



THE CHINESE UNIVERSITY OF HONG KONG
香 港 中 文 大 學

THE CHINESE UNIVERSITY OF HONG KONG

FACULTY OF LAW

Research Paper No. 2024-10

The Algorithmic Exploitation of Consumers

Eliza MIK

Chapter 8

Algorithmic Exploitation of Consumers

Eliza Mik

8.1 Introduction

Scholars and regulators are increasingly aware of the practical implication of such phenomena as algorithmic bias, price discrimination, blackbox AI as well as the misuse of the personal information of consumers. The dangers of algorithmic exploitation in the context of mass market consumer transactions remain, however, somewhat underexplored. One party to the transaction (e.g., Amazon, Meta, Google or BigTech) has all the technology and all the information while the other (the consumer or... human) has none. The key terms in the proceeding sentence are “technology” and “information.” In typical transactional contexts, such as those represented on ecommerce sites, one party provides and *controls* all the technology for the other party to use and has all the information about the products or services being offered, as well as the personal data of the other party. This situation is unprecedented and defies all the assumptions traditionally made about the contracting process.

In online interactions, one party designs and controls the entire transactional environment, often hiding the fact that a transaction is taking place. At present, neither the principles of contract law, nor consumer protection or privacy regulation are capable of addressing the problem of humans being exploited by advanced algorithms. Existing legal frameworks tacitly tolerate the absolute dominance of one party over the other. There are piecemeal solutions that address selective aspects of this phenomenon but there is no attempt to address the problem *in toto*. To aggravate matters, progress in such areas as affective computing, neuromarketing and interface design create a friendly transacting environment that detects, harvests and exploits each possible human weakness.

This chapter describes how technology-driven exploitative commercial practices have passed under the legal and regulatory radar. It examines the extent, if any, recent regulatory updates have managed to address or alleviate the impact of such practices. Given that regulators have a long history of technological incompetence, the chapter focuses on the combined effect of the technologies deployed in exploitative practices. While both regulators and the general public are increasingly becoming aware of the risks accompanying the pervasive use of ecommerce platforms and social media in the context of mental health, political manipulations, and more mundane commercial risks. Consumers are overpaying for their purchases or purchasing products they would not have acquired were it not for the “manipulative online interface.” The problem is not new. What is new is its scale.

The discussion commences with a broad outline of the problem, positioning it within a broader narrative and highlighting its intersections with other areas. Starting with a description of informational and computational asymmetries, it centers on their core implication – extreme personalization. The technologies involved in algorithmic exploitation are complex, but the point is simple: personalization may amount to a form of discrimination and may also obviate the need for the concept of “vulnerable consumer.” The chapter highlights the human tendency to trust computers and that technologies assisting consumers in their online activities operate *against* their interests. The discussion segues into the broader problem of artificial intelligence (AI) alignment to present the competing interests in the areas of surveillance capitalism and

consumer protection. The second part of the chapter discusses the legal instruments that *could* address algorithmic exploitation, starting from privacy and contract law to recent regulatory endeavors by the EU.

8.1.1 *Extreme Asymmetry*

Algorithmic exploitation has countless manifestations in recommender systems, microtargeting,¹ behavioral advertising, dark patterns and, as discussed below, extreme personalization.² It cannot be captured with a single term or equated with a single technology. Algorithmic exploitation derives from the combined, pervasive and mutually-enforcing effect of multiple technologies that influence and manipulate online consumer behavior.³ There is no overt pressure or coercion, but there is a user-friendly interface that entices consumers to visit a particular website, to focus attention on one graphic element, to ignore the link to the terms or regulatory disclosures and to impatiently click through consent management systems.

Technologies can roughly be divided into the user interface (website, app, or other device) and back-end technologies. The user interface is designed to encourage certain choices and to discourage others.⁴ Here, consumer behavior is influenced by means of colors, shapes and general layout. It is rarely appreciated that it is technologically possible to measure the effectiveness of alternative versions of a web page in real-time, on actual consumers, in order to find the most effective design, that is - the design that will lead to the maximum number of clicks or conversions.⁵ After all, the ability to guide one's attention towards particular elements generally translates into the ability to direct the next action. As virtually all online interactions take place via graphical user interfaces, such as websites or apps, most direct influences involve interface design.

What consumers see on the user interface is dictated by what happens in the back-end, in the data-centers filled with thousands of powerful servers hosting a range of technologies. The back-end is associated with the popular terms of Big Data and AI. In a nutshell, the personal information gathered from the online activities of consumers is collected, analyzed, and repurposed with the sole aim to improve the profitability of BigTech. In the digital economy, consumers become decontextualized and dehumanized datapoints.⁶ According to Shoshanna Zuboff, human experience is the raw material for translation into behavioral data,⁷ and this behavioral data is used to shape subsequent human experiences, particularly when it comes to purchasing decisions. In sum, the screen is the tip of a very large iceberg composed of an unprecedented arsenal of technologies that determine what consumers see, as well as how and when they see it. The screen influences what consumers do. Interface design is no longer dictated by purely aesthetic or artistic choices of creative professionals, but by data-driven decisions made by scientists and engineers. Every small detail on a website is calculated towards maximum profitability of the seller of goods or services. The problem is not only that one party has more information about a product or service that it is offering. The problem is that one party has more information about the other party as well as more computing power.

¹ P. Lorenz-Spreen et al., 'Boosting people's ability to detect microtargeted advertising' (2021) 11 Scientific Reports 15541.

² Michael Kearns and Aaron Roth, *The Ethical Algorithm* (OUP 2020) 123.

³ Peter-Paul Verbeek, 'Ambient Intelligence and Persuasive Technology: The Blurring Boundaries Between Human and Technology' (2009) 3 *Nanoethics* 231-242.

⁴ Julie Jacko, *The Human-Computer Interaction Handbook*, 3rd ed., (2012 CRC Press), 78-83.

⁵ Stephen Wendel, *Designing for Behavior Change* (O'Reilly, 2014), 256.

⁶ Kate Crawford, *Atlas of AI, Power Politics and the Planetary Costs of Artificial Intelligence* (Yale University Press 2021), 93, 94.

⁷ Shoshanna Zuboff, *The Age of Surveillance Capitalism* (Profile Books, 2019), 8.

Describing algorithmic exploitation as a problem of extreme information asymmetry does not fully convey its nature and scale. The present situation cannot be compared to anything in the past. The inequality of bargaining power has become an inequality of computing power. Technology has not only become omnipotent and dangerous, but often hidden and imperceptible. Online consumers fail to fully appreciate the influence of technology and it is easier to influence people if they are not aware of being influenced. The technological dominance of BigTech over consumers results in an advanced form of Skinner's 'operant conditioning,'⁸ by far exceeding the problems associated with traditional information asymmetries.

8.2 Extreme Personalization

Algorithmic exploitation derives from and encompasses extreme personalization.⁹ Personalization techniques make it possible to adapt the manner of displaying information and the content of such information to individual consumers, to the point of adjusting the layout of the transacting interface to the consumer's idiosyncratic characteristics.¹⁰ Personalization increases the effectiveness of other technologies as it enables the selection or adaptation of sales and marketing strategies to specific consumers and, more importantly, to specific states that individual consumers will be in throughout the day.¹¹ In effect, each consumer can be presented with a customized view of the marketplace.¹² Personalization is usually justified in terms of 'optimizing content' or 'increasing relevance' with the argument being that the average consumer cannot evaluate all the available information, due to time constraints or limited cognitive capabilities.

There is truth in the statement that too many choices and too much information leads to confusion and decreases the quality of the decision-making process.¹³ There is also, at first glance, nothing objectionable with tailoring a product or an offer to the specific needs or desires of an individual person. Personalization is acceptable if it derives from our express or implicit consent. Algorithmic exploitation, however, involves extreme personalization that occurs irrespective of or even against the wishes or desires of the consumer. Personalization aims at increasing profits for BigTech and not at facilitating or improving consumer choices. Personalization aims to entice consumers into more transactions, not to enable them to pursue their individual interests. Consumer preferences are inferred from the consumers' personal information— not from their direct instructions¹⁴ since the content displayed to the consumer is chosen on the basis of the information previously collected from the consumer. A vicious circle forms: prior choices that have been dictated or at least suggested by algorithms reinforce subsequent suggestions made by algorithms. Kearns & Roth observe:

⁸ Zuboff, at 296.

⁹ R A Baeza-Yates, 'Bias in Search and Recommender Systems' (2020) 14 Proceedings of the 14th ACM Conference on Recommender Systems.

¹⁰ Maurits Kaptein, Dean Eckles, 'Heterogeneity in the Effects of Online Persuasion' (2012) 26 J. Interactive Marketing 176, 186.

¹¹ Kearns & Roth, at 123; Berkovsky Shlomo, et al., 'Influencing Individually: Fusing Personalization and Persuasion' (2012) 2 ACM Transactions on Interactive Intelligent Systems 2; Soussan Djamasbi et al., 'Online Viewing and Aesthetic Preferences of Generation Y and the Baby Boomer Generation: Testing User Web Site Experience Through Eye Tracking' (2011) 15 Int'l J Electronic Com 121, 142; Ariel Porat and Lior J Strahilevitz 'Personalizing Default Rules and Disclosure with Big Data' (2014) 112 Michigan L Rev 1418, 1470.

¹² Frank Pasquale, *The Black Box Society* (Harvard University Press, Cambridge, 2015), 80.

¹³ Simona Botti, Sheena S. Iyengar, 'The Dark Side of Choice: When Choice Impairs Social Welfare' (2006) 25 Journal of Public Policy & Marketing 24.

¹⁴ Cf. Kevin Miller, 'Total Surveillance, Big Data, And Predictive Crime Technology: Privacy's Perfect Storm' (2014) 19 Journal of Technology Law & Policy 105.

Most systems are optimized by using prior user feedback, that is, clicks or other trackable user interactions. However, those interactions are biased to the choices that such systems offer to their users, as clicks can only be done on things that are shown to us. Hence, these feedback loops are tainted by presentation or exposure bias.”¹⁵

The consumers’ personal information is not used to discover their actual preferences but to increase the likelihood of a transaction, including the determination of the maximum price a consumer would be willing to pay.

Common examples of personalization are price steering and price discrimination. In the former instance, customers are nudged towards more expensive items; in the latter, different consumers are presented with different prices for identical products.¹⁶ Personalization could thus be regarded as a form of algorithmic discrimination, if we take the dictionary meaning of the word which includes differentiation. Some readers might object to this equation. After all, scholarship and regulators traditionally associate discrimination with unfair differentiations based on gender, race, and age. The problem is that personalization is based not only on the aforementioned attributes but encompasses a wide range of extremely fine-grained attributes, such as specific diseases, emotional states, addictive personalities or even midafternoon sugar cravings. Personal information is leveraged to detect certain states, both permanent and temporary. Those states can be discovered over an extended period of time, by observing the consumers from the moment they pick up their phones (mobile data collection devices) in the morning to the moment they set their alarms at night. The knowledge of such states, just like the presence of a bargaining advantage, is not objectionable. What is objectionable, however, is its commercial exploitation.¹⁷ It seems unfair to exploit the fact that somebody is depressed, be it due to a recent divorce or the passing of a loved one, and therefore more likely to succumb to special offers due to an impaired decision-making ability..

The online businesses do not create these states but take advantage of the accompanying decreases in rational decision-making. Technologies leveraging personal information largely obliterate the distinction between ordinary and vulnerable consumers.¹⁸ As is the case with discrimination, personalization can thus be equated with the exploitation of personal characteristics that often translate into potential vulnerabilities. The only difference is that in the case of personalization, the financial motive is more pronounced. Without entering a prolonged academic debate about specific definitions of algorithmic discrimination or bias, we can agree that such practices are a form of algorithmic exploitation.

Algorithmic bias is generally linked to systematic (or *systemic*) in a system that privileges one group at the expense of another¹⁹ and is usually associated with unfair differentiations based on race, religion, or gender.²⁰ Extreme personalization does not just discriminate against broader groups but introduces unfair distinctions based on specific human characteristics. Any

¹⁵ Kearns & Roth (n 1) 92.

¹⁶ Tal Z. Zarsky, ‘Mine your own Business! Making the Case for the Implications of the Data Mining of Personal Information in the Forum of Public Opinion’ (2002-2003) 2 Yale Journal of Law & Technology 55, 19-22; M. Grochowski et al., ‘Algorithmic Price Discrimination and Consumer Protection A Digital Arms Race?’ (2022) Special Issue, Technology & Regulation 36, 38.

¹⁷ See: Nathan Newman, ‘Search, Antitrust and the Economics of the Control of User Data’ (2014) 31 Yale Journal on Regulation 401, who describes the profiling of Internet users to detect financial ignorance and exploit such, at 444, 445.

¹⁸ Ryan Calo, ‘Digital Market Manipulation’ (2014) 82 George Washington Law Review 995, 999.

¹⁹ See generally, H Cramer et al., ‘Assessing and Addressing Algorithmic Bias in Practice’ (2018) 25 Interactions 58.

²⁰ M Garcia, ‘Racist in the Machine: The Disturbing Implications of Algorithmic Bias’ (2016) 33 World Policy Journal 111-117.

form of differentiation should be prohibited if such differentiation is based on attributes associated with a diminished capacity to make rational decisions. Just as the law prohibits discrimination based on religion, gender or race, it should prohibit discrimination based on grief or a shopping addiction. This is not to say that we should not protect vulnerable communities or groups, especially when it comes to data-driven algorithmic decisions in sensitive domains such as healthcare, social services, education, hiring, and criminal justice. It means, however, that we must recognize and react to the fact that it has become technologically possible to single out and exploit individual traits that make certain persons vulnerable although they do not belong to a protected class or group.²¹

8.3 Trusting Computers

The description of algorithmic exploitation would not be complete without mentioning three interrelated concepts, which amplify this phenomenon or can be regarded as prerequisites of its existence. These concepts are the Eliza Effect, affective computing, and automation bias. In principle, it has been established that humans tend to confide in computers and even to trust them more than other human beings. Kate Darling observes that people are more likely to provide computers with answers to personal questions as they are ‘less worried about the impressions they would make on the computer and less fearful of being judged by them.’²² In other words, human computer interactions favor self-disclosure of personal information. To aggravate matters, humans tend to anthropomorphize computers,²³ that is, to ascribe mental states to them and to treat them as if they were human. This is known as the Eliza Effect.²⁴ The notorious psychotherapist chatbot Eliza was built to demonstrate that the communication between man and machine was superficial. Its deployment proved the opposite - many people became emotionally attached to Eliza and entrusted ‘her’ with their confidential information. It is noteworthy that those who chatted with Eliza were fully aware that they were interacting with a bot. Moreover, the interactions occurred on a simple, if not primitive by today's standards, textual interface.

Additionally, humans tend to prefer suggestions from automated decision-making systems and to ignore contradictory information made without automation, even if correct, a phenomenon referred to as ‘automation bias.’²⁵ The Eliza Effect also converges with the continued progress in the area of so-called affective computing.²⁶ The latter denotes the ability of computers to detect and to tailor their responses to human emotions. The idea behind affective computing is that both conscious and unconscious emotions could be rendered as observable behavior for coding and calculation. A computer could harvest emotions as behavioral information and subsequently mimic such emotions. As early as 1997, Rosalind Picard warned of the possibility of AI to exploit mood-based buying habits. Although the technology was meant to empower not to subjugate,²⁷ it has since been widely deployed by

²¹ S. Barocas, M. Hardt, and A. Narayanan, *Fairness and Machine Learning* (fairmlbook.org 2019), <http://www.fairmlbook.org>.

²² Kate Darling, *The New Breed* (Henry Holt and Co. 2021) 167.

²³ Kate Darling, ‘Who is Johnny? Anthropomorphic Framing Human-Robot Interaction, Integration, and Policy’ in Patrick Lin, Keith Abney, and Ryan Jenkins (eds), *Robot Ethics 2.0* (OUP 2017).

²⁴ Joseph Weizman, ‘ELIZA- A Computer Program for the Study of Natural Language Communication Between Man and Machine’ (1996) 9 *Communications of the ACM* 36, 37.

²⁵ David Lyell and Enrico W. Coiera, ‘Automation bias and verification complexity: a systematic review’ (2017) 24 *Journal of the American Medical Informatics Association* 423.

²⁶ Rosalind W. Picard, *Affective Computing* (MIT Press 1997); Hayri Yigit et al., ‘Towards Evaluating e-Commerce Sites Purchase Intention using Affective Computing, a Preliminary Study’ in *International Conference on Computer-Human Interaction Research and Applications* (CHIRA 2022), 163.

²⁷ Darling, at 287.

social media and ecommerce platforms to make user experiences even more pleasant and to better mask commercial intent.²⁸ The combination of the Eliza Effect, automation bias and affective computing allows AI to create a data-driven, seemingly user friendly and yet deceitful and exploitative transacting environment.

8.4 *Quasi Agents – of Whom?*

In 2017, Michal Gal and Niva Elkin-Koren observed that the next generation of e-commerce will be conducted ‘by digital agents based on algorithms that can handle entire transactions: using data to predict consumers’ preferences, choosing the products or services to purchase, negotiating and executing the transaction automatically.’²⁹ They also predicted that such algorithmic consumers would outsource purchasing decisions to algorithms, ‘thereby minimizing the direct role they play in purchasing decisions.’³⁰ Gal and Elkin-Koren assumed that algorithms could reduce search and transaction costs, help consumers overcome biases to enable more rational choices, and create or strengthen their bargaining power. Speaking with the benefit of hindsight, we can counter these predictions and assumptions with the simple statement that it is difficult to speak of consumer choices when such choices are shaped by algorithms. Search engines, online marketplaces and chatbots assist consumers in achieving their goals: to find the relevant product or information, to compare prices, to place an order or to book a flight. Consumers are given tools that seemingly assist them but, in reality, act against them. Gal and Elkin-Koren observed, somewhat naively, that ‘the race between the two sides to identify and exploit each other’s shortcomings could lead to an algorithm war, the winner of which will enjoy a larger share of the transactional pie.’³¹

While idea of consumers exploiting the shortcomings of online platforms is unfathomable, it is true that consumers may think that a particular technology acts as their *quasi* agent, assisting them in finding the best deal or the lowest price. The technology does not, however, act on behalf or in the interest of the consumer but in the interests of the company who makes it available for consumers to use. A clear distinction must be made between those who encounter and interact with technology (consumers) and those who create and deploy the technology. Technology is designed to maximize the commercial endeavors of the provider and not to realize the personal goals of consumers. This distinction is made clear by Brian Christian:

Our digital butlers are watching closely. They see our private as well as our public lives, our best and worst selves, without necessarily knowing which is which or making a distinction at all. They by and large reside in a kind of uncanny valley of sophistication: able to infer sophisticated models of our desires from our behavior, but unable to be taught, and disinclined to cooperate. They are thinking hard about what we are going to do next, about how they might make their next commission, but they don’t seem to understand what we want, much less who we hope to become.³²

To complicate matters, to fully leverage AI’s superior abilities in terms of speed and efficiency, tech companies provide AI with a large degree of latitude or even autonomy. Amazon cannot directly supervise and confirm every operation, it can only set transaction parameters and let

²⁸ Ibid.

²⁹ Michal S. Gal and Niva Elkin-Koren, ‘Algorithmic Consumers’ (2017) 30 Harvard Journal of Law & Technology 309, 311.

³⁰ Ibid, at 311.

³¹ Ibid.

³² Brian Christian, *The Alignment Problem* (W.W. Norton, 2020), 275.

the algorithm ‘operate in the wild.’ This absence of direct supervision can lead to problems of misalignment. Which leads to the next point.

8.5 Algorithmic Alignment

Algorithmic exploitation intersects with the alignment problem, the challenge of ensuring that an AI system’s goals and behavior align with human values.³³ As indicated, technologies operate with increasing autonomy and at speeds that preclude humans from evaluating whether their operations are responsible or ethical. The alignment problem is attributable to a number of factors, including the difficulty to define and encode human values into an AI system.³⁴ An AI may extrapolate initial human preferences to achieve the desired objective while also leading to outright harmful consequences. For example, a system tasked with increasing profit may target particularly susceptible consumers based on their recent problems (bankruptcy, divorce, addiction). In effect, even if an algorithm was correctly programmed not to exploit vulnerable consumers, setting its objective function³⁵ to the maximization of corporate profit may, inadvertently, lead to such exploitation. This side effect may become amplified if the original intent is mis-specified. It is not that many consumers will pay a larger amount than others, but that many customers may engage in transactions they wouldn’t have otherwise entered into.

Misalignment may be accidental, not deliberate. More importantly, as humans have diverse and competing values, it may be impossible to formalize a unified set of goals that satisfies everyone’s preferences. In practice, there are two types of alignment. Direct alignment considers whether a system accomplishes the goals of its operator. Social alignment considers the system’s effects on society in general, including whether it imposes externalities on others. Whereas solutions to the direct alignment problem are technical and center on robustness and interpretability, social alignment addresses conflicts between individual and group-level goals. Existing scholarship often fails to distinguish between these two types. Brian Christian defines the problem as ‘how to ensure that these models capture our norms and values, understand what we mean or intend, and, above all, do what we want.’³⁶ Stuart Russell describes value alignment as ensuring that we do not ‘inadvertently, imbue machines with objectives that are imperfectly aligned with our own.’³⁷ These statements do not clarify who we or our refers to. Jason Gabriel asks: ‘How are we to decide which principles or objectives to encode in AI—and who has the right to make these decisions—given that we live in a pluralistic world that is full of competing conceptions of value?’³⁸ It is stated that ‘AI A is aligned with an operator H, if A is trying to do what H wants it to do.’³⁹ H, however, may want the AI to do something that will impose externalities on others and it is externalities that underlie the aforementioned distinction.

Externalities occur when an AI system affects consumers without their consent and not for their benefit. Examples are AI systems that manipulate consumers’ purchasing decisions under

³³ See generally, Jan H. Kirchner et al., ‘Understanding AI Alignment Research: A Systematic Analysis’ (Arxiv.org, 2022), <https://arxiv.org/pdf/2206.02841.pdf>

³⁴ Kearns & Roth, at 170, 171.

³⁵ In machine learning, the objective function is the goal set for a given algorithm, “something” to be optimized or achieved. In more technical terms, it is the mathematical function that measures the difference between the predicted output of a machine learning model and the actual target values; see generally: Stuart J Russell, Peter Norvig, *Artificial Intelligence: A Modern Approach* (4th ed Pearson 2021), 128, 129.

³⁶ Christian, *Alignment Problem*, at 19.

³⁷ Stuart J. Russell, *Human Compatible: Artificial Intelligence and the Problem of Control* (2019 Viking), 149.

³⁸ Jason Gabriel, ‘Artificial Intelligence, Values, and Alignment’ (2020) 30 *Minds & Machines* 411, 412.

³⁹ Paul Christiano, ‘Clarifying AI alignment’ (2018) AI Alignment Forum (Nov. 15, 2028), <https://www.alignmentforum.org/posts/ZcE7EKHTFMBs8eMxn/clarifying-ai-alignment>.

the false pretense of personalization or extract higher prices from vulnerable groups. Before deciding on *which* values or objectives the AI should be aligned with, we must first establish *whose* values or objectives are relevant. The resulting trade-off becomes immediately apparent: are we prioritizing company interests or consumer interests? This is not just about ethics and autonomy but also about economics. We know that AI may be aligned with the values of a company and thus misaligned with its customers. We also know that prioritizing the interests of Big Tech may (at least theoretically) lead to lower prices and increase shareholder value. The trade-off is multifaceted and difficult to present as a zero-sum game. Current approaches to the alignment problem abound with pledges to guarantee AI is fair, upholds human dignity, or promotes human flourishing. Such pledges cannot be translated into actions⁴⁰ and fail to address the problem of conflicting interests. High-level declarations conceal ‘political and normative discord’⁴¹ and cannot guide regulators. At a basic level, values must be translated into norms that can guide policymakers in making suitable laws and regulations.

8.6 Legal and Regulatory ‘Solutions’

Given its systemic character, the problem of algorithmic exploitation must be approached from multiple angles and with different regulatory approaches. Below is a brief description and commentary of such approaches. To date, declarations that “something must be done to ensure fair AI” or to combat “digital inequality,” have not been converted into concrete protections.

8.6.1 *The Privacy Aspect*

Without the ability to collect and process the personal information of billions of consumers, algorithmic exploitation would not be possible. Unfortunately, the regulatory reaction to algorithmic exploitation has come too late. Admittedly, technology moves too fast for any regulator to catch up. At the same time, algorithmic exploitation has been a growing trend for more than a decade and regulators have failed to recognize its scale and potency. Exploitative practices have been present for a long time, what has changed is the underlying technologies. There have been multiple opportunities to address this phenomenon, many of which have been squandered. By the time privacy instruments were enacted, surveillance capitalism had already flourished. Even those who disagree with the previous statement, must acknowledge that the General Data Protection Regulation’s (GDPR) Article 42 has had a limited impact on this phenomenon. The protections contained therein rely on two traditional mechanisms: consent and disclosure.⁴² In principle, as long as users are informed about what will happen with their personal information and as long as they provide their express consent, data collectors are essentially free to do whatever they want with personal information. Disclosure is synonymous with the provision of information. Providing more information in an information rich environment is, however, not conducive to the users gaining actual knowledge of the personal information being collected and used. Informing about a problem does not solve the problem.

⁴⁰ See generally, A Jobin et al., ‘The Global Landscape of AI Ethics Guidelines’ (2019) 1(9) *Nature Machine Intelligence* 389; Luciano Floridi, et al., ‘AI4 People— an Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations’ (2018) 28(4) *Minds and Machines* 689.

⁴¹ B. Mittelstadt, ‘Principles alone cannot guarantee ethical AI’ (2021) *Nature Machine Intelligence* 1.

⁴² Regulation 2016/679 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) (GDPR), Article 4 (11) definition of “consent,” Article 7.

⁴³ In the EU, such requirements also derive from national implementations of the Directive 2000/31/EC on Certain Legal Aspects of Information Services, in particular Electronic Commerce in the Internal Market and the Directive 2011/83/EC on Consumer Rights.

It is common knowledge that online privacy policies are rarely read. The GDPR “has forced disclosure of data collection practices. It has however not changed much in the way consumers can be protected. Simply, it has displaced the cause for inaction, for ‘disengagement’ from one where the consumer was blind, to one where it can now be deemed responsible for his or her failure to protect their privacy and data.”⁴⁴ Theoretically, the requirement of express consent to the collection and processing of personal information could have alleviated algorithmic exploitation by creating friction in the online interaction, forcing users to pause and reflect, however briefly, on the consequences of their actions. Consent has become normatively powerful, because it can override express prohibitions, including those contained in the newly enacted Digital Markets Act (DMA).⁴⁵ The DMA prohibits certain practices involving the processing and aggregation of personal data from platform services, services provided by a gatekeeper or by a third-party unless the user has been presented with a specific choice and has given express consent. In practice, express consent that takes the form of cookie notification bars that require the activation of one or more tick boxes. Cookie notification bars are widely perceived as a nuisance that one has to ‘click through’ in order to proceed. Some websites use more complex cookie management systems that allow users to set preferences for different types of cookies or to control the duration for which cookies are stored. Consumers, however, go online to work, shop and socialize and not to fiddle with privacy settings.

This type of express consent is a fiction. As most of us visit more than one website on more than one device, we constantly encounter interface restrictions (cookie notification bars) that must be overcome. The result is ‘consent fatigue,’ a phenomenon that occurs when individuals are asked to provide consent for various services so frequently that they become desensitized and ignore or rush through consent requests.⁴⁶ Needless to say, AI systems can measure the level of user engagement and hence detect such fatigue. Provided with such information, Big Tech can design interfaces that fulfill all legal requirements but reduce the likelihood of actual review. Consequently, companies deploying such systems can comply with the consent and disclosure requirements in the GDPR, while minimizing the likelihood of users actually reviewing their privacy options. Paradoxically, the very technologies that enable algorithmic exploitation can be deployed to further discourage users from disagreeing to the harvesting of their personal information.

8.6.2 *The Contractual Aspect*

Contract law seems to be of relevance for two reasons. First, our analysis should commence with establishing the baseline: what level of exploitation, if any, is permitted? Regulations should only be debated when existing rules are unable to provide a solution. It is thus necessary to identify the permissible degrees of transactional exploitation allowed in contract law. Second, the pervasive commercialization of online activity leads to its ‘contractualization.’⁴⁷ Most online interactions are subject to terms of use, contracts that purport to govern the very act of entering a website. Admittedly, we go online to consume certain content, such as movies or news articles or to communicate with others, be it for personal or professional purposes. A large part of our online activities could thus be described as contracts for the acquisition of

⁴⁴ C. Riefa, 20; see also: Christine Utz et al., ‘(Un)informed consent: Studying GDPR consent notices in the field’ (2019) Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communication Security 973-990.

⁴⁵ Article 5 DMA; within the meaning of Article 4, point (11) and Article 7 of Regulation (EU) 2016/679.

⁴⁶ For a discussion of mindlessness of consent see, Brett Frischmann, ‘Thoughts on Techno-Social Engineering of Humans and the Freedom to Be Off (or Free from such Engineering)’ (2016) 17 Theoretical Inquiries in L 535.

⁴⁷ See Margaret J Radin, *Boilerplate, The Fine Print, Vanishing Rights, and the Rule of Law* (Princeton University Press, 2013).

certain services. Contract law emerges as the dominant mechanism of regulating online activity. Despite the common belief that contract law glorifies intention and the ‘meeting of minds,’ contract law provides a flexible framework for individuals to maximize their welfare and achieve their private ends. In fact, given the tension between the right to pursue one’s interests and the need to respect the interests of others, this legal area has often been regarded as an instrument of potential commercial oppression.

In 1944, long before commerce became enhanced by technology, Friedrich Kessler emphasised that unlimited freedom of contract enables enterprisers to legislate by contract, often ‘in a substantially authoritarian manner without using the appearance of authoritarian forms.’⁴⁸ Similarly, Brian Coote observed that unless the parties are of equal bargaining power or if the stronger party is prepared to exercise self-restraint, freedom of contract could be an instrument of oppression.⁴⁹ More recently, Nicols Suzor recognised the role of contracts in unilaterally creating and shaping billions of relationships and their potential for subverting values.⁵⁰ Consequently, we must refrain from idealizing the traditional contracting process and acknowledge that it is inherently adversarial and antagonistic.⁵¹ Many contracting scenarios are characterized by imbalances in power and information. No relief is granted ‘just because’ one party enjoyed a bargaining advantage. Bargaining advantages based on superior negotiation skills or better information, are permitted, especially if they derive from a person’s investment in the acquisition of such skills or information. Contract law rewards knowledge and competence. There is no general duty to disclose information unless there is a duty not to misrepresent.. Even if one party knows that the other misunderstands the transaction, the contract remains valid and enforceable. The market fosters expertise so that ‘a knowledgeable party must generally be allowed to take advantage of a less knowledgeable (mistaken) party.’⁵² Some forms of manipulation can be regarded as bargaining techniques, which are expected to be countered with similar techniques or with an awareness that what is communicated may not be factually correct.⁵³ One party is permitted to ignore and hence take advantage of the informational deficiencies or misconceptions of the other as long as such deficiencies or misconceptions are not directly caused the party. The only prohibition is to deliberately manipulate the factual assumptions relied on by the other party in deciding whether to enter into a contract or to actively induce someone to act on inaccurate or incomplete information. Consequently, the point at which the contracting process would be regarded as compromised is difficult to determine.

If we are trying to establish a baseline for the level of ‘permissible exploitation,’ we should examine a hypothetical situation where neither party enjoys a technological advantage. We can assume that in such a situation, each party is allowed and expected to engage in its own bargaining strategy. We can also assume that each party is able to recognize and, to an extent, counter the bargaining strategy of the other. Once we move online and one party is ‘technologically augmented,’ the other may be unable to recognize such strategies and may assume there are none. The online consumer may be unable to detect the technological advantage enjoyed by the other party and to counteract that advantage. Arguably, once bargaining power derives from a technological advantage, the original assumptions can no

⁴⁸ Friedrich Kessler, ‘Contracts of Adhesion – Some Thoughts about Freedom of Contract’ (1943) 43 Columbia Law Review 629, 640.

⁴⁹ Brian Coote, *Contract as Assumption: Essays on a Theme* (Oxford: Hart Publishing, 2010), 33.

⁵⁰ Nicols Suzor, ‘Order Supported by Law: The Enforcement of Rules in Online Communities’ (2012) 63 Mercer Law Review 523, 523.

⁵¹ *Walford v Miles* [1992] 2 AC 128 at 138.

⁵² Mindy, Chen-Wishart, ‘Objectivity and Mistake: The Oxymoron of *Smith v. Hughes*’ in J. Neyers and R. Bronough, S.G.A. Pitel, eds., *Exploring Contract Law* (Hart, 2009), 357.

⁵³ Rick Bigwood, *Exploitative Contracts* (OUP, 2003) 49.

longer be made.⁵⁴ Existing theories and principles were developed at a time where the aforementioned ‘pursuit of one’s interests’ was grounded in real-life interactions between humans, transacting without technological assistance.

The main prerequisites of enforceability, the legal protection of the contractual relationship, are intention and consideration. With regards to intention, the principle is that the statements of the transacting parties are evaluated objectively, and a contract comes into existence if both parties objectively appear to have agreed on a given transaction. There is no requirement of actual, subjective intention and in some circumstances contracts can be formed inadvertently. It also follows that contractual consent need not be express or informed. The objective theory of contract is also qualified by some exceptions, referred to as ‘vitiating factors.’ Addressing deficiencies in intention, these exceptions delineate the level of transactional exploitation or the permissible pursuit of self-interest in contract law.⁵⁵

Vitiating factors constitute the main mechanisms that counteract traditional exploitation. Although contract law does not differentiate between informed and free consent,⁵⁶ it recognizes that the contracting process can be affected by information failures as well as cognitive factors. Each vitiating factor addresses a different deficiency in the contract formation process and has its own narrowly formulated criteria of application. However, as I have described elsewhere,⁵⁷ the examination of individual vitiating factors reveals that they cannot counteract the practices commonly associated with algorithmic exploitation. Moreover, with regards to consideration, we must remember that contract law relies on a purely subjective understanding of value.⁵⁸ The unfairness of a transaction is rarely a reason to terminate a contract since the consideration provided by each party need not be adequate, only sufficient in the eyes of the law. It follows that the sale of a Mercedes for 3 peppercorns will be unobjectionable, at least from the perspective of the common law of contract. The same can be said of an exchange of the right to collect one’s personal information ‘in return for’ the right to access content.

8.6.3 *Unfair Commercial Practices Directive*

The Unfair Commercial Practices Directive (UCPD)⁵⁹ aims to enable consumers to make informed and meaningful choices. Drafted in a technology-neutral manner, Article 5 prohibits unfair commercial practices, defined as ‘practices that (a) are contrary to the requirements of professional diligence, and (b) materially distort or are likely to materially distort the economic behavior of the average consumer.’ A material distortion occurs when a practice impairs the consumer’s ability to make an informed decision, ‘causing the consumer to take a transactional decision that he would not have taken otherwise.’⁶⁰ The term ‘transactional decision’ is interpreted broadly⁶¹ and includes decisions that may not lead to a contract or result in actions

⁵⁴ Lyria Bennet Moses, ‘How To Think About Law, Regulation And Technology: Problems With Technology As A Regulatory Target’ (2013) 5(1) *Law, Innovation and Technology* 1, 17.

⁵⁵ Bigwood, *Exploitative Contracts*, 92.

⁵⁶ Mindy Chen-Wishart, ‘The Nature of Vitiating Factors in Contract Law’ in Gregory Klass et al, eds., *Philosophical Foundations of Contract Law* (Oxford University Press, 2014) 296.

⁵⁷ Eliza Mik, ‘The Erosion of Autonomy in Online Consumer Transactions’ (2016) 8 *Law Innovation & Technology* 1.

⁵⁸ P.S. Atiyah, ‘Contract and Fair Exchange’ (1985) 35 *University of Toronto Law Journal* 1, 19.

⁵⁹ 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, as amended by Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019.

⁶⁰ UCPD Article 2 (e).

⁶¹ UCPD Article 2 (k).

with legal consequences.⁶² Actual distortion is not required, the potential to do so suffices. Moreover, the material distortion requires neither actual economic loss nor substantive unfairness. Although *prima facie* powerful, the ability of Article 5 to address algorithmic exploitation is minimized by the assumptions underlying the term ‘average consumer.’ The latter is deemed to be rational, reasonably well-informed and circumspect.⁶³ These assumptions defy actual consumer behavior as shown by the findings of behavioral economics and neuromarketing that are used to exploit consumer behavior.⁶⁴

Article 5(3) grants additional protections to consumers who are vulnerable due to mental or physical infirmity or age. Consumer vulnerability has become a popular term relating to online exploitation: ‘a person is vulnerable if their permanent or momentary psychological characteristics makes it particularly difficult for them to make autonomous choices and to exert agency over their actions under full consideration of their consequences and outcomes.’⁶⁵ It is important to note that vulnerability need not derive from any of these attributes but is a dynamic state which affects all consumers at different times and circumstances,⁶⁶ and can derive from interactions or from the environment.⁶⁷ More importantly, as indicated in the context of personalization, AI systems do not target vulnerabilities as such but fine-grained states in which a specific person is more likely to click or purchase. The concept of an average consumer is of no importance seems obsolete since each consumer can be vulnerable in its own, idiosyncratic way. Digital markets are breeding grounds for vulnerability. Natali Helberger and others propose the concept of ‘digital vulnerability’ to describe a universal state of defencelessness and susceptibility to the exploitation of power imbalances inherent in the online environment.⁶⁸ Christine Reifa observes that vulnerability is the norm rather than the exception.⁶⁹ If, however, vulnerability is a proxy for susceptibility to manipulations or impaired decision-making then it should not be limited by its source. Each consumer is, in his or her own way, susceptible to manipulations at certain times.

Article 6 prohibits the provision of false information or correct information presented in a manner that deceives or is likely to deceive. Unfortunately, the prohibition is restricted to information concerning the existence or characteristics of a single product or vendor,⁷⁰ and does not extend to information concerning ranges of products or vendors. Annex 1 blacklists the provision of materially inaccurate information on market conditions or the availability of a product ‘with the intention of inducing the consumer to acquire the product at conditions less favorable than normal market conditions.’⁷¹ Article 7(1) shifts the focus from falsehoods to

⁶² European Commission Guidance on the Implementation/Application of Directive 2005/29/EC on Unfair Commercial Practices, (Guidance) 23.

⁶³ UCPD Recital 18; Guiseppe Abbamonte, ‘The Unfair Commercial Practices Directive and its General Prohibition’ in *The Regulation of Unfair Commercial Practices under EC Directive 2005/29* (Hart 2007), 21, 24.

⁶⁴ See R. Incardona and C. Poncibò, ‘The Average Consumer, the Unfair Commercial Practices Directive, and the Cognitive Revolution’ (2007) 30 *Journal of Consumer Policy* 21; Russell B Korobkin and Thomas S Ulen, ‘Law and Behavioral Science: Removing the Rationality Assumption from Law and Economics’ (2000) 88 *California L Rev* 1511.

⁶⁵ I. Strümke, M. Slavkovik, and C. Stachl (2023) ‘Against Algorithmic Exploitation of Human Vulnerabilities’ ArXiv, abs/2301.04993, 4.

⁶⁶ M. Abourehani Mohammadi, et al., ‘Identification psychological disorders based on data in virtual environments using machine learning’ (2020) 7(4) *Journal of Cognitive Psychology* 1-12.

⁶⁷ Lisa Waddington, ‘Vulnerable and confused: the protection of vulnerable consumers under EU law’ (2013) 38 *European Law Review* 757, 768.

⁶⁸ N. Helberger et al., *EU Consumer Protection 2.0, Structured Asymmetries in Digital Consumer Markets* (BEUC 2021).

⁶⁹ C. Riefa, ‘Protecting Vulnerable Consumers in the Digital Single Market’ (2022) 33 *European Business Law Review* 12.

⁷⁰ Article 6 (1) & 6 (2).

⁷¹ UCPD Annex I, point 18.

exclusions by prohibiting omissions of material information that cause or are likely to cause – a transactional decision that would otherwise not have been taken. It could address some forms of algorithmic exploitation were it not for the fact that BigTech could avail itself of the qualification that such omissions may be justified by the ‘limitations of the communication medium.’⁷² Article 7(2) addresses manipulative ways of presenting information, including the failure to identify commercial intent, effectively creating an obligation to disclose the fact that a given interaction is transactional in nature. Moreover, Article 7(4a) requires online businesses, other than search engines, to disclose the parameters determining the ranking of products presented to the consumer as a result of the search query and their relative importance. While the requirements may, theoretically, assist users in understanding search results it also requires that users engage with certain technical details. The consumer is likely to be confused because this information must be provided directly on the query interface, resulting in a cluttered, visually intensive interface. In effect, this disclosure requirement may be ignored in the same way that consumers ignore cookie notification bars.

8.6.4 *Artificial Intelligence Act*

The proposed Artificial Intelligence Act (AIA) could alleviate certain aspects of algorithmic exploitation as it prescribes certain transparency obligations for systems that (i) interact with humans, (ii) are used to detect emotions or determine association with (social) categories based on biometric data, or (iii) generate or manipulate content (deep fakes). Consumers must be informed when they interact with an AI system or when their emotions or characteristics are recognized through automated means. If an AI system is used to generate or manipulate image, audio or video content that appreciably resembles authentic content, there is an obligation to disclose that the content is generated through automated means, subject to exceptions for legitimate purposes (law enforcement, freedom of expression). These disclosures, as the theory goes, would allow persons to make informed choices or withdraw from a given interaction. The problem with this approach is that consumers often do not care whether they are dealing with another human or with an AI. As indicated above, consumers are more willing to disclose personal information in automated interactions. The AIA’s central provision is found in Article 5. It prohibits the placing on the market, putting into service or use of an AI system that:

- (a) deploys subliminal techniques beyond a person’s consciousness or purposefully manipulative or deceptive techniques, with the objective to or the effect of materially distorting a person’s or a group of persons’ behaviour by appreciably impairing the person’s ability to make an informed decision, thereby causing the person to take a decision that that person would not have otherwise taken in a manner that causes or is likely to cause that person, another person or group of persons significant harm;
- (b) exploits any of the vulnerabilities of a person or a specific group of persons, including characteristics of such person’s or a such group’s known or predicted personality traits or social or economic situation age, physical or mental ability with the objective or to the effect of materially distorting the behaviour of that person or a person pertaining to that group in a manner that causes or is likely to cause that person or another person significant harm.

⁷² UCPD Guidance 50

The prohibition is, unfortunately, not accompanied by any explanation of its core terms. The choice of the term subliminal is also questionable. Rostam Neuwirth suggests that perception beyond our consciousness should be termed ‘paraliminal perception, as ‘para’ means beyond.’⁷³ Paraliminal perception would denote the ‘threshold for information that lies beyond our sensory abilities or within our sensory abilities but beyond the cognitive abilities of the mind to detect.’⁷⁴ Given the unclear distinction between the abilities of the senses and the abilities of the brain, ‘beyond’ is a more suitable word for paranormal or extrasensory modes of perception, such as precognition or intuition, while ‘below’ indicates that a given stimulus is perceived by the brain while remaining beyond the scope of consciousness. The regulator is, effectively, trying to determine the threshold of awareness and assumes that such a state exists but does not clarify what constitutes subliminal or a supraliminal stimulus. It is unclear whether ‘something subliminal’ can ‘materially distort’ human behaviour. It is, after all, imperceptible.

Human perception and cognition are complex, difficult to measure and subject to scientific disagreement. What if a particular technology distorts human behavior without being subliminal? Combining terms like ‘subliminal’ with ‘beyond a person’s consciousness’ is bound to create problems in interpretation. How do we define consciousness? How do we separate nonconscious and conscious processes?⁷⁵ Moreover, human perception is multisensory and each of the senses is assumed to have a different threshold.⁷⁶ As ‘thresholds for a given stimulus vary both intra- and interpersonally’⁷⁷ the only way of establishing a violation of the prohibition would be to set discrete thresholds for each individual. This, however, would be impracticable and require a universal threshold on the basis of a legal fiction of the ordinary or reasonable consumer. The difficult distinction between awareness and non-awareness may render the prohibition futile.⁷⁸ Fortunately, these shortcomings are alleviated by the prohibition of other techniques that are “purposefully manipulative or deceptive.” The latter would include dark patterns and, arguably, more extreme forms of personalization.

Another problem concerns the requirement ‘in order to materially distort a person’s behaviour.’ This formulation assumes that a particular technique can in fact affect a person’s behavior in a significant and measurable manner. This creates difficult questions of proof and necessitates or presumes the existence of a stable baseline against which the ‘distorted’ behavior can be compared. A better approach would be to use the term ‘modification’ because it would capture more subtle manipulations. The additional requirement that such distortion must significantly impair the person’s decision-making ability *and* cause him or her to take a decision that would not have been otherwise taken, precludes this provision from being effective in practice. A ‘material distortion’ would have sufficed by itself, so would the ‘appreciable impairment.’ While the difficulties of proving distorted behavior and the impairment of informed decision-making are significant, the difficulties of proving that the any of the said techniques caused the person to ‘take a decision that that person would not have otherwise taken’ seem insurmountable. The provision necessitates a negative proof that something would not have happened were it not for the subliminal, manipulative, or deceptive technique. Would it have to be established that a given person (or group of persons) *would not have* clicked a link or purchased a product? Combined with the requirement that such decision cause or is likely to cause significant harm, subsection (a) will not fulfill its protective function. A single decision, which would otherwise not have been taken, is unlikely to cause ‘significant

⁷³ Rostam Neuwirth, *The EU Artificial Intelligence Act: Regulating Subliminal AI Systems* (Routledge 2022), 17-18

⁷⁴ Neuwirth, *EU Artificial Intelligence Act*, at 18.

⁷⁵ *Ibid.*, at 64.

⁷⁶ *Ibid.*, at 66

⁷⁷ *Ibid.*, at 68, 69.

⁷⁸ *Ibid.*, at 68.

harm.’ Such harm will, however, result from the aggregate effect of many, often daily decisions, that are the product of subtle but continuous manipulations and deceptions. Deception and manipulation are harms in themselves and need not be qualified with the need for significant harm.

As algorithmic exploitation is a large-scale, pervasive, phenomenon affecting millions of people, focusing on one decision that will cause harm is nonsensical. Societal harm does not typically arise from a single occurrence of an AI practice but from the widespread, repetitive or accumulative character of the practice that affects everyone.⁷⁹ The AIA should not just protect person’s or groups of persons, but society at large and also address indirect or aggregate harms.⁸⁰ While it remains difficult to measure or even establish the impact of AI techniques on a single person or even group of persons, it is relatively easy to measure actual human behavior and the economic impact of even the slightest change in a transacting interface on a larger scale. Similar observations can be made with regards to section (b). While it is commendable that the regulator shifted away from the concept of vulnerable consumer and included a wide range of possible sources of vulnerability, the protective effect of this section is weakened by the requirements of material distortion and significant harm. As alluded to above, the exploitation of idiosyncratic vulnerabilities is a harm in itself and needs no further qualifications.

8.6.5 *Digital Services Act*

The Digital Services Act (DSA)⁸¹ confirms the regulator’s awareness that the manner of presenting information directly effects customer behavior.⁸² The online interface decides what customers see and do. Unfortunately, the prescribed solutions are unrealistic as they falsely assume that customers are willing to read regulatory disclosures and to fiddle with the settings. The DSA seems to provide the perfect solution for algorithmic exploitation by prohibiting dark patterns, ‘practices that materially distort or impair, either on purpose or in effect, the ability of recipients of the service to make autonomous and informed choices or decisions,’ nudging or persuading persons to ‘engage in unwanted behaviours or into undesired decisions which have negative consequences for them.’⁸³ The definition in the DSA closely follows the accepted description of the phenomenon of dark patterns. The latter are commonly understood as design techniques used in online interfaces that intentionally manipulate or deceive users into taking actions they may not have intended or desired.⁸⁴ Dark patterns can take various forms, including visual cues, interface elements, hidden advertisements, or content placement to focus users’ attention on specific actions or outcomes, while downplaying or hiding alternative options. Dark patterns generally prioritize the interests of the designers or their clients (such as increasing revenue or user engagement) over the well-being, autonomy, or informed consent of users. Dark patterns are virtually synonymous with most aspects of algorithmic exploitation by exploiting cognitive biases, emotions, and other psychological factors. The DSA specifically mentions online interfaces featuring ‘exploitative design choices to direct the recipients [users]

⁷⁹ Nathalie A. Smuha, *Beyond the Individual: Governing AI’s Societal Harm* (2021) 10 *Internet Policy Review* 1.

⁸⁰ See: Max Tegmark, ‘Position Paper on the AI Act,’ *Future of Life Institute* (2021).

⁸¹ Regulation (Eu) 2022/2065 Of The European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act).

⁸² DSA, Recital 70.

⁸³ DSA, Recital 67.

⁸⁴ C. Gray et al., ‘The Dark (Patterns) Side of UX Design’ (2018) 1 *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* 1-14; C. Bösch et al., ‘Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns’ (2016) 4 *Proceedings on Privacy Enhancing Technologies* 237; A. Mathur et al., ‘Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites’ (2019) *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW), 1–32.

to actions that benefit the provider of online platforms, but which may not be in the recipients' interests.'

More specifically, Article 25(1) titled 'Online interface design and organization' states that online platform providers 'shall not design, organise or operate their online interfaces in a way that deceives or manipulates the recipients of their service or in a way that otherwise materially distorts or impairs the ability of the recipients of their service to make free and informed decisions.' Unfortunately, as the DSA applies exclusively to intermediary services⁸⁵ not the online economy as a whole, the prohibition applies only to online platform providers.⁸⁶ It follows that despite the perfect definition, the very scope of the DSA precludes it from addressing a large range of exploitative practices. For example, while prohibiting the practices when Amazon provides a marketplace for third party sellers, it does not prohibit the same practices when Amazon offers products on its own behalf.

The DSA also prescribes transparency in advertising, including customized disclosure requirements to alert consumers that the displayed information is an advertisement as well as the parameters used to determine the target recipient.⁸⁷ The aim is to prohibit advertisements based on profiling.⁸⁸ In addition to other disclosure obligations,⁸⁹ customers must be provided with salient, clearly identifiable and unambiguous individualized information 'for them to understand when and on whose behalf the advertisement is presented.' The relevant information, including explanations of the main parameters used for profiling and the logic behind such mechanisms, must be directly accessible from the online interface where the advertisement is presented. Such explanations should include information on the method used for presenting the advertisement, the main profiling criteria used, and instructions of how to change such criteria.

Similarly, the DSA prescribes that customers be informed about how recommender systems impact the manner information is displayed and be provided with the ability to influence the manner information is presented. Platform providers must clearly state in their terms and conditions 'the main parameters used' in recommender systems, including options for the customers to modify or influence such parameters.⁹⁰ The latter must include: the criteria which are most significant in determining the information suggested to the recipient of the service and the reasons for the relative importance of those parameters. The functionality to modify or influence the main parameters must be 'directly and easily accessible from the specific section of the online platform's online interface where the information is being prioritised.'⁹¹ These requirements unrealistically assume that consumers have the motivation and technical expertise to analyze and to understand such information.

Summing up, consent and disclosure obligations deriving from different legal instruments apply in tandem so that the design of any online interface must allow for all of them. This results in a cluttered interface filled with too much information. The average consumer already

⁸⁵ See Article 1(1) and Article 2(2), as well as recitals 5, 13 and 15; see also, Regulation (Eu) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services Article 2 (2) for definition of "online intermediation service."

⁸⁶ Article 3(i) for definition of 'online platform.'

⁸⁷ Article 26 DSA; additional transparency requirements are imposed on providers of very large online platforms or of very large online search engines, such requirements are to benefit those who purchase advertising services, not customers, see DSA Art 39 and Recitals 45, 46.

⁸⁸ Art 26 (3) DSA.

⁸⁹ See, e.g.: Regulation (EU) 2016/679, in particular the right to object, automated individual decision-making, including profiling, and specifically the need to obtain consent of the data subject prior to the processing of personal data for targeted advertising; the disclosure of commercial communications deriving from Directive 2005/29/EC.

⁹⁰ DSA Art 27(1).

⁹¹ DSA Art 27(3).

suffers from information overload, limited attention spans and cognitive strain.⁹² Providing more information is generally pointless because it does not guarantee its communication, not to mention comprehension.⁹³ It has been established that an increase in interface elements results in a decrease of the likelihood of users actually accessing such elements, be they links, tick boxes or pop-up windows.⁹⁴ Unsurprisingly, fewer clicks and less clutter lead to more user friendly interfaces.⁹⁵

8.7 Conclusion

Law, in its present state, reveals an unexpected tolerance to practices that a reasonable person would find objectionable. Absent overt pressure resulting in directly measurable harm, many forms of algorithmic exploitation do not register on the radar of existing legal instruments. Recent regulatory proposals can be regarded as inadequate and fundamentally misconceived, especially with regards to the concepts of the average consumer and the various sources of vulnerability. It is unclear whether the gaping loopholes derive from bad drafting skills or the failure to appreciate what is technologically possible.

Admittedly, some of the issues discussed above might seem like unnecessary academic hair splitting. We must, however, remember that the smallest inaccuracy in the manner a provision is drafted will be exploited and lead to an aggravation of pervasive algorithmic exploitation. For example, debates whether certain AI practices should be *below*, not *beyond* human perception may seem frivolous, if not unnecessary. Finding the correct terminology is important not only to preclude metaphysical discussions of consciousness but also to prevent fine-grained interpretations that could be turned to the advantage of companies using AI systems.

On one hand, the manipulation of commercial decisions seems trivial in comparison to teen suicide or the subversion of the democratic process. On the other, the fact that entire transactions can be engineered in a manner that meets legal requirements while, at the same time, subtly reducing the likelihood of consumers noticing regulatory disclosures, notices or warnings, should not just raise academic eyebrows but also regulatory alarms. The average consumer, upon learning of the scale of algorithmic exploitation, would be incredulous how little has been done.

⁹² Josef Falkinger, 'Attention Economies' (2007) 133 J Econ Theo 267.

⁹³ Andrew Goodwin, 'Brave New World: Digital Disclosure of Financial Products and Services' (2016) 11 CMLJ 442; O. Ben-Shahar, *More Than you wanted to know: the Failure of Mandated Disclosure* (Princeton University Press, 2014)

⁹⁴ B. A. Huberman. et al, 'Strong Regularities in World Wide Web Surfing' (1998) 33 Science 76.

⁹⁵ Amazon.com, Inc. v. Barnesandnoble.com, Inc., 73 F. Supp. 2d 1228, 1236 (W.D. Wash. 1999) vacated, 239 F.3d 1343 (Fed. Cir. 2001).