characterised by a lack of judicial intervention where contracting parties are of equal bargaining strength. For example, in *MSC Mediterranean Shipping* the court reiterated that there is no 'general organising principle' of good faith in English law.[128] While the common law develops in a more gradual manner[129], civil systems usually place an obligation on parties to operate under a general principle of good faith that can be understood as imposing a duty of 'playing fair', 'coming clean' or 'putting one's cards face upwards on the table'; overall, it is a principle of 'fair and open dealing'.[130] For example, in *Interfoto* the court acknowledged that even where good faith is not explicitly invoked

also C.M.D.S. (Charlotte) Pavillon, 'The Interplay Between The Unfair Commercial Practices Directive And Codes Of Conduct' (2012) 5 Erasmus Law Review at 267

[124] CFR, art 16; See also Weatherill, S. (2014). '*Use and Abuse of the EU's Charter of Fundamental Rights: on the improper veneration of 'freedom of contract*". European Review of Contract Law, 10(1), 167-182 at 167; Prassl, J. (2013). *'Freedom of Contract as a General Principle of EU Law?' Transfers of Undertakings and the Protection of Employer Rights in EU Labour Law: Case C-426/11 Alemo-Herron and others v Parkwood Leisure Ltd'.* Industrial Law Journal, 42(4), 434-446 at 434

[125]Unfair Contract Terms Directive 93/13/EEC

[126] *Walford v Miles* [1992] 1 All ER 453 (HL) at 460; *MSC Mediterranean Shipping Company SA v Cottonex Anstalt* [2016] EWCA Civ 789 (CA)

[127] Reshma Korde, '*Good faith and freedom of contract*' (2000) 7 UCL Juris.Rev 142 at 142

[128] *MSC Mediterranean Shipping Company SA v Cottonex Anstalt* [2016] EWCA Civ 789 (CA) at 45

[129] *Interfoto Picture Library Ltd v Stiletto Visual Programmes Ltd* [1989] 1 QB 433 (CA) 439 339

[130] *Interfoto Picture Library Ltd v Stiletto Visual Programmes Ltd [1989] 1 QB 433 (CA) 439 339 at 439*

in the reasoning, the common law obtains results similar to a general duty of good faith through different means.[131] This is often done through interpretation or implied terms.

The doctrines of fraud, duress, unconscionable conduct, misrepresentation, and, in some instances, the absence of good faith amount to 'demonstrated problems of unfairness'.[132] Developed in national law, the standard for intervention bears significant influence on the 'Unfairness Test' as introduced by the UCTD.[133] The test for unfairness is whether contrary to the requirement of good faith, there is a significant imbalance in the party's rights and obligations under the contract to the detriment of the consumer.[134] Whether a term is unfair is determined by not only taking into account the nature of the subject matter of the contract, but by reference to *all the circumstances when the term was agreed* and to all of the other terms of the contract or of any other contract on which it depends.[135]

Additional protection for consumers subjected to dark patterns can be found in the Unfair Terms in Consumer Contracts Directive (UTCCD)[136]. The Directive includes reference to good faith in respect of consumer contracts, overcoming the reluctance in some member states to require good faith in negotiations. The UTCCD gives effect to the public interest in ensuring consumers are protected against unfair terms.[137] A term is unfair if it has not been individually negotiated and if 'contrary to the requirement of good faith, it causes a significant imbalance in the parties' right and obligations arising under the contract, to the detriment of the consumer'.[138] The basis of the UTCCD is that unfair terms exist only because of the unequal power between businesses and consumers. In *Océano,* the CJEU confirmed that the rationale underlying the UTCCD is rebalancing the unequal position of the parties and the resulting inability of consumers to influence the content of contracts.[139] As the absence of good faith is generally used to obtain an unfair advantage, good faith is imposed upon traders to equal out the impact of any power imbalance. The imposition reflects the circumstances in which good faith duties are imposed under member state law: where parties meet on unequal terms. The UTCCD's Recitals state that an assessment of unfairness must be supplemented by an '*overall evaluation of the different interests involved*', while the overall evaluation constitutes the requirement of good faith.[140] Further, in assessing good faith, attention must be paid to:

> '…the strength of the *bargaining positions* of the parties, whether the consumer had an *inducement* to agree to the term and whether the goods…were sold or supplied to the *special order* of the consumer…the requirement of good faith may be satisfied…where [the seller] deals *fairly and equitably* with the other party whose *legitimate interests* he [or she] has to *take into account*'.[141] [Emphasis added]

The UTCCD covers a narrow set of contracts (business-to-consumer only) but subjected a wide range of

[131] H. Collins, 'Implied Terms: The Foundation In Good Faith And Fair Dealing' (2014) 67 Current Legal Problems at 297, 311.
[132] For a good example of this from the Courts of England and Wales, see *Interfoto Picture Library Ltd v. Stiletto Visual Programmes Ltd* [1989] QB at 433 per Lord Bingham
[133] Consumer Rights Directive, art 3(1)
[134] European Commission Policy Summary, '*Unfair contract terms directive*', <https://ec.europa.eu/info/law/law-topic/consumers/consumer-contracts-law/unfair-contract-terms-directive_en<, accessed 21 July 2021
[135] For example, United Kingdom's Consumer Rights Act 2015, Section 62(5) giving effect to the Consumer Rights Directive
[136] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts OJ L 95, 21.4.1993, p. 29–34
[137] A public interest that has since been judicially recognised: Case C-168/05 *Mostaza Claro* (2006) All ER (D) 322 (Oct) 38
[138] Unfair Terms in Consumer Contracts Directive, art 3(1)
[139] C-240/98 *Océano Grupo Editorial SA v Murciano Quintero* at 25 and C-241-244/98 *Salvat Editores SA v Sanchez Alcón Prades et al* [2000] All ER (D) 873 (Jun) 25; However, note the countervailing academic view that the Directive is better explained as a response to a market failure arising from information asymmetry: e.g. Michael Schillig, 'Directive 93/13 and the 'price term exemption': a comparative analysis in the light of the 'market for lemons' rationale' (2011) 60(4) ICLQ 933
[140] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, recital 16
[141] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, recital 16

terms to review.[142] The wording of the unfairness test (including the reference to good faith) can be found in the Directive's recitals and requires consideration of: (a) the strength of the bargaining positions of the parties; (b) whether the consumer had an inducement to agree to the term; (c) whether the goods or services were sold or supplied to special order of the consumer; and (d) the extent to which the seller or supplier has dealt fairly and equitably with the consumer. The UTCCD also indicates that good faith goes further than simply restraining taking advantage: it requires deference to the interests of the consumer.[143]

The Consumer Rights Directive also notes that good faith requires 'an overall evaluation of the different interests involved'.[144]Recent guidance provided by the Competition and Markets Authority (the 'CMA' is the regulator charged with seeking injunctions for unfair terms under the Consumer Rights Act (CRA) in the United Kingdom), suggests that the good faith in the CRA[145] amounts to an organising principle. For example, the CMA notes that the CRA is intended to protect consumers at *all stages* of their dealings with traders.[146] The guidance also indicates that 'good faith' relates to the drafting and *presentation* of a contract, as well as the way in which it is *negotiated, formed, and carried out*.[147] At a minimum, these comments give a practical indication of the kinds of terms that could be brought before the courts to injunct.

Arguably, these comments also support the notion that good faith is expected in a broad and general sense in consumer dealings in digital environments as well and could be applied to unfair design techniques when used to drive users toward acceptance of the terms and conditions. This is because the concept of good faith cannot apply to a term itself, which is merely a result of negotiations; good faith must apply to the *conduct* (the process of formation and performance) that gets the term into the contract, the conduct that revolves around performing the substance of the term, and the conduct that attempts to assert rights under the term.[148]

Clearly the UTCD intertwines good faith into fairness. The inclusion of good faith under the Unfairness Test amounts to an organising principle that broadly permeates and influences the behaviour of traders in both negotiation and performance. Opportunistic behaviour and bad standards of commercial morality and practice[149] would amount to a violation of both principles. Thus, dark patterns that obfuscate the terms and conditions of the contract, hide important details, and make it appreciably harder to find information could violate the UTCD if a contract term is hidden away. The Consumer Rights Directive (CRD)[150] covers all terms except 'core' ones (the main subject matter of the contract and the price payable) if they are *prominent* and *transparent*[151] and hiding information would be a misleading omission under the UCPD.

Good faith does not compel the suppression of all self-interest (as in fiduciary obligations). Transactions may be fulfilled in the pursuit of profit and commercial interests; however, a trader may not operate unconstrained. Good faith requires more than honesty in fact, particularly as the parties are of unequal

---

[142] Richard Stone and James Devenney, Text, Cases and Materials On Contract Law (4th edn, Routledge 2017) atchp.7.3, referring to Law Commission Report Number 292 and Scottish Law Commission Report Number 199 (Cm 6464 24 February 2005) at para 6

[143] Elizabeth Macdonald, 'Scope and Fairness Of The Unfair Terms In Consumer Contracts Regulations: Director General Of Fair Trading V First National Bank' (2002) 65 The Modern Law Review. at 763, 769

[144] Directive, at recital 16; CMA Guidance (Competition and Markets Authority, '*Unfair contract terms guidance*', <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/450440/Unfair_Terms_Main_Guidance.pdf>, accessed 21 July 2021 at para.2.20

[145] Consumer Rights Act 2015

[146] CMA Guidance at para.1.51

[147] CMA Guidance at para.2.21

[148] Michael Bridge, '*Doubting Good Faith*' (2005) 11 NZBLQ 426 at 439

[149] *Director General of Fair-Trading v First National Bank plc* [2001] UKHL 52 at 17

[150] 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')

[151] For an example of this requirement manifesting itself in national law, see United Kingdom's Consumer Rights Act 2015, at Section 64

bargaining power. This suggests that the duties at the core of good faith amount to an obligation on traders to act 'fairly, openly and equitably', such that any pursuit of self-interest is undertaken in a manner that the community would consider commercially reasonable and decent. Thus, a trader acts fairly where she acts honestly, cooperatively and with integrity such that she does not deliberately, unconsciously or unreasonably take advantage of the consumer's weaker bargaining position; openly where the terms of the contract are clear, transparent, prominent and fully expressed and communicated to the consumer; and equitably where she has duly considered the consumer's legitimate interests in drafting and carrying out the contract to level the impact of the inequality of bargaining power.[152] The conduct required in practice is driven almost entirely by context (e.g. in a contract formed at a distance, communication expectations may be high) or subject matter (e.g. in a contract where the processing of personal data is intertwined, where there is a knowledge imbalance, consideration of the consumer's expectations may feature prominently). In all cases, good faith is designed to ensure equal and fair bargaining between the parties. Acting 'fairly, openly, and equitably' is essential to the integrity of the contractual relationship.

Dark Patterns and Enforcement

Despite the GDPR coming into force a number of years ago now, regulators have been criticised for a lack of meaningful enforcement measures and the non- issuance of fines.[153] Like data protection, the consumer protection's limitations of extant enforcement mechanisms have long been identified as compromising the effectiveness of the consumer protection regime.[154] 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[155] and a series of new enforcement measures therein can play a powerful role in the regulation of dark patterns. With further reform coming in the form of the Directive on representative actions for the protection of the collective interests of consumers ('Collective Redress Directive')[156] (the GDPR is provisionally listed as one of the instruments covered), collective action can be used to enforce the breach against data subjects that were involved with business-to-consumer transactions (i.e., any advertising or contract scenario), using the specific collective action model.

The consumer protection regime not only facilitates the collectivization of resources, but can reduce actual costs while providing consumers with greater participation rights at national rather EU level; for example, the GDPR does not require member states to allow complaints by advocacy groups independent of a data subject's mandate, it merely permits them to do so.[157] Article 11(1) UCPD and Article 7(2) UCTD require member states to ensure consumer rights organizations can bring an action before the national courts and/or administrative authorities. Alongside Article 23 CRD, these provisions obligate Member States to ensure that 'adequate and effective means exist' to ensure compliance with the Directives. The consumer protection acquis provides a significant number of *ex-ante*, *ex-post*, and

---

[152] Case C-415/11 *Aziz v Caixa d'Estalvis de Catalunya, Tarragona i Manresa* [2013] All ER (D) 181 (Mar) at 69, 76.
[153] Dietmar Neuerer, '*Data protection officer Kelber brings new EU authority into play against Facebook & Co*', Handelsblatt. 28 Jan 2020, at https://www.handelsblatt.com/politik/deutschland/datenschutz-verstoesse-datenschuetzer-kelber-bringt-neue-eu-behoerde-gegen-facebook-und-co-ins-spiel/25479302.html?ticket=ST-1442480-R1b691bwE3OeNIRBus6z-ap2, accessed 04 July 2021; Nicole Kobie, (Wired), 27 April 2020, '*Germany says GDPR could collapse as Ireland dallies on big fines*', <https://www.wired.co.uk/article/gdpr-fines-google-facebook> accessed 04 July 2021.
[154] Leiser and Caruana (2020) citing 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.
[155] Directive (EU) 2019/... of the European Parliament and of the Council of ...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, recital 29
[156] 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
[157] General Data Protection Regulation, art 80(2)

preventative measures that could be deployed against a variety of dark patterns. For example, Article 7(1) UCTD, in the interest of consumers and competitors, preventative measures to prevent the continued use of unfair terms in contracts, while 7(2) UCTD permits a consumer rights organization can raise an action before national courts to determine whether terms are unfair and apply appropriate and effective means to prevent their use. The GDPR has equivalent provisions for stopping breaches (i.e., injunction measures) and permitting representative entities enforcing provisions.[158]

A person acting as a data subject will have the right to redress under GDPR. The person acting as a consumer will have the right to redress under the consumer protection *acquis*. A data subject who is also a consumer, in a business-to-consumer relationship can exercise their rights twice: once as a consumer and once as a data subject. The Regulation on cooperation between national authorities responsible for the enforcement of consumer protection laws[159] ('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'[160] or 'widespread infringement with a Union dimension'[161], to bring about the cessation or prohibition of that infringement.[162] Where appropriate, the competent authorities will impose penalties with the entry into application of the Directive on Enforcement and Modernisation of Consumer Law[163] 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,[164] the Unfair Commercial Practices Directive[165], and the Consumer Rights Directive.[166]

Furthermore, the new 'Collective Redress Directive'[167] is set to replace the 'Injunctions Directive'[168] and will introduce class-action style litigation for consumers across the EU. On the surface, this would constitute a far broader procedure than provided for under Article 80 GDPR; fortunately, the GDPR is provisionally listed in Annex I as one of the instruments that will be covered by the Directive. Accordingly, it could be possible for data subjects that are consumers in a business-to-consumer

[158] General Data Protection Regulation, art 80
[159] 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, 27.12.2017, p. 1–26.
[160]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, 27.12.2017, p. 1–26, art 3(3)
[161] 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, 27.12.2017, p. 1–26, art 3(4)
[162] 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, 27.12.2017, p. 1–26, art 21
[163] Directive (EU) 2019/2161 as regards the better enforcement and modernisation of Union consumer protection rules, OJ L 328, 18.12.2019, p. 7–28.
[164] Directive (EU) 2019/2161 as regards the better enforcement and modernisation of Union consumer protection rules, OJ L 328, 18.12.2019, p. 7–28, art 1 (new Art 8b to be inserted in Directive 93/13/EEC)
[165] Directive (EU) 2019/2161 as regards the better enforcement and modernisation of Union consumer protection rules, OJ L 328, 18.12.2019, p. 7–28, art 3 (Art 13 of Directive 2005/29/EC to be replaced by a new Art 13 - Penalties)
[166] Directive (EU) 2019/2161 as regards the better enforcement and modernisation of Union consumer protection rules, OJ L 328, 18.12.2019, p. 7–28, art 4 (Art 24 of Directive 2011/83/EU to be replaced by a new Art 24 - Penalties)
[167] Proposal for a Directive of the European Parliament and of the Council on representative actions for the protection of the collective interests of consumers, and repealing Directive 2009/22/EC, COM/2018/0184 final - 2018/089 (COD)
[168] 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, 1.5.2009, p. 30–36.

relationship to use collective redress. Article 80 and the Collective Redress Directive will be read in conjunction with case law determining their symbiotic interplay.

Consumers, organizations acting on behalf of, and regulators are not the only actors that can restrain the use of dark patterns. Article 11(1) UCPD expressly allows for a competitor to raise an action against another trader for their commercial practices if it is 'in the interest of consumers'.[169] 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. Although Article 82(1) GDPR states 'any person' suffering 'material or non-material damage because of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered', there is nothing in the Regulation's text or guidance document to suggest that 'any person' extends to competitors. However, under Article 11(2) a competitor can raise an action with a national regulator to prevent competitors using a dark pattern. The breach must show the impact on consumers, not just on the market or the other businesses. Any dark pattern that results in increased data capture could result in an economic advantage over a more scrupulous data controller. A competitor could complain to the national regulators for the commercial practices of another when the commercial practice causes harm to the consumer.

In conjunction with the e-Commerce Directive[170], under Article 5 UCPD, regulators can enforce the requirement of professional diligence against platform operators hosting services active in the EU that use dark patterns whenever they become aware of any illegal activity taking place on their websites.[171] Under the Consumer Protection Cooperation (CPC) Regulation[172], competent authorities of the Member States and EEA countries, with the support of the European Commission, have the legal obligation to cooperate in cross-border cases to enforce the EU consumer law in the Single Market. Recital 40 of the E-Commerce Directive further clarifies that 'service providers have a duty to act with a view to preventing or stopping illegal activities'. Based on Article 14 of the same Directive, information society service providers, which act as hosting services are not liable for the information stored by their users when they have no actual knowledge of illegal activities or content. However, Article 14(l)(b) requires that 'the provider upon obtaining knowledge or awareness [of illegal activity or information], acts expeditiously to remove or disable access to the information'. Article 14(3) further clarifies this Article shall not affect the possibility for an administrative authority 'of requiring the service provider to terminate or prevent an infringement'. In this context, in accordance with the e-commerce and the professional diligence requirements under Article 5 of the UCPD, platforms could be ordered to take steps to prevent breaches of law, such as an application using a dark pattern. During the Covid-19 pandemic, the Consumer Protection Authorities released a common position including ambitious language about how platforms should handle malicious and unscrupulous traders using unfair commercial practices to take advantage of the panic about the pandemic.[173] Platforms responded positively, voluntarily taking various proactive measures to eliminate harmful content.[174] This interplay

[169] See also Unfair Commercial Practices Directive, recitals 6 and 8.
[170] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), OJ L 178, 17 July 2000, at 1–16.
[171] Commission Recommendation of 1 March 2018 on measures to effectively tackle illegal content online (C (2018) 1177 final) on clearer 'notice and action' procedures for notifying illegal content, including fast-track procedures for 'trusted flaggers'.
[172] 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)
[173] European Commission/Consumer Protection Cooperation (CPC) Network Common Position pf CPC Authorities Stopping scams and tackling unfair business practices on online platforms in the context of the Coronavirus outbreak in the EU, <https://ec.europa.eu/info/sites/info/files/live_work_travel_in_the_eu/consumers/documents/cpc_common_position_covid19.pdf>, accessed 04 July 2021.
[174] Common position of the Consumer Protection Cooperation Network (CPC) on rogue traders during the COVID 19 Outbreak, Scams related to Covid-19: Common Position of the Consumer Protection Cooperation Network (CPC) on rogue traders during the COVID-19 19 Outbreak, <https://ec.europa.eu/info/live-work-travel-

between Art 5 UCPD and the e-commerce Directive reveals two things: first, in a consumer context, the UCPD's fairness principle can be applied to platforms; second, it is presently deployed with far greater certainty than its 'uncertain' and 'elusive' equivalent in the GDPR.

Conclusion

Dark patterns have emerged as a manipulative design technique that compromise the integrity of the *raison d'entre* of the data and consumer protection regimes. Some take advantage of the GDPR's lack of regulatory authority over the pre-processing environment. Others manipulate users into entering transactions that they otherwise would not make. Academic scholarship from design, consumer psychology, and data protection have identified these techniques as compromising the integrity of the digital ecosystem as well as the principles of autonomy and fairness. They also compromise the ability of users to make rational decisions. As dark patterns compromise the GDPR's requirements for design and compromise the regulatory procedures and parameters a data controller must satisfy as part of the framework for protecting the processing of personal data and compromise performance standards like fairness and professional diligence that define a firm's duty and obligations to users, regulators have shown increased interest over the use of manipulative design in the user experience and interfaces.

The European Union's consumer protection regime has been underutilized but is ripe for shining light on malicious and manipulative dark patterns. The acquis can not only supplement the data protection regime, but it also stands on its own, as a first order instrument more suitable to regulate pre-contractual and pre-processing environments. Its fairness principle is better suited and developed than its equivalent in the data protection regime. Rather than using strict parameters to determine data protection violations, fairness, in the consumer protection sense, can be applied to the entire context and environment in which the processing occurred. As there is a general obligation for Member States to ensure that 'adequate and effective means exist' to ensure compliance with the Directives in the interests of consumers, ongoing reform of the consumer protection regime, and of the Directives on unfair contract terms, unfair commercial practices, and consumer rights may also provide a significant and immeasurable deterrent effect on the use of abusive dark patterns. Better enforcement can rectify the challenges facing the data protection regime.

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.

One of the most important strategies for protecting the digital ecosystem is regulation, yet our present regulatory system for the protection of personal data is often not up to task. An excessive reliance on 'single mechanisms' and the 'principles' of the data protection regime is misguided. All instruments have strengths and weaknesses, but the GDPR is not sufficiently flexible and resilient to successfully address all user problems across all environments.[175] Rather than compartmentalizing regulatory responses along whether a person is a 'data subject' or a 'consumer', a better strategy will seek to harness the strengths of one regulatory mechanism while compensating for its weaknesses using others. Accordingly, a mix of regulatory instruments tied to specific policy objectives is needed for enhanced 'user' protection from dark patterns; for example, proper application of the principle of privacy-by-design to the entirety of the system architecture and any user interfaces could establish whether the design techniques are fair under the consumer protection regime which is better posed to assess the pre-contractual and pre-processing environment. Only this kind of regulatory pluralism, backed up with

eu/consumers/enforcement-consumer-protection/scams-related-covid-19_en#replies-from-online-platforms-including-measures-taken>, accessed 04 July 2021.

[175] B.-J. Koops, 'The Trouble with European Data Protection Law' (2014) 4(4) International Data Privacy Law, 250-261.

appropriate enforcement and sanctions can provide the kind of empowerment that both regimes claim to provide.