Choice Architectures in the Digital Economy: Towards a New Understanding of Digital Vulnerability

Helberger, N.; Sax, M.; Strycharz, J.; Micklitz, H.-W.

DOI
10.1007/s10603-021-09500-5

Publication date
2022

Document Version
Final published version

Published in
Journal of Consumer Policy

Journal of Consumer Policy (2022) 45:175–200
https://doi.org/10.1007/s10603-021-09500-5

ORIGINAL PAPER

Choice Architectures in the Digital Economy: Towards a New Understanding of Digital Vulnerability

N. Helberger[1] · M. Sax[1] · J. Strycharz[2] · H.-W. Micklitz[3]

Received: 15 July 2021 / Accepted: 11 November 2021 / Published online: 22 December 2021

Abstract
In the digital economy, consumer vulnerability is not simply a vantage point from which to assess some consumers' lack of ability to activate their awareness of persuasion. Instead, digital vulnerability describes a universal state of defencelessness and susceptibility to (the exploitation of) power imbalances that are the result of the increasing automation of commerce, datafied consumer–seller relations, and the very architecture of digital marketplaces. Digital vulnerability, we argue, is architectural, relational, and data-driven. Based on our concept of digital vulnerability, we demonstrate how and why using digital technology to render consumers vulnerable is the epitome of an unfair digital commercial practice.

Keywords Digital marketplaces · Unfair commercial practices · Data-driven marketing strategies · Dark patterns · Platforms · Manipulation

In this article, we will revisit the notion of consumer vulnerability for the digital economy. The idea (l) of the "average consumer"[1] permeates large parts of European consumer law and has been pivotal in building a narrative of consumer empowerment and enabling consumers to protect themselves through active and well-informed choices in the marketplace. This is contrasted by the "vulnerable consumer"—a concept that singles out certain groups of consumers that are more susceptible to unfair commercial practices than others, and less able to protect themselves.[2] We will argue that, in digital markets, consumer vulnerability is not simply a vantage point from which to assess some consumers' lack of ability to activate their awareness of persuasion. In digital marketplaces, most if not all consumers are

[1] In the sense of a consumer who can be considered to be reasonably well-informed, observant and circumspect, European Court of Justice, Case C-210/96 *Gut Springenheide and Tusky* [1998] ECR I-4657, para 31.
[2] Article 5 (3) UCP defines the vulnerable consumer as a member of a "clearly identifiable group of consumers who are particularly vulnerable to the practice or the underlying product because of their mental or physical infirmity, age or credulity in a way which the trader could reasonably be expected to foresee.".

✉ N. Helberger
n.helberger@uva.nl

[1] Institute for Information Law, University of Amsterdam, Amsterdam, The Netherlands

[2] University of Amsterdam, Amsterdam School of Communication Research, Amsterdam, The Netherlands

[3] European University Institute, Florence, Italy

potentially vulnerable. Instead of singling out certain groups of consumers, digital vulnerability describes a universal state of defencelessness and susceptibility to (the exploitation of) power imbalances that are the result of increasing automation of commerce, datafied consumer–seller relations, and the very architecture of digital marketplaces. Finally, we will demonstrate why using digital technology to render consumers vulnerable is the epitome of an unfair digital commercial practice.

With the digitization of consumer markets, consumers as well as traders increasingly rely on algorithmic profiling, automated decision-making, and predictive analytics. Nothing has made that more obvious than the COVID-19 crisis, with large parts of consumer activity moving into online spaces and onto digital platforms such as Amazon, Bol.com, eBay, and online supermarket ordering systems. These systems are largely data-driven or otherwise using optimisation strategies[3] to recommend services, remind us of products that we might still like to buy, or provide us with personalized offers and promotions. Our online consumer behaviour is registered 24/7, monitoring every step in the consumer journey, submitting us to a constant stream of A/B testing and interventions to optimize the system and the consumer–seller relationship. Data-driven commercial strategies are embedded in a sophisticated web of smart speakers, intelligent household appliances, in-store surveillance, and apps and trackers that feed into the stream of data—data that will ultimately create virtual representations of consumers and, perhaps more importantly, consumer "commercialisation potential". The overall objective of these practices is to render consumers receptive to digital marketing strategies that use digital technologies to optimize commercial practices with the goal of selling products and services to consumers. Doing so can enhance the consumer experience, help the consumer to find the goods and services they are looking for, and intensify and personalize the relationship between trader and consumer. The use of digital technology and data analytics, however, can also be the source of new power imbalances between consumers and traders, and new forms of unfair commercial practices.

The creation of personalized "persuasion profiles"[4] in combination with the (ability to implement) adaptive targeting strategies that would deliver the right message at the right time and place to the right consumer lies at the heart of new targeted advertising strategies that seem increasingly to form the backbone of online advertising (Strycharz et al., 2019). These strategies can range from contextual advertising and advertising strategies that are based on rather broadly defined demographics, such as age or gender, to more fine-grained targeting (for instance, matching demographic characteristics with observed behaviour) to very fine-grained forms of psychographic targeting that rely on psychological insights into the personality and behaviour of a consumer, her values, opinions and interests (Burkell & Regan, 2019). Persuasion profiles are only the tip of the iceberg. On a more structural level, the platformisation of e-commerce and the creation of digital choice environments enables new strategies of influencing the choices of consumers that are embedded into the very architecture of these services. Dark patterns, for example, are architectural "user interface design choices that benefit an online service by coercing, steering, or deceiving users into making unintended and potentially harmful decisions" (Chivukula et al.,

[3] We are indebted to Michael Veale for pointing out that optimization strategies can, but do not have to be exclusively driven by analyzing (personal) data.

[4] Defined as "collections of estimates of the expected effects of different influence principles for a specific individual. Hence, an individual's persuasion profile indicates which influence principles are expected to be most effective." (Kaptein et al. 2015b, p. 41).

2019; Forbrukerrådet, 2018; Mathur et al., 2019). Practices can range from default settings, bait and switch, sneak into basket, disguised advertising interfaces, and forced continuity or design choices that make price comparison more difficult (Cara, 2019; Mathur et al., 2019). In such digital choice environments, technology is used more generally to shape the very relationship between advertisers, sellers, and consumers and give it permanence and knowledge of the consumer that evolves over time and intensifies with time (Bol et al., 2018). Examples include e-commerce, media, or fitness apps that users instal on their mobile devices, but also the proliferation of chatbots and virtual assistants whose very mission is to adapt to their users by learning about them and generating knowledge and the power to persuade, but also to proactively engage in triggering—or even creating—(new) vulnerabilities (Calo, 2013).

Unfair commercial practice law can have an important role in assessing the fairness of these practices (Helberger, 2016; Micklitz & Namyslowska, 2020). Indeed, the law's capacity to do so will be an important focal point of this article. A central element in assessing the fairness of any commercial practice is the underlying concept of the consumer, and the extent to which they can be expected to deal in a reasonably well-informed, observant and circumspect way with these practices, or whether they belong to the category of so-called vulnerable consumers. Originally designed to single out situations in which consumers, for reasons largely related to their own personal characteristics (e.g., their age), are particularly susceptible to forms of market persuasion, the concepts of average and vulnerable consumers play an important role in assessing the fairness of a commercial practice. The questions that this article discusses is: what protection can the concept of consumer vulnerability offer the digital consumer? Is the distinction between the average and the vulnerable consumer still fit for the digital age, and if not, do we need a new understanding of "digital vulnerability"? What would its elements be? In so doing, we concentrate explicitly on the conditions that consumers encounter in digital markets, the provisions of the Unfair Commercial Practices Directive (UCP) and, where relevant, the General Data Protection Regulation (GDPR).

Consumer Vulnerability Under Current Consumer Law: A Closer Look

The concept of vulnerable users plays an important role in law generally, not only in consumer law. The vulnerability concept is often used to identify users, or groups of users, that require particular regulatory/policy attention because of their lack of bargaining power, structural inequalities, and other market or social conditions that make them more susceptible to harm (e.g., in the form of discrimination or unequal treatment). At times, it is also used as a concept to allow differentiation in situations in which uniform treatment of all would lead to unfairness for some (Leczykiewicz Weatherill, 2016). For example, Peroni and Timmers (2013) show how in the case law of the European Court of Human Rights, the acknowledgement of vulnerability status for particular groups (such as Roma, people with mental disabilities, people living with HIV, and asylum seekers) has led the court to find special positive obligations on the part of the state, increase the weight of harm in proportionality analysis, and reduce states' margin of appreciation.[5] Malgieri and Niklas (2020) trace the development of vulnerability as a concept in data protection law, mostly

[5] See also Chapman and Carbonetti (2011).

confined to the case of minors who are less aware of potential risks and consequences of data collections and who therefore warrant a higher level of protection (e.g., with respect to the right to transparency, profiling, and informed consent).[6] And in the proposed EU AI Regulation, AI systems that exploit the vulnerabilities of a specific group of persons due to their age, physical, or mental disability shall be banned.[7][8]

Vulnerability in Current Consumer Law

Article 5 (3) UCP describes the vulnerable consumer as a member of a "clearly identifiable group of consumers who are particularly vulnerable to the practice or the underlying product because of their mental or physical infirmity, age or credulity in a way which the trader could reasonably be expected to foresee." As such, the concept of the vulnerable consumer cannot be seen separated from the concept of the average consumer. Together, the concepts of average and vulnerable consumer form the benchmark from which a commercial practice must be assessed (Waddington, 2013). The way both concepts interact showcases an inherent tension in consumer law between protecting users as the weaker party in commercial dealings and enabling consumers to play their role as active and autonomous market participants.

As a rule, commercial practices must be assessed from the perspective of the average consumer, the prototype of European consumer law, who is "reasonably well-informed and reasonably observant and circumspect" (Recital 18 UCP). It is the perspective of the average consumer that is in the first place relevant when assessing the fairness of a particular practice. Article 5 (3) describes the exception to the rule (Micklitz & Namyslowska, 2020). A small range of practices, namely practices that are "likely to materially distort the economic behaviour only of a clearly identifiable group of consumers who are particularly vulnerable to the practice" (Article 5 (3) UCP), if specifically targeted at such consumers are to be assessed from the perspective of an "average member" of a group of vulnerable consumers. A practice that might be acceptable from the perspective of the average consumer may constitute unfairness when targeted at, and assessed from, the perspective of the vulnerable consumer.

Consumers, at least under the UCP, can be considered vulnerable because of their personal characteristics, namely mental or physical infirmity, age or credulity and the effect that these characteristics have on their ability to deal with commercial practices. There is some discussion in the literature as to what extent this list is exhaustive or not (Duivenvoorde, 2013; Howells et al., 2018; Micklitz & Namyslowska, 2020). Common to all the categories listed in Article 5(3) UCP is the focus on internal characteristics within the consumer that affect their ability to adequately deal with commercial practices. Not part of the analysis are external factors such as the degree of exposure to certain practices, or

[6] Recitals 38, 58, 65, and 75 GDPR.

[7] Art. 5 (b) of the Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS, Brussels, 21.4.2021 COM(2021) 206 final.

[8] 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") (Text with EEA relevance).

the consequences that such practices may have for an individual consumer (Duivenvoorde, 2013).

Unlike in human rights law or data protection law, where qualification as a vulnerable group can trigger particular legal obligations or protective duties for states or stakeholders, targeting messages at vulnerable consumers is not in itself an unfair practice, nor does it directly translate into extra (fiduciary or protective) responsibilities or additional information obligations for sellers. Nor, too, is targeting commercial messages at vulnerable consumers an unfair commercial practice as such (Annex 1 UCP, apart from No. 28 – targeting commercial practices directly at children). Consumer vulnerability can be a factor when assessing whether a practice qualifies as either misleading or aggressive. The judge will then assess that practice from the perspective of that particular group.[9] Bluntly speaking, the current role of the vulnerable consumer criterion is that of a vantage point from which commercial practices can be assessed, nothing more, and nothing less. In practice, its role is extremely limited.

Rethinking Vulnerability: Theoretical Considerations

For a critical discussion of the current concept of consumer vulnerability in the context of digital market practices, and before moving to a discussion of digital vulnerability in the next section, it is useful to position Article 5 (3) UCP in the context of the broader theoretical vulnerability discourse. This is so for at least two reasons: First, it helps us to understand (the limitations of) the current way in which the UCP defines consumer vulnerability. Second, it informs our understanding of the future role that unfair commercial practice law should play in dealing with digital consumer vulnerability.

Conceptualizing consumer vulnerability under the UCP (and also the GDPR and human rights law) has traditionally been an attempt to identify particular groups of consumers, or characteristics in consumers, that render a consumer or a group of consumers (such as minors, or the elderly) more susceptible to harm, unequal treatment, and unfairness (Duivenvoorde, 2013). This is what Cole (2016) calls the "victim approach" to vulnerability, as the concept is used to draw attention to the inherent weakness of particular groups, or their inability to fend for their own interests. This framing of consumer vulnerability as a diminished capacity to understand advertising, or to maximize utility and wellbeing (Craig Smith & Cooper-Martin, 1997), resonates with conceptualiszations of consumer vulnerability in the market research and behavioural literature (Baker et al., 2005). It also corresponds rather well with European (neo)-liberal ideals about the role of consumers as active market participants who through their informed choices help to create the conditions of fair and functioning marketplaces.[10] The vulnerable consumer with their inherent and external limitations is an exception to that ideal.

More recent critical advances in the vulnerability literature have criticized this approach of identifying particular groups of vulnerable users as unnecessarily stigmatizing, patronizing, and disconnected from social reality (Cole, 2016; Malgieri & Niklas, 2020). Among

[9] Reich (2016, p. 153) points out that there are, for example, no specific information obligations in the directive. Doubtful at least whether the vulnerability criterion plays a role in the context of Arts 6–8 (Howells 2018, p. 70).

[10] European Economic and Social Committee, EU Consumer Policy strategy 2007–2013 Empowering Consumers, Enhancing Their Welfare, Effectively Protecting Them, at 2–6, COM (2007) 99 final (Mar. 13, 2007).

the most prominent and influential proponents of an alternative approach to vulnerability is Martha Albertson Fineman with her vulnerability theory. According to Fineman, vulnerability is a consequence of human embodiment, carrying with it "the ever-present possibility of harm, injury, and misfortune" (Albertson Fineman, 2008), and therefore "no individual can avoid vulnerability". According to this universal understanding of vulnerability, vulnerable consumers are not the exception; they are the rule. This is essentially the opposite approach to that stipulated by the UCP.

Concerns about the unnecessarily static and stigmatizing effects of a non-universal approach to consumer vulnerability also resonate in the critical consumer law literature. Here, legal scholars have criticized the rigidity of the distinction between either the average or the vulnerable consumer, and the risk of framing consumer protection law as something that only "the weak" are in need of (Howells et al., 2018, pp. 28–29). Arguably, the digitisation of consumer markets is further fuelling these concerns. As Calo points out, digital marketing strategies "tend […] to collapse the ethical and legal distinction between the ordinary and vulnerable consumer" (Calo, 2013, p. 1033). In other words, the vulnerable consumer is no longer the exception, nor is the ordinary or average consumer the rule. Every consumer has a persuasion profile.[11] The digitization of consumer markets and electronic transactions has enabled entirely new forms of personalized persuasion strategies that discover, and build on, individual biases, weaknesses, preferences, and needs and that can be directed, very purposefully, at making consumers—even those that do not belong to the typical categories of vulnerable consumers—vulnerable, in the sense of affecting their ability to rationally deal with a particular marketing practice.

Interestingly, in more recent policy documents from the European Commission, a subtle shift towards this more universal thinking about vulnerability can be observed, and a push for abandoning the static, categorical definition can be discerned (London Economics et al., 2016). A more recent interpretation of consumer vulnerability offered by the European Commission recommends taking "into account that consumer vulnerability is situational, meaning that a consumer can be vulnerable in one situation but not in others, and that some consumers may be more vulnerable than others" (European Commission, 2016).

For some, this more universal understanding of consumer vulnerability probably goes too far. Reich, for example, suggests that the concept of consumer vulnerability needs to be distinguished from the concept of consumer weakness in order to avoid expanding the concept too far (Reich, 2016, p. 141). Concerns about lack of distinctiveness and ability to take into account individual conditions also resonate in the writings of some critiques of universal vulnerability theory. Albertson Fineman (2008, p. 10) concedes: "[b]ecause we are positioned differently within a web of economic and institutional relationships, our vulnerabilities range in magnitude and potential at the individual level. Undeniably universal, human vulnerability is also particular: it is experienced uniquely by each of us and this experience is greatly influenced by the quality and quantity of resources we possess or can command". Still, the universal approach has been criticized because it would leave too little room for considering individual differences, for example because of identity or social status. It can precisely enforce the binary distinction between vulnerable/non-vulnerable that vulnerability theory sought to abolish, but in reverse (Cole, 2016; Cooper, 2015).

Critics of Fineman's vulnerability theory have therefore argued in favour of further building on vulnerability theory in a way that acknowledges the way identities and

[11] In this sense, also Micklitz and Namyslowska (2020), UGP-RL Art. 5 RN 64, who point to the limited usability of the fictive notion of the average consumer in the light of algorithmic personalization strategies.

privileges influence social practices (Cooper, 2015). After all, not all people are alike, some are more affluent, privileged, or better equipped than others. To account for the inequalities this may create, it is necessary to acknowledge the influence of different identities and privileges within each of us as consumers and how they influence social practices (Cooper, 2015). In a similar vein, Cole criticizes the fact that universalism makes it impossible to acknowledge distinctions between particularly vulnerable users: "The concept has been rendered so broad as to obscure the needs of specific groups and individuals, undermining its promise as a conceptual frame to understand and challenge systemic inequalities" (Cole, 2016, p. 267). In response, critics have suggested moving beyond using vulnerability as a label, and transferring attention towards the factors that transform the theoretical possibility of being vulnerable into a concrete situation of unfairness (Peroni & Timmer 2013, p. 1074).[12]

When looking into potential sources of vulnerability, or factors that contribute to making consumers vulnerable, we can turn to a rich body of research in behavioural economics and psychology. Researchers in that field have for some time acknowledged that categorical approaches, such as the one stipulated in Article 5 (3) UCP, essentially disregard external and societal factors that contribute to making consumers vulnerable (Baker et al., 2005). It also falsely creates a perception that consumers are either vulnerable or not. As Baker et al. point out, "actual vulnerability arises from the interaction of individual states, individual characteristics, and external conditions within a context where consumption goals may be hindered and the experience affects personal and social perceptions of self" (Baker et al., 2005, p. 134). In consumer research, the term vulnerability has a broad range of applications, such as individual characteristics (for instance, age, race, physical capabilities), social phenomena (such as stereotyping), business practices (e.g., store layouts, marketer manipulations), and environmental forces (such as natural disasters) (Baker et al., 2005). In general, the consumer research literature relates to two main streams of thought: vulnerability as a result of disadvantages and of marketer manipulation. Regarding disadvantages, research in this stream focuses on individuals disadvantaged through their individual characteristics, socio-economic status, and available resources (Hill & Sharma, 2020). In the case of manipulation, researchers have, for example, examined why and how interpersonal influence can make consumers vulnerable to marketing scams (Langenderfer & Shimp, 2001). Others point out that it is not so much belonging to a group of particular consumers that marks these individuals as vulnerable, but "it is the circumstances that consumers face that determine their vulnerability" (Hill & Sharma, 2020, p. 4). In a similar vein, Cartwright suggests also including contextual, relational, and situational factors, and draws a useful distinction between informational vulnerability (the one that the UCP also focuses on) and pressure, supply, redress and impact vulnerability (Cartwright, 2015). Finally, Berg (2015) underlines that, when studying vulnerabilities, one needs to draw a clear distinction between vulnerabilities and capabilities. Whilst past research has often treated both these constructs as synonymous, reduced capabilities should be seen as possible individual, internal vulnerability drivers, and they should be distinguished from external (i.e., contextual, relational, and situational (Cartwright, 2015)) vulnerability drivers composed of markets' varying consumer conditions or the choice architecture, and that are not related to the capabilities of a single individual. The findings from the behavioural literature hence confirm the intuitions of critical theoretical vulnerability thinkers that indeed everyone

[12] See also Luna (2009), suggesting a layered concept with a focus on the aspects that contribute to vulnerability at its source.

may experience vulnerability in some situations and that consumers may vary in the extent to which they are vulnerable in different contexts—across time and place (Hill & Sharma, 2020).

Looking forward, then, an important contribution of recent theoretical advances in the thinking on vulnerability theory is the recognition that vulnerability is not a state of exception, reserved for particular groups of consumers, but a universal condition. This is also particularly true of digital markets. An important aim behind digital market practices is to identify different circumstances under which persons can be rendered vulnerable, as well as individual trigger points. Thereby, consumer vulnerability becomes a design goal that systems can be optimized for. The behavioural literature has helped to advance our insights into the factors that can contribute to vulnerability, pointing to an array of internal and external (contextual, relational, and situational) factors.

Moreover, both the theoretical and empirical literature show that vulnerability is not only caused by internal factors (as stipulated in Article 5 (3) UCP). Instead, equally or even more influential are external factors and broader societal or institutional arrangements that "originate, sustain, and reinforce vulnerabilities" (Peroni & Timmer, 2013, p. 1059). Proponents of a more universal theory of vulnerability argue that it is not (inherent) vulnerability that distinguishes users and creates inequalities, but rather "systems of power and privilege that interact to produce webs of advantages and disadvantages" (Albertson Fineman, 2008, p. 16). In other words, next to individual factors it is necessary to explore the external and systemic factors that contribute to consumer vulnerability, which is what the next section will do for the case of digital consumer vulnerability.

Finally, the fact that vulnerability is not (only) an inherent condition but the product of external market or societal circumstances and power structures contains important policy implications. Essentially this means that consumers are not simply vulnerable, but that some market structures and configurations make them vulnerable, or even worse: exploit their vulnerabilities. This insight can have important implications for consumer law and policy. Whereas current unfair commercial practice law is essentially focused on accommodating internal vulnerabilities, a more universal vulnerability perspective that also takes into account external factors shifts the analytical focus from vulnerability as a benchmark or vantage point towards an investigation of the role that unfair commercial practice law can have in addressing these more systemic and external circumstances and potential power imbalances. Indeed, as Albertson Fineman (2008, p. 9) has argued, vulnerability theory can be a "powerful conceptual tool with the potential to define an obligation for the state to ensure a richer and more robust guarantee of equality than is currently afforded under the equal protection model". In practice, this means that to truly understand and conceptualize consumer vulnerability, it is necessary to explore market practices, systemic, and institutional conditions that create vulnerability in the first place. This is what the following section will do for the case of digital market practices.

Towards a Concept of Digital Vulnerability

In response to mounting criticism of the traditional interpretation of the vulnerable consumer, the static, categorical definition seems to have been abandoned in more recent guidance documents (London Economics et al., 2016). In a more recent communication, the European Commission (2016) defined the vulnerable consumer as: "A consumer, who, as a

result of socio-demographic characteristics, behavioural characteristics, personal situation, or market environment:

- Is at higher risk of experiencing negative outcomes in the market;
- Has limited ability to maximise their well-being;
- Has difficulty in obtaining or assimilating information;
- Is less able to buy, choose or access suitable products; or
- Is more susceptible to certain marketing practices."

It is worth noting that this new definition by the Commission has moved away from the original focus of Article 5 (3) UCP on internal factors and group vulnerability, towards taking into account not only a more universal conception of vulnerability, but also the relevance of external (situational, contextual, and relational) factors, such as the market environment (see previous section). But what does this mean for digital vulnerability in concrete terms?

With digital practices, commercial messages are only one part in a larger, systemic approach to influencing consumer behaviour. The message is part of the system and can no longer be separated from the technical infrastructure that generates it, because it is a result of what Kaptein et al. (2015) call an "adaptive persuasive system". Accordingly, to be able to evaluate commercial practices in terms of their fairness, it is not enough to evaluate the message; the systemic set-up and the way technology shapes the relationship between consumer and advertiser should also figure prominently in such an analysis.

It follows that a concept of digital vulnerability fit for the digital society should somehow mirror the industry's relentless search for experimental and creative digital marketing practices that seek to "optimize" consumers' patterns of behaviour. The industry tries to identify and target different sources and triggers of vulnerability, as well as a wide range of circumstances under which consumers are—or can be rendered – vulnerable. Our concept of vulnerability should be similarly *dynamic*.

Conceptual Refinements Needed

Before one starts thinking about the conceptual *refinements* that are needed to arrive at a notion of digital vulnerability, it helps to ground such an analysis in a basic, uncontroversial understanding of what the concept of vulnerability generally is about. Anderson (2014, p. 239) provides a helpful minimal definition of vulnerability: "a person is *vulnerable* to the extent to which she is not in a position to prevent occurrences that would undermine what she takes to be important to her." Thus, vulnerability is about one's relation to the world, the forces (social, physical, technical) in the world that can affect anything one deems important, and one's (lack of) control or power over those forces. In the context of digital consumer markets, then, vulnerability is about the power or ability of commercial actors to affect the decisions, desires, and behaviour of the consumer in ways that the consumer, all things considered, does not condone, but also is not in a position to prevent. The challenge, then, is to refine the concept of vulnerability in such a manner that it allows us to capture *all* those ways in which consumers can be affected adversely by actors in digital marketplaces without being able to prevent those occurrences. Moreover, vulnerability does not originate solely in a person's (fixed) characteristics, but in a person's *relation* to other actors.

A first, foundational, conceptual refinement can be found in the work of Rogers et al. (2012) and Mackenzie et al. (2014). Their taxonomy of vulnerability differentiates between *sources* and *states* of vulnerability. This basic distinction will help structure the following discussion.

Sources of Vulnerability

To start with sources of vulnerability, they distinguish between inherent and situational sources. Inherent vulnerabilities are "intrinsic to the human condition" and "arise from our corporeality, our neediness, our dependence on others, and our affective and social natures" (Mackenzie et al., 2014, p. 7). These are the kinds of vulnerabilities Albertson Fineman (2008) discusses. For example, all human beings need social and affective relations and are vulnerable to those relations falling away due to circumstances beyond their own control. Another example is people's need for a healthy body and mind to live a flourishing life and the associated inherent vulnerability to diminishing health due to a wide range of factors. In contrast, situational vulnerabilities are those vulnerabilities that are not an intrinsic part of the human condition, but only arise in particular contexts or situations. These situational vulnerabilities are thus external to the person in question and should be understood in line with the "external factors" affecting vulnerability which were discussed in the previous section. A variety of influences of a different nature—"personal, social, political, or environmental"—can cause or exacerbate inherent and situational vulnerabilities. For example, a failed relationship can make one vulnerable to having one's feelings hurt, a storm can make one vulnerable to having one's property destroyed, and collections of large amounts of data can make one vulnerable to having one's persuasion profile inferred and used for targeting practices.

It is important to emphasize that different people live, act, and decide under different circumstances. So the influence of potential sources of vulnerability on the *specific* situation of an individual is *mediated* by the *specific* circumstances of that person. People live under different socio-economic conditions, which co-determine their ability to respond to diverse sources of vulnerability. Moreover, every person has (to a varying degree) different psychological characteristics which determine (1) one's susceptibility to particular influences, as well as (2) one's ability to *react* to those influences. Finally, past behavioural research points out that the level of cognitive processing and the resulting limitations and biases in decision-making are not uniform, but depend on one's abilities, psychological characteristics, and the context in which the processing takes place (Stanovich et al., 2016).

Another important element to consider is the temporal dimension of situational vulnerabilities. Inherent vulnerabilities are intrinsic to the human condition and are therefore, in principle, always present. But situational vulnerabilities can "be short term, intermittent, or enduring" (Mackenzie et al., 2014, p. 7). For example, a person can experience an unpleasant incident at work and, as a result of that incident, be susceptible to negative or harmful social influences for a few days due to feeling very hurt or insecure. We can, however, also think of situational vulnerabilities that are rather persistent, without being inherent vulnerabilities. Think of a person that suffers from a non-chronic disease for months or years. Their health status may make them situationally vulnerable to being adversely affected by particular influences for longer periods of time (months or years).

States of Vulnerability

Besides asking what causes vulnerabilities, we should also ask *how* vulnerabilities can manifest themselves. This is where the different *states* of vulnerability come in: vulnerabilities can be "dispositional" and "occurrent" (Mackenzie et al., 2014, pp. 8–9). (Both inherent and situational vulnerabilities can be dispositional and occurrent.) The category of "dispositional vulnerabilities" roughly translates to *potential* vulnerabilities. Put differently, dispositional vulnerabilities are those vulnerabilities that have not yet manifested themselves but that could do so given the underlying circumstances—and here one can think of all the inherent and situational sources already discussed. The category of "occurrent vulnerabilities" simply refers to those dispositional vulnerabilities that also actually manifest themselves. Mackenzie et al., (2014, p. 7) provide a helpful example to explain this admittedly abstract but important distinction:

> "[A]ll fertile women of childbearing age are dispositionally vulnerable to life-threatening complications in childbirth. But whether or not a pregnant women is occurrently vulnerable to such complications will depend on a range of factors, both inherent and situational, such as her physical health, medical history, socioeconomic status, geographical location, access to health care, and cultural norms relating to pregnancy and childbirth."

One does not necessarily need to adopt these specific terms to see the usefulness of the distinction. To be able to see and, if needed, address all (potential) vulnerabilities, it is necessary to look beyond those vulnerabilities that already actually occur *right now*. Because dispositional vulnerabilities may *seem* less immediate than occurrent vulnerabilities (which have, by definition, already materialized), it is easy to overlook their significance. In the digital society, however, dispositional vulnerabilities require as much attention as occurrent vulnerabilities. Many situations and contexts involve a structural yet latent potential for triggering or creating vulnerabilities that have not yet materialized. Think, for instance, of a digital service that collects large amounts of user data to infer persuasion profiles. The mere fact that the digital service holds persuasion profiles of its customers renders those customers *dispositionally* vulnerable to, for instance, manipulation. Even if a company does not use those persuasion profiles *right now*, we can and should still ask whether collecting such persuasion profiles is desirable. Dispositional vulnerabilities warrant special attention in our contemporary digital marketplaces, where data-driven dynamically adjustable digital choice architectures can not only identify inherent (ever-present) vulnerabilities, but can also learn/infer how different consumers can be rendered vulnerable under different conditions.

The concept of "dispositional vulnerabilities" thus helps to reveal how vulnerabilities are not necessarily permanent and tied to fixed characteristics of only some persons—i.e., "the vulnerable"—but could potentially materialize for everyone. However, the claim that *everyone* can be rendered dispositionally vulnerable in the digital society needs careful interpretation. It does not follow from this claim that (1) everyone can or always will be rendered *equally* vulnerable and (2) that actual, experienced vulnerabilities always materialize for everyone. The idea of universal dispositional vulnerable (every person has biases, psychological tendencies meaning no person is completely unpersuadable or unmanipulable) still allows for very nuanced stories about the differentiated impact of digital choice architectures on different persons. Put simply, the level of risk involved can be different for each user. For example, some users have more cognitive or technical resources at their

disposal than others to understand the digital environments they navigate and to resist the influences those environments try to have on their behaviour. So, despite a shared dispositional vulnerability to manipulation, the tech-savvy user will have a relatively low risk of being misled, whereas a more naïve user may have a higher risk of being misled. Cognitive limitations and biases are not distributed uniformly over the population and can differ from context to context (Stanovich et al., 2016).[13] Also consider the fact that a general claim of the presence of universal dispositional vulnerability *already implies* that actual—i.e., occurrent—vulnerabilities can materialize differently for different people. Person A may be more susceptible to "social" nudges (e.g., being reminded of what your friends have done in order to stimulate certain behaviours in you), whereas person B may be especially susceptible to user interface tricks where particular buttons/options that suit the vendor or made more salient.

In sum, the claim of universal dispositional vulnerability in the digital society should not be confused with the claim that everyone always is actually experiencing vulnerability, or with the claim that everyone can or will experience the same type or the same degree of vulnerability.

Digital Vulnerability Is Architectural

Building on the basic distinction between sources and states of vulnerabilities, we now turn to specific characteristics of the digital marketplace that introduce the need for a concept of digital vulnerability. An increasing number of interactions between consumers and vendors take place within digital choice architectures. To understand vulnerabilities in the digital society, we need to understand the *properties* of such digital choice architectures. In what follows, we propose that (1) the *architectural* and (2) the relational nature of vulnerabilities bears emphasis, as well as (3) the degree in which a lack of privacy exacerbates or reinforces digital vulnerabilities. In the next section, we discuss three examples to concretize our theoretical discussion on digital vulnerability.

So let us start with the architectural nature of digital vulnerability. The term "choice architecture" was popularized by Thaler and Sunstein (2008). In their book *Nudge*, they explained how choice architectures can be designed to change behaviour, by anticipating known cognitive and affective biases in their design. They mainly focused on analogue choice architectures that are first designed and then put into place (semi)permanently. After the "agile turn" (Gürses & Van Hoboken, 2018), however, such (semi) linear design processes have been transformed. Contemporary digital choice architectures are (1) data-driven, (2) dynamically adjustable, and (3) personalizable. These properties allow for constant experimentation by and optimization of choice architectures.

Because digital choice architectures are data-driven, they can collect user data *continuously*, allowing choice architects to learn how different users interact with the digital environment. The inferred behavioural patterns can be used to propose changes to the digital environment to change patterns of behaviour to secure (more) desirable outcomes for the vendor. This is where the significance of *dynamic adjustability* becomes clear. Contemporary digital choice architectures can be adjusted at any given time. Moreover, different "versions" of a digital environment can be run at the same time (e.g., the by the now (in) famous A/B testing) to perform experiments which allow one to test the effect of different

[13] Thanks to an anonymous reviewer for pointing this out and helping us to refine our argument here.

design choices in real time. The insights from these experiments can then be used to personalize elements of the choice environment in order to optimize the behaviour patterns of groups of users or individual users. This entire process of collecting user data, running experiments, and making adjustments is *cyclical* rather than *linear*. Due to this cyclical nature of contemporary digital commercial practices, a certain "depth" also pertains to the resulting commercial relations and their potential for exploitation of vulnerabilities. By constantly learning more about a consumers' characteristics and their responses to particular cues, the potential for effective manipulation also grows (Susser et al. 2019a).

It is important to emphasize that operating one's choice architecture in this manner is relatively easy nowadays. Consider the app economy, with availability of affordable off-the-shelf services that help app developers to "optimize" their apps roughly as described above. Both Apple and Google—which together dictate the terms of the app economy as intermediaries through their app stores—offer extensive support programs for app developers.[14] Google also offers app developers its Firebase[15] off-the-shelf mobile and web app service, with a wide range of built-in analytics and optimization services.

In terms of consumer vulnerabilities, these contemporary digital choice architectures essentially offer an infrastructure to *automate* the *continuous* search for exploitable consumer vulnerabilities. "Business analytics and optimization" practices are aimed at finding out how to get consumers to "engage" with products and services and how to "convert" them as efficiently as possible. In practice, this comes down to continuously running experiments to discover *any* kind of psychological tendency or cognitive or affective bias that can be leveraged for growth. Here, the importance of focusing on dispositional vulnerabilities becomes clear again. Contemporary businesses do not limit themselves to identifying and targeting clearly observable and already present vulnerabilities; quite to the contrary, the real competitive edge resides in the ability to identify and target personal circumstances and characteristics that make a person dispositionally vulnerable but that have not yet resulted in actual, occurrent vulnerabilities.

In the digital society, vulnerability is architectural because the digital choice architectures we navigate daily are designed to infer or even create vulnerabilities. The vulnerabilities—be they dispositional or occurrent—that consumers can experience are not an unfortunate by-product of digital consumer markets; vulnerabilities are the product of digital consumer markets.

To concretize these conceptual remarks on the architectural dimension to digital vulnerability, consider the following example. Platforms such as Facebook, Instagram, YouTube, Twitch, and TikTok have an interest in maximizing data flows between user and platform. Such platforms also control the digital choice architectures within which privacy policies are presented to users and users must consent to particular data practices. This complete control over the choice environment can, of course, be used to gently nudge users towards those consent options which maximize data flows. Digital vulnerability is at play here in (at least) two distinct ways. First, user data can be employed to "optimize" the privacy settings environment for maximal data flows based on knowledge about how users interact with these choice environments. Second, and related, by "optimizing" the privacy settings environment for maximal data flows, platforms can, in turn, further strengthen their position of power by gaining even more insight into the behaviour and psychology of their users. A

[14] See, e.g., Google's "Google Play Guides' and their 'Academy for App Success" (https://developer.android.com/distribute/best-practices) and Apple's extensive guides on "Business & Analytics" (https://developer.apple.com/app-store/articles/).

[15] https://firebase.google.com/

telling example was recently provided by internal documents that were unsealed because of a lawsuit in the USA. In the unsealed document, internal communications between Google employees showed that even those that were involved with the design of the privacy settings often failed to understand how those settings worked (Cox, 2020).

Digital Vulnerability Is Relational

So far we have established the existence of different sources and states of vulnerability, and that contemporary digital choice architectures offer an infrastructure to identify and exploit a wide range of vulnerabilities by design. An additional perspective that requires elaboration is the *relational* nature of vulnerabilities in the digital society. People are not (just) vulnerable in total isolation; more often than not, it is precisely people's relational ties to others that make them vulnerable to other actors and influences.

Consider, for example, the properties of digital choice architectures discussed above. The potential for identifying and targeting vulnerabilities grows as consumers keep using a particular service or app for a longer period of time. Usage over time means collection of user data over time, which translates to more insights into the vulnerabilities of the user, which in turn translates into more possibilities for efficacious adjustments of the choice architecture to influence behaviour over time. Unsurprisingly, commercial digital services often seek to build ongoing relationships with their users, by "engaging" them and getting them "hooked" (Eyal, 2014). Ongoing commercial relationships grow the potential for exploitation of vulnerabilities.

Another important consideration is the often *asymmetrical* nature of ongoing commercial relationships. As consumers keep using the same services, apps, or platforms over time, the commercial entities offering those services, apps, or platforms will be able to collect and analyse more user data and, as a result, be better able to identify exploitable vulnerabilities. Put simply: as commercial digital relations persist over time, power imbalances become more significant as a direct result of the ongoing relationship. This consideration aligns well with the consideration above about the "depth" component of ongoing commercial relationships and the increasing potential for effective manipulation. Moreover, as consumers use a service, app, or platform for longer periods of time, the more "intense" the relationship may become. As consumers get accustomed to a particular service, app, or platform, they may have a harder time exiting those services, apps, or platforms, or switching over to other suppliers. So the better a seller is able to build an ongoing relationship with a user (partly as a result of the seller's increased knowledge about the user's persuasion profiles), the closer one gets to a situation that resembles (or even constitutes) a situational monopoly (Lele, 2007).

Trust also plays an important role in the process of building ongoing relationships with users in datafied environments and the associated potential for exploiting vulnerabilities. Conceptually, trust and vulnerability are—necessarily—*intertwined* (Wiesemann, 2017). Trust always exists in the absence of certainty; trust under conditions of absolute certainty ceases to be trust. It follows that by trusting someone or something, one *necessarily* makes oneself dispositionally vulnerable to having that trust betrayed.[16] Now, to be sure,

[16] Baier speaks of "special vulnerability" in this context: "If part of what the truster entrusts to the trusted are discretionary powers, then the truster risks abuse of those and the successful disguise of such abuse. The special vulnerability which trust involves is a vulnerability to not yet noticed harm, or to disguised ill will" (Baier 1986, p. 239).

the intertwinement of trust and vulnerability is a fact of life and not bad as such. But trust can of course be *exploited* to render people vulnerable and, in turn, exploit these vulnerabilities. This is where contemporary digital choice architectures come in, for they are the types of environment that are especially suitable for exploiting trust to render consumers vulnerable.

To see why, consider that "trust is a psychological state that represents the trusted person or object as trustworthy, and this may or may not actually be the case" (Nickel, 2015, p. 552). In other words, trust and trustworthiness can come apart (Baier, 1986; Hardin, 2002): "Showing that people trust (within) a design does not imply that it is trustworthy, nor the other way around" (Nickel, 2015, p. 559). Trust is a psychological state that can be evoked, instilled or engineered, whereas trustworthiness refers to the actual factual circumstances that make something *worthy* of trust. Data-driven digital environments that can learn about their users and, moreover, can dynamically be adjusted based on what they learn, are precisely the types of (digital) environments that can *engineer* trust by finding out what it is that makes users trust something and change (elements of) the digital environment accordingly to evoke (a psychological state of) trust. The resulting trust renders consumers vulnerable to the exploitation of that trust. So when consumers trust a digital service, one should always ask whether that trust is warranted, or merely the result of clever targeting.

In the digital society, it is thus especially clear that vulnerabilities typically originate in the *relations* consumers have with digital choice architectures, or with those implementing and operating them. Few consumers enter the digital marketplace as already vulnerable persons, simply by virtue of their personal characteristics. Most of the time, it is precisely people's ongoing involvement in various digital markets and services that renders them *increasingly* dispositionally vulnerable to having their (economic) behaviour manipulated. The longer the relationship between a consumer and a digital service or app persists, the more the app or service establishes a position of power as a result of increased knowledge about its users. Vulnerability, in sum, should not be seen as a (semi-)static *property* of a person that exists independently of a person's relation to their environment; quite to the contrary, it is *precisely* a person's dynamic relationship to their environment that causes them to move in and out of states of vulnerability, depending on the circumstances. To the extent that these circumstances are (largely) controlled by sellers—as is the case in contemporary digital choice architectures—sellers occupy a key position which allows them to identify (or even evoke) and exploit digital vulnerabilities.

Vulnerability as Lack of Privacy

As has become clear, the data-driven nature of contemporary choice architectures contributes to their potential to exploit consumer vulnerabilities. In the digital society, the ability to collect and analyse user data contributes significantly to sellers' position of power. Limiting access to (user) data that help sellers learn about consumers can limit sellers' ability to identify or evoke vulnerabilities which can then be targeted. If we understand privacy as people's ability to control access to those things—places, decisions, as well as information and data—that are important to them, then privacy can be understood to function as an autonomy-enhancing value (Roessler, 2005). Privacy can function as a kind of "shield"

around consumers, protecting them from data practices that may weaken their own position of power vis-à-vis a seller (Calo, 2017). Lack of privacy does not *of itself*, strictly speaking, constitute vulnerability. Rather, the overall lack of privacy that consumers experience fuels precisely those data-driven practices that promote exploitation of vulnerabilities. At the same time (centralized), control over consumer data can result in new accumulations of market power and power imbalances (see, e.g., Laux et al., 2021).[17]

To address a lack of privacy as a potential source of vulnerability, lessons can be learned from the GDPR (Malgieri & Niklas, 2020). Specifically, Article 9 GDPR on the processing of special categories of data is interesting in this regard. By imposing more stringent rules on the processing of data that are considered to be especially sensitive (for instance, data encoding racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic, biometric, and health data, and data concerning one's sex life or sexual orientation) vulnerable individuals or groups are afforded additional protection. Interestingly, and highly relevant for this study, the European Data Protection Board (EDPB) has stipulated that situations in which advertisers use knowledge of the vulnerabilities of data subjects for targeted messages can fall under the prohibition of automated profiling in Article 22 GDPR (EDPB 2020, p. 24). Maglieri & Niklas (2020) have suggested that vulnerability should also play a role in Data Impact Assessments and obligations to privacy by design. Although the GDPR's role in addressing (digital) vulnerability is worth exploring, it also should be mentioned that the "special categories of data" approach suffers from the same outdated outlook on what makes people or data vulnerable and worthy of (additional) protection. The idea that one can distinguish between types of data that are inherently sensitive versus types of data that are *not* inherently sensitive mirrors the outdated approach of ascribing vulnerability to a subset of persons based on a set of predetermined personal characteristics (i.e., age, and physical or mental fitness, to name but some).

Three Examples of Exploiting Digital Vulnerability

Based on the proposed conceptual refinements, we want to discuss three concrete examples of how digital services can exploit (or create) digital vulnerability.

Building of Long-Term Trust Relationship (Vulnerability Is Relational)

For-profit health apps are an example of apps that try to build long-term trust relationships with users and that risk creating or exploiting vulnerabilities in doing so. To start, it is important to observe that nearly all the widely used health and lifestyle apps are for-profit services (MyFitnessPal, Headspace, Strava, to name but some) which operate as *freemium* services. These apps can, in principle, be used for free, but app providers do try to build ongoing relationships with users; in a freemium app context, users must keep coming back to an app and "store value" (Eyal, 2014) into an app because this will increase the chance that those same users can be monetized. On their advice pages for app developers, Apple proposes to "prepare for the long term"[18] because monetization of users works best over time. In this long-term perspective, trust is key. On the same developer page, Apple quotes a selected app developer who explains how important it is to develop *trust*: "[f]rom their

[17] Art. 29 WG: power imbalance as source of vulnerability: Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP 248 rev.01, 10.

[18] https://developer.apple.com/app-store/freemium-business-model/.

first session, we're trying to develop trust with the user. […] Over time, as they see value in the service and the tools we provide, many are going to want to pay for those more robust features".[19] Building of long-term trust relationships is thus key in the freemium context.

It bears emphasis that users that keep coming back to an app can be profitable for a variety of reasons: the more users continue to use an app, (1) the more advertising can be sold, (2) the greater the chances that, somewhere down the line, users can be seduced to pay for additional (premium) services, and (3) the more user data can be collected, which can be sold to third parties or can be used to reinforce 1) and 2).

In the health app context, there is usually a promise that the more a consumer uses an app and the better the app can "get to know" the consumer, the better the app will be able to support (or empower) the consumer in their pursuit of a healthier lifestyle. Users are basically asked to trust a health app to serve users' interests, and volunteer access to their data as well as their decisional sphere with the promise of receiving support for healthy lifestyle endeavours. Such a promise (and a question to trust the health app) can be *especially* appealing—or hard to resist—in the health app context, because health apps deal with health. And health is, as a fact of life, a necessity for every person—one quite literally needs one health to live one's life. Moreover, health performs an important social function (Crawford, 2006) and is often seen as a signifier of being a good, responsible, trustworthy citizen (Lupton, 2013).

Now, to be sure, such relationships between health apps and their users can be empowering and helpful to users. At the same time, however, these relationships also introduce all preconditions for digital vulnerability by virtue of being *ongoing* relationships where health apps learn more and more about their users' patterns of behaviour and psychology. Health app providers can find themselves in a serious position of power, where a user has trusted them with privileged insights into their behaviour and psychology to be helped with some aspect of their health. Such a position of power also grants health app providers the ability either to identify existing vulnerabilities of their user or to render their users vulnerable to commercial practices that *exploit* their privileged position of power. What emerges is a thin line between, on the one hand, collecting user data (often health-related) to help or support users and, on the other hand, exploiting user data to target vulnerabilities for financial gain in a manipulative manner (Sax, 2021a, 2021b). The incentive to build trust relationships with users to ensure optimal monetization can thus, especially in the health (app) context, also introduce digital vulnerability.

Harvesting and Using Consumer Information to Identify or Create Exploitable Vulnerabilities (Vulnerability Is also About Privacy)

The gaming app Pokémon Go provides an example of how a lack of privacy can introduce and/or exacerbate digital vulnerability. Pokémon Go is an augmented reality gaming app for smartphones where Pokémon appears on a map of the real world, based on a player's location. GPS always has to be turned on for the game to work. Pokémon Go is a freemium game, meaning that Niantic, the game developer and publisher, has to find ways to monetize the user base after they have installed and started playing the game. The game experience is carefully optimized for and geared towards so-called microtransactions, very small financial investments (typically a few euros or dollars) to acquire access to virtual items or events in the game. Pokémon Go is especially good at using collected user data to tweak the gaming experience in real time to boost microtransactions.

[19] https://developer.apple.com/app-store/freemium-business-model/.

To understand how a lack of privacy can introduce and/or exacerbate digital vulnerability, it is informative to look at some key game mechanics. There are a few main activities players can undertake in the Pokémon Go game. First of all, players can walk around in the real world and on their corresponding virtual map Pokémon will "spawn" (i.e., appear). The game engine decides which Pokémon spawn; the player has zero control over the spawns. By encountering and catching different Pokémon with pokéballs, players try to complete their Pokémon collection. Second, players can receive "eggs" which, when put into an "incubator", will be "hatched" when a player walks around in the real (and thus corresponding virtual) world for a certain number of kilometres. Different eggs have different "hatch distances", meaning that eggs that require more kilometres to be walked for the egg to hatch will often—but not always—give the player rarer Pokémon. Third, at set locations called "gyms", a very strong Pokémon that has to be beaten by a group of players will appear every now and then. These events are called "raids", and to participate in raids players need to have a "raid pass" which can be used one time to access a raid.

Now, importantly, pokéballs, incubators, and raid passes can be purchased for a small fee (the so-called microtransactions). To make the game as profitable as possible, Niantic wants to design and tweak the gaming experience in such a manner that players are seduced to spend money on pokéballs, incubators, and raid passes. This is where the players' lack of privacy comes in. Pokémon Go collects not only real time location data, but also lots of user data which encode in a very precise how each individual user interacts with the game. These user data allow Niantic to experiment constantly with different types of nudges and offers. For example, they can change the type of Pokémon that can come out of different eggs and see how this affects the purchasing of incubators. In response, Niantic can, and often will, announce limited time events with specific Pokémon (which turned out to be popular based on user data) in eggs, with a bulk discount on incubators. Another example is Niantic varying the placement, duration, and type of raids that appear in the world, in combination with (bulk) discounts on raid passes. In short, by analysing the behaviour patterns of all its users, and their real-time movement through the real (and thus also virtual) world, Niantic can design highly persuasive (or: manipulative?) tweaks to the gaming experience and offers in the in-game shop.

The users' lack of privacy is precisely what allows Niantic to design its notoriously addictive gaming experience. Their use of user data to design game tweaks, offers, and events *in response to* what Niantic thinks/infers the players are responsive to also clearly shows the risk of rendering players vulnerable to these advanced commercial practices.

Creation of Structural Situational Monopolies (Vulnerability Is Architectural)

Gaming apps but also health apps and the use of data-driven practices on certain online platforms are also examples of how the way the app platform is geared towards creating an environment in which users are rendered vulnerable to particular persuasive attempts. A concept that behavioural economists call "situational monopolies" is useful in explaining this. Situational monopolies describe a situation in which products or services are marketed to a captive audience that can then, for instance, be charged higher prices than would be reasonable if consumers were fully autonomous in their choices (Trebilcock, 1993). Situational monopolies are different from structural monopolies. The latter are characterized by the existence of a dominant player in the overall market. Unlike structural monopolies, situational monopolies are circumstantial: In principle, consumers could exercise choice because there are competing products, but because of particular circumstances, they find

themselves in a situation of reduced choice and unequal bargaining power. Whereas structural monopolies are typically analysed under competition law, situational monopoly situations have been dealt by courts under the doctrine of duress and unequal negotiation power (Trebilcock, 1993, p. 355). Baker and Siegelmann (2014) give the example of add-on or "second stage" products, like extra insurances that are offered by the provider of a service. Other insurances are available to users, but the way, for instance, a car company markets and offers a particular insurance as the only viable choice exercises pressure on consumers in such a way that they are willing to even pay higher prices or accept less favourable conditions than if they would buy the insurance from another company.

An argument can be made that a gaming app or a health app that uses the relationship it has built with its users, in combination with data-driven insights into users' preferences and willingness to pay can, under certain circumstances, also constitute a situational monopoly. An example are situations in which the privileged relationship with, and knowledge about, the user is used to influence the autonomous choice of users for competing products and services (even if such products are in principle available). Or, alternatively, influence their willingness to pay a higher price than they would normally do under conditions of functioning competition. Strategic architectural choices can be an important element in creating and reinforcing a situational monopoly position in the digital space. A platform like Facebook is constantly looking for ways to make its infrastructure flexible enough to incorporate new services and functionalities (Helmond et al., 2019). By doing so, Facebook becomes better able to "capture" users in the Facebook experience; the more services and functionalities are integrated into the Facebook experience, the easier it is to suggest to users a Facebook-related functionality or service they are looking for. The seamless integration of services such as Instagram Shopping, WhatsApp Communication, Instant Articles, or Facebook shops creates an immersive environment in which users encounter news, sellers, advertisers, friends, and colleagues without ever having to leave the platform. Consider, for instance, the popularity of Facebook Messenger and the acquisition of WhatsApp by Facebook. For Facebook users, the use of Facebook Messenger is now built seamlessly into the user experience. When a Facebook user wants to message someone, Facebook Messenger is supposed to feel as the "natural" service of choice. Another example is the news. Facebook has, over the years, integrated more and more news functionalities and sources, up until the point where it now has deals with respected global and national news organizations to provide news to users within the Facebook ecosystem. The Facebook recommendation algorithm is then a powerful data-driven mechanisms to connect these different services, saving users the need to switch to outside services and providers, and thereby, quite literally, creates a captive audience. Regulatory proposals, such as the European Digital Services Act (DSA), that re-affirm the discretion of the platform to decide whether or not to offer users the choice between competing recommendation logics, or opt for non-personalisation further contribute to the consolidation of that situational monopoly.

Unlike Facebook, other digital services combine control over a platform with control over end user devices and the technical operating system to offer access to a universe of products and services, as, e.g., Google does, making it impossible or very difficult for users to use products and services from another service universe, like that of Apple. Control over a virtual platform and the technical hardware is also an important architectural choice used by many health app providers to increase their hold on users, making switching ever more difficult. In all these situations, it is the combination of data-driven insights over the user, a service platform geared to establishing lasting relationships with users and certain architectural choices that reduce the likelihood of users moving outside the service universe and thereby reducing autonomy and choice. This becomes especially clear if one accepts a

theory of autonomy which doesn't solely focus on a person's *mental capacities* for reasoning independently, but also takes into consideration a more relational perspective which emphasizes how a person's ability for practicing their autonomy is co-determined by their (digital) surroundings (see Sax, 2021a and Sax, 2021b for a fuller elaboration of this view). So, if one wants to analyse whether a deliberately engineered (quasi-)situational monopoly threatens consumer autonomy, one should not only ask whether a person's capacity for reasoning is *directly* undermined and whether that person could still *formally* choose otherwise. It is equally important to ask which options/choices are really open to people, and how easy it is to see and understand those other options/choices. If a platform uses data to learn about its users and steer users away from noticing or considering other choices, that can indeed impact autonomy even if other options are still *formally* available and a person's mental capacities are not directly undermined.

Though situational monopolies so far have been typically discussed in relation to uncompetitive pricing or coercing choice, in a more data-driven argument, we argue that the concept needs to be extended to situations in which users, because of the situational monopoly, are willing to divulge also with more data than they would normally do under competitive situations and if they felt entirely free to choose.

Implications for Consumer Law and Policy

The current approach towards vulnerability in Article 5 (3) UCPD is outdated and not particularly useful in addressing the situation of the digital consumer. And yet, it is influential also outside the UCP and echoed, for example, in the draft AI regulation (AIA) that proposes an equally limited concept of vulnerability in its Art. 5 (b) AIA. Singling out and labelling particular groups of consumers as vulnerable by considering all other digital consumers as "normal" are also not in line with our findings that digital vulnerability is essentially a universal condition that potentially applies to all consumers in the digital marketplace. What is more, the current approach tends to perpetuate the status quo and is therefore also not particularly helpful from a consumer law and policy point of view.

We have argued that digital vulnerability is inherently *relational* and *architectural* in nature and results from power imbalances between consumers and sellers: consumer vulnerabilities can be identified and/or created because consumers interact with sellers within digital environments that can *learn* about them and be *adapted* accordingly. Given the data-driven nature of contemporary digital commercial practices, every consumer is to a varying degree *dispositionally* vulnerable to being profiled and targeted exploitatively. For consumer law and policy, this means that instead of labelling certain groups or individuals as "vulnerable" or non-vulnerable on the basis of some (semi-) permanent personal characteristic(s), the focus should shift to the properties and commercial practices of digital choice environments that can render everyone (dispositionally) vulnerable under the right conditions. Or, as Cole suggests: "Vulnerability has to be reframed as a claim about injustice" (Cole, 2016, p. 273).

The importance of the architectural and relational side of vulnerability cannot be overemphasized. In the ongoing political discussions around the recent EU proposals for the digital market, there is a strong tendency to differentiate between practices that render the consumer vulnerable and those that might even empower the consumer. The European Commission has announced a revision of the UCPD Guidelines for December 2022. Here, the European Commission seems to be trying to distinguish between lawful and unlawful

practices, whilst leaving out the external structural dimension. Whilst it is true that, for instance, profiling is not necessarily detrimental to consumers, our conceptualisation of digital vulnerability requires to look first at the external structural dimension of vulnerability enshrined in profiling which is under analysed and underrepresented in the search for a feasible regulatory design. Not least due to the strong focus of the potential detrimental effects of the individual consumer, the debate is turning away of what we identify to be the "true problem" for consumers. The external architectural design has to be kept distinct from the internal individual effects in concrete circumstances.

Therefore a renewed, universal perspective on consumer vulnerability involves a range of important implications for law and policy. First, establishing that the (dispositionally) vulnerable consumer is the norm, rather than the exception, translates into a conceptual shift and a new focus on identifying and declaring those practices unfair that exploit vulnerabilities and power asymmetries, thereby leading to situations of unfairness and inequality. If we all are vulnerable in principle, the real question is not so much whether we are vulnerable, but when digital technologies are used to single us out, to make us dispositionally vulnerable through the choice architecture and (ab)use our inherent vulnerabilities to make us take decisions that we would otherwise not have taken. This also means though that the fact that (almost) every consumer is rendered dispositionally vulnerable by contemporary digital commercial practices is not enough to speak of an unfair commercial practice. The dispositional vulnerability materializes when a seller decides to target those *dispositional* vulnerabilities in order to *actually* adversely influence—or distort as a result of competition—the behaviour of consumers (in this sense also Duivenvoorde, and Calo who suggests a distinction between making vulnerable, and exploiting vulnerabilities). A dispositional vulnerability then becomes an occurrent vulnerability, which is where the actual unfairness is introduced.[20]Interestingly, this aspect of using digital technology to exploit or even create vulnerabilities with the goal of influencing behaviour is also reflected in Art. 5 (b) of the proposed AI regulation, albeit with view to physical or psychological harm, not consumer harm. Still, the proposed Art. 5 (b) AIA has clearly made the shift from vulnerability as a state or vantage point to assess the fairness of a practice, to a constituting element of a practice that is considered unfair, even unacceptable.

For consumer law in general, and UCP in particular, our analysis suggests that Article 5 (3) UCP is not the right frame to help us identify unfairness in the digital marketplace. The current definition of vulnerability would have to be considerably stretched so as to cover our conceptualization of digital vulnerability.[21] Article 5 (3) is designed as an exception to the rule. The benchmark is the average consumer. Integrating into Article 5 (3) architectural and relational vulnerability would interfere with the overall design of the UCPD and would reverse the relationship between the average and the consumer. Whilst it could not be excluded that courts might be prepared to go down that way, it seems legally and politically correct to underline the policy shift by clarifying the definition of vulnerability at least with regard to the digital economy. The UDCP as it stands is not able to guarantee that consumers are treated fairly and declare unlawful the abuse of institutional and structural advantages that some firms have vis-à-vis the vulnerable consumer. A revision of the UCPD is therefore needed. In whatever wording might be proposed, discussed, and finally agreed upon, the term "manipulation" has to be avoided. Manipulation requires per

[20] See also Art. L-122–8-L-122–10 French Code de la Consommation (*abus de faiblesse*) which defines abuse of vulnerability as an unfair commercial practice.

[21] For such an attempt, see Hacker (2021).

definitionem intent. Calling for intent as a precondition of unfairness would, however, lead in the wrong direction. What matters is not intent but the architecture, the design, and not what kind of strategies the designer pursues. Overall it would turn the clock back to the beginning of exercising control over commercial practices. It took nearly a century to free the control of commercial practices from all sorts of negligence and to focus just on the potential effects, independent of any commercial intentions.

In the search for an appropriate solution, it is worth exploring potential synergies with the GDPR. As Malgieri and Niklas have pointed out, the potential of data-driven commercial practices and digital choice architectures to exploit dispositional vulnerabilities should also play a role in data protection impact assessments and privacy by design. Both are elements of professional diligence that could then, again, inform interpretation of Article 5 (1) UCP. More generally, one could argue that the act of creating digital dependencies and asymmetrical (power) relationships and the resulting influence over autonomous choices also creates new professional duties and obligations of professional diligence in the sense of Article 5 (1) and (2) UCP.[22]Our analysis can also provide the starting point for the re-interpretation of concepts such as undue influence under Art. 9 of the UCP in the light of digital market practices.[23]

The implications of a new conception of consumer vulnerability go beyond the need to rethink protection of the individual consumer. So far, under the (neo)-liberal market model, large commercial tech platforms have enjoyed ample room to shape the digital marketplace. Within the confines of the GDPR and competition law, they were essentially left free to build digital choice architectures and a flourishing app economy. The underlying premise was that the laissez-faire approach in a prospering digital marketplace favours the average consumer, who—empowered through choice and information—will maximize their welfare. The role of consumer and data protection law in that context is to further empower the consumer and help them play an active role in the marketplace. The reality, as we demonstrated, makes the "average consumer" an unrealistic prototype. Digital marketplaces are characterized by structural power imbalances and choice architectures that are designed for exploiting individual differences and biases. Viewing these developments from a more universal vulnerability perspective teaches us that attempts at empowering users vis-à-vis digital platforms are futile as long as regulators do not also tackle the structural power imbalances and inequalities that manifest themselves in the architectures they create. And because these imbalances are structural as well as relational, so must be the solutions. For example, providing users with more information about the parameters used to decide why they are targeted with certain messages (the solution suggested by Art. 24 draft DSA) may contribute to their enlightenment, but it is difficult to see how this information can contribute to removing those sources of structural imbalance, particularly in situations in which, as we describe, data-driven strategies are used to create relational dependencies or digital situational monopolies. Changing the defaults, opening up systems, giving consumers agency to influence decision paths, fighting lock-ins, abolishing data monopolies—in short, addressing vulnerability and bringing fairness into the digital market place is not simply a question of empowering consumers, but of changing digital markets.

Once we understand that digital technologies can be used to exploit vulnerabilities for profit, and thereby render potentially each of us vulnerable but also change the very

[22] Spindler and Seidel (2018), arguing in favour of special fiduciary obligations, and other positive obligations (based on ethics), due diligence.

[23] For a more extensive analysis of these suggestions, see Helberger et al., 2021 and Sax 2021b.

conditions of fair competition in digital markets, another important question is whether there are certain data-driven practices that are simply unacceptable in a digital market place and therefore should always be considered unfair. This is the approach that the AI regulation took, but also the UCPD contains an Annex of listed practices that are always considered unfair. Possible blacklisted commercial digital practices to add to the annex could be, e.g., the use of psychographic profiles or other optimisation-based approaches to a similar effect to exercise emotional or psychological pressure with the aim of selling products or services causing a transactional decision; the use of personal data which the trader knows or must know was obtained unlawfully for any digital commercial practice; the use of data-driven or optimialisation strategies that actively discourage users from exercising their right to data portability or switching to other services, or the use of psychographic profiles or similar optimisation based approaches to exercise emotional or psychological pressure with the sole goal of selling products.[24]

The Consumer as Societal not as Market Actor

As a final observation, so far, the focus of our analysis has been very much on consumer law and the impact of certain digital market practices on consumers' economic decisions. It is worth mentioning that, in the digital society, the distinction between the consumer as economic actor and the citizen as social actor is further eroded (Scammell, 2000). The data that exists about us, as consumers, can be used to take (automated) decisions that affect us in different areas of our life, including politics and work. Consumption-related data are used to identify target groups for political campaigns, and data collected about the way people live their lives, such as data from fitness and lifestyle apps or social media, or how they inform themselves (data from media usage) are combined in unprecedented ways to be used outside the commercial realm as well, to influence elections, screen employees, and decide about insurance and social benefits. Governments combine "citizen data" with consumption data (for instance, in the field of credit scoring) (Citron & Pasquale, 2014) to engage in new forms of data-driven governance and public service provision (Dencik et al., 2019). In all these activities, governments often rely on the services of (large) commercial parties, often the same parties that are the main drivers behind commercial profiling and targeting strategies (Van Dijck et al., 2018). Ultimately, all these practices can also determine who gets access to which commercial/public services at what price, and who is refused access or is provided with access on less favourable conditions (Barocas & Selbst, 2016; Fisman & Luca, 2016).

Consumer law, with its current focus on economic decision-making, is little prepared to deal with the broader societal implications of consumer vulnerability in other aspects of social life. Broadly, the same is true for data protection law, which very much focuses on concrete acts of data processing in individual cases, and the rights and concerns of individual users vis-à-vis digital market practices. Partly this is a result of the way the competencies between the EU and Member States are distributed. The EU is granted powers to regulate the market and adopt consumer policies. The EU, however, has no power to regulate the society. This, if at all, is left to the Member States. Consumer policy is being understood first and foremost as

[24] See also EPDS (2021).

a tool to complete the internal market. This is reflected in the rather narrow definition of the consumer in EU law. The failure to address the more societal implications of consumer vulnerability is the result of a gap in the European legal framework—a gap that needs addressing. Put to the extreme it means to question whether the EU has the competence and therewith the legitimacy to shape a digital European society through the backdoor of the internal market competence in Art. 114 TFEU.

Acknowledgements We would like to thank Kasper Drazewski, Agustin Reyna, Ursula Pachl, Vanessa Mak, Christiane Wendehorst, Philipp Hacker, Michael Veale, Finn Myrstad, Gerald Spindler, Peter Rott, Ryan Calo and the participants of the European Consumer Protection 2.0 Online Feedback Workshop for their comments and inspiration. All mistakes and omissions are entirely those of the authors. This article is based in parts on a report that the authors wrote, commissioned by BEUC: N. Helberger, O. Lynskey, H.-W. Micklitz, P. Rott, M. Sax, J. Strycharz, EU CONSUMER PROTECTION 2.0. Structural asymmetries in digital consumer markets, Brussels, 2021, online available at https://www.beuc.eu/publications/beuc-x-2021-018_eu_consumer_protection.0_0.pdf.

Funding The research for this article has in parts be funded by a research project for the European Consumer Organisation BEUC, under the CONSUMER PROTECTION 2.0 project. All opinions and ideas are entirely those of the authors.

Data availability We have only used publicly available resources in the form of public reports and policy documents, journal publications and books.

Code Availability Not applicable.

Declarations

Conflict of Interest/Competing Interests The authors declare no competing interests.

References

Albertson Fineman, M. (2008). The vulnerable subject: Anchoring equality in the human condition. *Yale Journal of Law & Feminism, 20*, 1–24.

Anderson, J. H. (2014). Autonomy and vulnerability entwined. In C. Mackenzie, W. Rogers, & S. Dodds (Eds.), *Vulnerability: New Essays in Ethics and Feminist Philosophy* (pp. 134–161). Oxford University Press.

Baier, A. (1986). Trust and antitrust. *Ethics, 96*(2), 231–260.

Baker, S. M., Gentry, W. J., & Rittenburg, T. L. (2005). Building an understanding of the domain of consumer vulnerability. *Journal of Macromarketing, 25*(2), 128–139.

Baker, T., & Siegelmann, P. (2014). Behavioral economics and insurance law: the importance of equilibrium analysis. In D. Teichman & E. Zamir (Eds.), *Oxford Handbook of Behavioral Economics and the Law*

Barocas, S., & Selbst, A. D. (2016). Big data's disparate impact. *California Law Review, 104*(3), 671–732.

Berg, I. (2015). Consumer vulnerability: Are older people more vulnerable as consumers than others? *International Journal of Consumer Studies, 39*(4), 284–293.

Bol, N., Dienlin, T., Kruikemeier, S., Sax, M., Boerman, S.C., Strycharz, J., & de Vreese, C.H. (2018). Understanding the effects of personalization as a privacy calculus: Analyzing self-disclosure across health, news, and commerce contexts. *Journal of Computer-Mediated Communication*, 23(6), 370–388.

Burkell, J., & Regan, P. M. (2019). Voter preference, voter manipulation, voter analytics: Policy options for less surveillance and more autonomy. *Internet Policy Review, 8*(4), 1–24.

Calo, R. (2013). Digital market manipulation. *George Washington Law Review, 82*(4), 995–1051.

Calo, R. (2017). Privacy, vulnerability, and affordances. *DePaul Law Review, 66*(2), 591–604.

Cara, C. (2019). Dark pattern in the media: A systematic review. *Network Intelligence Studies, 7*(14), 105–113.

Cartwright, P. (2015). Understanding and protecting vulnerable financial consumers. *Journal of Consumer Policy, 38*, 119–138.

Chapman, A., & Carbonetti, B. (2011). Human rights protections for vulnerable and disadvantaged groups: The contributions of the un committee on economic, social and cultural rights. *Human Rights Quarterly, 33*, 682–732.
Chivukula, S. S., Watkins, C., McKay, L., & Gray, C. M. (2019). "Nothing comes before profit" asshole design in the wild. *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*, 1–6.
Citron, D. K., & Pasquale, F. (2014). The scored society: Due process for automated predictions. *Washington Law Review, 89*(1), 1–34.
Cole, A. (2016). All of us are vulnerable, but some are more vulnerable than others: The political ambiguity of vulnerability studies, an ambivalent critique. *Critical Horizons, 17*(2), 260–277.
Cooper, F. R. (2015). Always already suspect: Revising vulnerability theory. *N.C. L. Rev., 93*, 1339–1379.
Cox, K. (2020, August 25). Unredacted suit shows Google's own engineers confused by privacy settings. *ArsTechnica*. https://arstechnica.com/tech-policy/2020/08/unredacted-suit-shows-googles-own-engineers-confused-by-privacy-settings/. Accessed 20 December 2021.
Craig Smith, N., & Cooper-Martin, E. (1997). Ethics and target marketing: The role of product harm and consumer vulnerability. *Journal of Marketing, 61*(3), 1–20.
Crawford, R. (2006). Health as a meaningful social practice. *Health, 10*(4), 401–420.
Dencik, L., Hintz, A., Redden, J., & Treré, E. (2019). Exploring data justice: Conceptions, applications and directions. *Information, Communication & Society, 22*(7), 873–881.
van Dijck, J., Poell, T., & de Waal, M. (2018). *The platform society: Public values in a connective world*. Oxford University Press.
Duivenvoorde, B. (2013). The protection of vulnerable consumers under the unfair commercial practices directive. *Journal of European Consumer and Market Law, 2*(2), 69–79.
European Commission. (2016). Understanding consumer vulnerability in the EU's key markets. Factsheet, Brussels. https://ec.europa.eu/info/sites/info/files/consumer-vulnerability-factsheet_en.pdf. Accessed 10 June 2021.
Eyal, N. (2014). *Hooked: How to build habit-forming products*. Portfolio/Penguin.
Fisman, R., & Luca, M. (2016). Fixing discrimination in online marketplaces. *Harvard Business Review, 94*(12), 88–95.
Forbrukerrådet. (2018). *Deceived by design: How tech companies use dark patterns to discourage us from exercising our rights to privacy*. Report. https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf. Accessed 21 June 2021.
Gürses, S., & Van Hoboken, J. (2018). Privacy after the agile turn. In E. Selinger, J. Polonetsky, & O. Tene (Eds.), *Cambridge Handbook of Consumer Policy* (pp. 579–601). Cambridge University Press.
Hacker, Ph. (2021) *Manipulation by algorithms. Exploring the triangle of unfair commercial practice, data protection, and privacy law*. European Law Journal (Forthcoming)
Hardin, R. (2002). *Trust and trustworthiness*. Russell Sage Foundation.
Helberger, N., Lynskey, O., Micklitz, H.-W., Rott, P., Sax, M., Strycharz, J. (2021). EU consumer protection 2.0. Structural asymmetries in digital consumer markets, Brussels, 2021. https://www.beuc.eu/publications/beuc-x-2021-018_eu_consumer_protection.0_0.pdf. Accessed 21 June 2021.
Helberger, N. (2016). Profiling and targeting consumers in the internet of things – A new challenge for consumer law. In R. Schulze & D. Staudenmayer (Eds.), *Digital revolution: Challenges for contract law in practice* (pp. 135–162). Nomos.
Helmond, A., Nieborg, D. B., & Van der Vlist, F. N. (2019). Facebook's evolution: Development of a platform-as-infrastructure. *Internet Histories, 3*(2), 123–146.
Hill, R. P., & Sharma, E. (2020). Consumer vulnerability. *Journal of Consumer Psychology, 30*(3), 551–570.
Howells, G., Twigg-Flesner, C., & Wilhelmsson, T. (2018). *Rethinking EU consumer law*. Routledge.
Kaptein, M., Markopoulos, P., De Ruyter, B., & Aarts, E. (2015). Personalizing persuasive technologies: Explicit and implicit personalization using persuasion profiles. *International Journal of Human-Computer Studies, 77*, 38–51.
Laux, J., Wachter, S., & Mittelstadt, B. (2021). Neutralizing online behavioural advertising: Algorithmic targeting with market power as an unfair commercial practice. *Common Market Law Review, 58*(3), 719–750.
Leczykiewicz, D., & Weatherill, S. (Eds.) (2016). *The image of the consumer in EU law: Legislation, free movement and competition law*. Bloomsbury Publishing.
Lele, M. (2007). *Monopoly rules. How to find capture and control the world's most lucrative markets in any business*. Kogan Page Ltd.

London Economics, VVA Consulting, & Ipsos Mori consortium (2016). *Consumer vulnerability across key markets in the european union.* Study for the European Commission, DG Justice and Consumers, Brussels. https://ec.europa.eu/info/sites/info/files/consumers-approved-report_en.pdf. Accessed 10 June 2021.

Luna, F. (2009). Elucidating the concept of vulnerability: Layers not labels. *International Journal of Feminist Approaches to Bioethics, 2*(1), 121–139.

Lupton, D. (2013). Quantifying the body: Monitoring and measuring health in the age of mhealth technologies. *Critical Public Health, 23*(4), 393–403.

Mackenzie, C., Rogers, W., & Dodds, S. (2014). Introduction: What is vulnerability, and why does it matter for moral theory? In C. Mackenzie, W. Rogers, & S. Dodds (Eds.), *Vulnerability: New Essays in Ethics and Feminist Philosophy* (pp. 1–29). Oxford University Press.

Malgieri, G., & Niklas, J. (2020). Vulnerable data subjects. *Computer Law & Security Review, 37*, 105415.

Mathur, A., Acar, G., Friedman, M.J., Lucherini, E., Mayer, J., Chetty, M., & Narayanan, A. (2019). Dark patterns at scale: Findings from a crawl of 11k shopping websites. *Proceedings of the ACM on Human-Computer Interaction, 3* (CSCW). https://doi.org/10.1145/3359183. Accessed 20 December 2021.

Micklitz, H.-G., & Namyslowska, M. (2020). Münchener Kommentar Zum Lauterkeitsrecht, Art. 8 Rdnr. 22.

Nickel, P. J. (2015). Designing for the value of Trust. In J. van der Hoven, P. E. Vermaas, & I. Van der Poel (Eds.), *Handbook of Ethics, Values, and Technological Design* (pp. 551–567). Springer.

Peroni, L., & Timmers, A. (2013). Vulnerable groups: The promise of an emerging concept in European human rights convention law. *International Journal of Constitutional Law, 11*(4), 1056–1085.

Reich, N. (2016). Vulnerable consumers in EU law. In D. Leczykiewicz & S. Weatherill (Eds.), *The Image of the Consumer in EU Law: Legislation, Free Movement and Competition Law*. Bloomsbury Publishing.

Roessler, B. (2005). *The value of privacy*. Polity Press.

Rogers, W., Mackenzie, C., & Dodds, S. (2012). Why bioethics needs a concept of vulnerability. *International Journal of Feminist Approaches to Bioethics, 5*(2), 11–38.

Sax, M. (2021a). Optimization of what? For-profit health apps as manipulative digital environments. *Ethics and Information Technology*.

Sax, M. (2021b). *Between empowerment and manipulation: The ethics and regulation of for-profit health apps*. PhD dissertation, University of Amsterdam.

Scammell, M. (2000). The internet and civic engagement: The age of the citizen-consumer. *Political Communication, 17*(4), 351–355.

Spindler, G. and Seidel, A. (2018). Die zivilrechtlichen Konsequenzen von Big Data und Aufklärungspflichten. *NJW*, 2153–2157.

Stanovich, K. E., West, R. F., & Toplak, M. E. (2016). *The rationality quotient: Towards a test of rational thinking*. MIT Press.

Strycharz, J., van Noort, G., Smit, E., & Helberger, N. (2019). Protective behavior against personalized ads: Motivation to turn personalization off. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *13*(2). https://doi.org/10.5817/CP2019-2-1

Susser, D., Roessler, B., & Nissenbaum, H. (2019a). Technology, autonomy, manipulation. *Internet Policy Review*, *8*(2).

Susser, D., Roessler, B., & Nissenbaum, H. (2019b). Online Manipulation: Hidden influences in a digital world. *Georgetown Law Technology Review, 4*(1), 1–45.

Thaler, R. H., & Sunstein, C. R. (2008). *Nudge: Improving decisions about health, wealth, and happiness*. Yale University Press.

Trebilcock, M. (1993). *The limits of freedom of contract*. Harvard University Press.

Wiesemann, C. (2017). On the interrelationship of vulnerability and trust. In C. Straehle (Ed.), *Vulnerability, Autonomy and Applied Ethics* (pp. 157–170). Routledge.