Digital Vulnerability as a Power Relation: Hyper- and Hypo-Autonomy and Why Thick Privacy Matters

Irina Domurath

A. Introduction

Vulnerability has been a topic in EU Law at least since the adoption of the Unfair Commercial Practices Directive (EC) 2005/29 (hereinafter UCPD).[1] The point that is repeatedly being made is that there are different risk factors that can lead to consumer vulnerability in certain fields.[2] There is widespread agreement among EU consumer law scholars that the protective standard of the reasonably circumspect consumer in EU Law is a normative standard that has not much to do with reality and, more importantly, does not adequately protect European consumers. Nevertheless, the reasonably-circumspect-consumer standard has remained in place. Nowadays, there is a renewed interest in the concept of vulnerability, converging again to a remarkable agreement in EU consumer law scholarship that digital technologies have led to new vulnerabilities of consumers.[3] The very premise of this volume is that digital technologies create a new type of vulnerability: digital vulnerability.

1 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').

2 For example, Peter Cartwright, 'Understanding and Protecting Vulnerable Financial Consumers' [2015] Journal of Consumer Policy; Norbert Reich, 'Vulnerable Consumers in EU Law' in Dorota Lecykiewicz and Stephen Weatherill (eds), *The Images of the Consumer in EU Law: Legislation, Free Movement and Competition Law* (Hart Publishing 2016); Jan Trzaskowski, 'Is It Unfair to Mislead Vulnerable Consumers ?' 1, Irina Domurath, *Consumer Vulnerability and Welfare in Mortgage Contracts* (Hart Publishing 2017).

3 See for example Christine Riefa, *Protecting Vulnerable Consumers in the Digital Single Market*, 33 Eur. Bus. Law Rev. 607–634 (2022).

What has aided this scholarly agreement on 'digital vulnerability' is the ubiquity and opacity of data collection embedded in an almost casual (hardly debated) surveillance context. Surveillance - not in the traditional sense by states and public authorities - but also and especially by private companies whose very business models lies on the collection, analysis, and sale of consumer data has become extremely pervasive.[4] The political economy terms for this are 'surveillance capitalism' and 'informational capitalism'. The first refers to a new form of capitalism that aims to predict and modify human behaviour as a means to produce revenue and gain market control.[5] 'Information capitalism' describes the alignment of capitalism as a mode of production with informationalism (accumulation of knowledge and higher levels of complexity in information processing) as a mode of development,[6] where market actors use knowledge, culture, and networked information technologies in order to extract and appropriate surplus value.[7] This surplus value is created through personalized marketing algorithms, which are specifically designed to exploit consumer weaknesses. These systematic influences at the precise time an individual is irrational collapse any meaningful distinction between the rational, normatively average and vulnerable consumer.[8] They undermine any idea of standardized protection, including the taking-into-account of collateral damage for non-average-consumers.[9] In times of personalised marketing, the idea of an 'average' consumer is outdated.

Surveillance is made possible by large-scale privacy intrusions. New technologies have not only increased the extent of what is being monitored is (more permanent data) but have also made searching more efficient and cheaper, which increases the burden of monitoring; the limits of privacy

4 Frank Pasquale, Black Box Society - The Secret Algorithms that Control Money and Information (2015).

5 Shoshana Zuboff, 'Big Other: Surveillance Capitalism and the Prospects of an Information Civilization' (2015) 30 Journal of Information Technology 75.

6 Manuel Castells, *The Information Age Vol I: The Rise of the Network Society* (Blackwell Publishing 1996), 14–18.

7 Julie E Cohen, *Between Truth and Power - The Legal Constructions of Informational Capitalism* (Oxford University Press 2019), 5-6.

8 Ryan Calo, *Digital market manipulation*, 82 George Washington Law Rev. 995–1051 (2014), 1033.

9 Jan Trzaskowski, Your Privacy Is Important To Us! - Restoring Human Dignity in Data-Driven Marketing (2022).

are eroded.[10] In fact, data protection regimes are reflections of the idea that all individuals are 'vulnerable' to power balances created by digital technologies.[11]

Privacy is however neglected in the current conceptualizations of *digital vulnerability*. While discussions on the digital vulnerability of consumers have already brought about a thickened understanding of what digital vulnerability is and where it comes from, the concept of privacy is still a neglected and under-conceptualized component of the concept. This contribution aims to remedy this neglect and analyse the role of privacy – and also what type of privacy – for the concept of digital vulnerability. It brings together the discussions surrounding digital vulnerability and privacy with a view to connecting the two concepts. In this way, the hope is to enable further discussions in order to understand the impact of a lack of privacy on digital vulnerability.

In what follows, I will first outline the discussions on vulnerability in EU Law (B), including criticism to the way in which vulnerability is hitherto understood and the proposals for adopting the concept of digital vulnerability. I will characterize *digital vulnerability* as a power relation, in which the hypo-autonomy of consumers contrasts with the hyper-autonomy of structurally powerful companies. Then, I will turn to the idea of privacy (C), explain its intrinsic value, before contrasting the what I call thin understanding of privacy in EU Law with a thick understanding of privacy in the privacy literature. Finally, I will explain how the concept of digital vulnerability can benefit from incorporating a thick concept of privacy (D).

B. Vulnerability in EU Law

In this section, I will distinguish the concept of (general) vulnerability and the new concept of digital vulnerability. While the first is well-known in EU Law, the second is not yet part of the EU legal order even though pushes towards broader interpretations of the framework exist.

10 Lawrence Lessig, *The Architecture of Privacy: Remaking Privacy in Cyberspace*, 1 Vanderbilt J. Entertain. Technol. Law 56–65 (1999).

11 Calo, *supra* note 8.

I. Static, personal, exceptional

The concept of vulnerability is well known in EU consumer law. It describes a category of consumers, who are – according to Article 5 (3) UCPD - 'particularly vulnerable' to certain commercial practices 'because of their mental or physical infirmity, age or credulity in a way which the trader could reasonably be expected to foresee.' The concept of vulnerability serves to assess the (un)fairness of the commercial practice in question from the perspective of the average member of that vulnerable group. It does not lead to higher standards of information or more obligations of traders. Instead, it serves as a factor when assessing the unfairness of a commercial practices. Vulnerable consumers are the ones who are at a higher risk of experiencing negative outcomes in the market, have limited ability to maximise their well-being, have difficulty in accessing information, are less able to choose and buy, or are more susceptible to certain marketing practices.[12]

Otherwise, consumer law does not contain many references to vulnerability. For the digital sphere, the DSA works with a similar concept of vulnerability with regard to countering illegal hate speech on platforms. Recitals 62, 95, and 104 DSA mention 'vulnerable recipients of the service, such as minors.' Recital 94 DSA stipulates that assessments and mitigations of risk with regard to recommender systems need to elicit measures to 'prevent or minimise biases that lead to the discrimination of persons in vulnerable situations, in particular where such adjustment is in accordance with data protection law and when the information is personalised on the basis of special categories of personal data' of Article 9 GDPR.

In European technology and data law, the approach is very similar. Art 5 I lit b) AI Act prohibits AI systems that exploit the 'vulnerabilities of a specific group of persons due to their age, physical or mental disability'. Similarly to Art 5 (3) UCPD, it emphasizes the goal of materially distorting' the behaviour of a person pertaining to that group in a manner that causes or is likely to cause that person or another person physical or psychological harm.' Notably, Article 5 I AI Act moves away from using 'vulnerability' as a means to *assess* fairness to using it as a constituting element for a prohibition of technology. In the GDPR, the only mention of vulnerability

12 European Commission, Study on consumer vulnerability in key markets across the European Union (EACH/2013/CP/08), http://ec. europa.eu/consumers/consumer_evidence/market_studies/vulnerability/index_en.htm.

can be found in Recital 75, which refers to the 'personal data of vulnerable persons, in particular of children' as a category of data the processing of which poses a risk to the rights and freedoms of natural persons. According to Recital 38 GDPR, specific protection should apply where personal data of children is used for the purposes of marketing or profiling. In terms of legal consequences, only information-related rules can be found in the GDPR, see for example Article 40 II lit g) GDPR.

A few aspects stand out in these uses of *vulnerability*. It is regarded as an exception to the rule of non-vulnerable people. In consumer law, the reasonably circumspect consumer is the normative benchmark, whereas vulnerability is circumscribed to a special type of person. It refers to a specific group of people that is in need of special protection, arguably as opposed to other 'normal' people. What is more, the concept of vulnerability is a personal one. It is based on personal status or characteristics, usually relating to impaired cognitive capacity. Children and the elderly are considered vulnerable because their age is connected to cognitive limitations. Mental disability is another personal characteristic that is considered to lead to cognitive limitations. These limitations are the reason for applying more protective rules. *Vulnerability* is also a static concept: autonomy-impairment is considered to underlie all dealings of those individuals, which is the precise reason why there are afforded special and exceptional protection. This also holds true for the more general prohibitions in the AI Act. For those reasons, the static and personalistic approach to vulnerability in EU Law has been subject to criticism and ample discussion.[13]

13 Geraint G Howells, HW Micklitz and Thomas Wilhelmsson, *European Fair Trading Law - The Unfair Commercial Practices Directive* (Ashgate 2006), 111-117. This dichotomy has been criticized in the literature, for example in Geraint Howells, Christian Twigg-Flesner and Thomas Wilhelmsson, *Rethinking EU Consumer Law* (Routledge 2018); but especially so in the field of financial services, see for example: Peter Cartwright, 'The Vulnerable Consumer of Financial Services: Law, Policy and Regulation' 1; Peter Cartwright, 'Understanding and Protecting Vulnerable Financial Consumers' [2015] Journal of Consumer Policy; Lorna Fox O'Mahony, Christian Twigg-Flesner and Folarin Akinbami, 'Conceptualizing the Consumer of Financial Services: A New Approach?' (2015) 38 Journal of Consumer Policy 111; Irina Domurath, *Consumer Vulnerability and Welfare in Mortgage Contracts* (Hart Publishing 2017); Irina Domurath, 'The Case for Vulnerability as the Normative Standard in European Consumer Credit and Mortgage Law – An Inquiry into the Paradigms of Consumer Law' (2013) 3 Journal of European Consumer and Market Law 124.

In other words: consumer vulnerability is the impaired capacity to act on the market in accordance with one's self-interest.[14] It finds its basis in the idea of impaired autonomy. While the reasonably circumspect, fully autonomous consumer in EU Law benefits from freedom of contract and negotiation or unfairness control of contracts of adhesion, the less autonomous ones are protected (in specific) instances.[15] Article 5 (3) UCPD concerning the danger of manipulation and Art 5 (1) lit b) Proposed AI Act are examples of this approach. Autonomy is understood as freedom from manipulation. In the UCPD, the reference point is young age, physical or mental disability, or incredulity, as examples of diminished autonomy, which make the people concerned vulnerable to the distortion of their economic behaviour. Because of young age or some other personal impairment, there is an increased risk of entering into agreements that distort their behaviour. In any case, impaired personal autonomy leads to vulnerability, namely the subjection to manipulation of economic behaviour.

II. Digital vulnerability

Consumer research argues that the reasonable circumspect consumer as a standard for protection under EU Law is obsolete in the digital sphere because digital vulnerability affects everyone. It is universal. This reverses the current vulnerable-not vulnerable dichotomy.[16] Consequentially, proponents of the adoption of a *digital vulnerability* concept argue for a regulatory shift and the reversal of the current vulnerability-paradigm, especially in unfair commercial practices law. Instead of seeing the vulnerable consumer as an exception to the normative benchmark of the reasonably circumspect consumer, they acknowledge that all consumers are – albeit in different degrees – vulnerable to exploitative practices. This goes beyond the proposal of the EU Commission to modulate the average-consumer-test in the digital sphere, even to the perspective of one single person, if the

14 Calo, *supra* note 98, 1034.

15 Howells, Twigg-Flesner, and Wilhelmsson, *supra* note 13, 27 et sub.

16 Natali Helberger et al., *EU Consumer Protection 2.0: Structural asymmetries in digital consumer markets*, EU Consumer Protection 2.0. Structural asymmetries in digital consumer markets - A joint report from research conducted under the EUCP2.0 project (2021), at 5; Federico Galli, Algorithmic Marketing and EU Law on Unfair Commercial Practices (2022), 205.

practice is highly personalized.[17] With this approach, the Commission does not give the average-vulnerable dichotomy, but merely tweaks the vulnerability-assessment.

Research on digital vulnerability draws on the concept of intersectionality,[18] attempting at a more multi-faceted and less static idea of vulnerability. Definitions of digital vulnerability now converge towards an understanding that emphasizes structural asymmetries in the *relation* between actors rather than personal characteristics of *individuals*. Two characteristics of the concept distinguish it from the current static and personalistic understanding of vulnerability in EU Law: it is relational and layered.

1. Influence of intersectionality: vulnerability as relational

The probably most influential contemporary conceptualizations of vulnerability are the ones by feminist scholars Fineman and Luna. According to Fineman, vulnerability derives from our embodied humanity that carries with it the ever-present possibility of harm.[19] Because of different economic and institutional positions and relationships, individual vulnerability occurs at a range in magnitude and potential. Fineman's universal, human vulnerability is experienced uniquely by each individual and is greatly influenced by the quality and quantity of the resources we possess or can command.[20] Luna conceptualizes Fineman's idea of the individual experiences of an inherently human vulnerability with an intersectional perspective.[21] She argues that vulnerability is layered and relational.[22] She observes that depending on the specific circumstances – whether political, economic, social, cultural - people can acquire layers of vulnerability. Vulnerability is relational, because people are not vulnerable per se, but are

17 EU Commission Notice, Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market (2021/C 526/01), 100.

18 The concept was introduced by Kimberle Crenshaw, *Demarginalizing the Intersection of Race and Sex: A Black Feminist Critique of Antidiscrimination Doctrine, Feminist Theory and Antiracist Politics*, 1989 Fem. Leg. Theor. 139–167 (1989).

19 Martha Albertson Fineman, 'The Vulnerable Subject: Anchoring Equality in the Human Condition' (2008) 20 Yale Journal of Law and Feminism 1, 9.

20 ibid., 10.

21 Crenshaw, *supra* note 18.

22 Florencia Luna, 'Elucidating the Concept of Vulnerability: Layers Not Labels' (2009) 2 International Journal of Feminist Approaches to Bioethics 121, 128-129.

rather *made* vulnerable. Varied and changing circumstances render individuals vulnerable.[23] Everybody can be vulnerable in certain circumstances and the circumstances do not necessarily occur naturally but can also be engineered and controlled. Vulnerability conceptualized as a layered and relational universal human experience has moved the discussions beyond binary dichotomies where vulnerability is or is not situated in static, personal characteristics leading to stigmatization and discrimination.

2. Two definitions

Helberger et al put forward a concept of digital vulnerability that is based on a refined, universalist idea of Fineman that vulnerability is an ever-present possibility of harm or misfortune. Fine-tuning the concept to the digital age, they define digital vulnerability as a universal state of defencelessness and susceptibility to power imbalances' in the digital sphere, characterized by automation of commerce, datafied consumer-seller relationships and the architecture of the digital marketplace.[24] They argue that digital vulnerability needs to be a dynamic concept that responds to the adaptive persuasive systems employed in digital marketing.[25] Following Rogers et al,[26] they distinguish between inherent (Fineman's) and situational sources of vulnerability on the one hand, and dispositional (potential) and occurrent (manifest) states of vulnerability.[27] Fitting also with, however not specifically referring to, Luna's conceptualization, they emphasize that digital vulnerability is both architectural, meaning the – not accidental - product of digital consumer markets as well as relational - manifest in the ongoing asymmetrical relation between consumers and service providers.

Galli, in turn, adopts more specifically Luna's idea of layers. For him, digital vulnerability – understood as a potential negative impact on consumer wellbeing in the digital sphere -[28] in the context of algorithmic marketing consists of four layers, which can interact, albeit not necessarily. The foundational layer of all digital vulnerability, for Galli, is the architecture, the 'objective way of being', of algorithmic marketing that makes

23 ibid.
24 Helberger et al., *supra* note 16, 5.
25 Helberger et al., *supra* note 16, at 183.
26 Wendy Rogers, Catriona MacKenzie & Susan Dodds, *Why bioethics needs a concept of vulnerability*, 5 Int. J. Fem. Approaches Bioeth. 11–38 (2012).
27 Helberger et al., *supra* note 16, 184-185.
28 Galli, *supra* note 16, 192.

everybody vulnerable who is active on the digital market. The second layer consists of privacy as the increasing function of autonomy vis-à-vis sellers. Third, situational vulnerabilities can exist that relate to personal and consumption-relation situations and patterns, such as consumption intervals or behavioural limitations in decision-making. The upper layer consists of personal characteristics, such as age or mental conditions. In this conceptualization, the architectural layer that concerns all consumers is the one that always remains, even if the other layers are not present in any given case.

Both accounts understand vulnerability as a more dynamic and universal situation than is acknowledged in current EU Law. They put emphasis on the architectural nature of vulnerability: Helberger et al stress that vulnerability is the necessary, and even intentional, product of the choice-architecture on digital consumer markets,[29] while Galli highlights that the way in which algorithmic marketing is made (architecture) 'cascades through' all other layers of vulnerability.[30]

3. Hyper- and hypo-autonomy: the power relation in digital vulnerability

The two ideas of digital vulnerability fit well with a definition of vulnerability I proposed elsewhere: the exposure to risk and the lack of resilience to avoid harm from the materialization of those risks.[31] Updated for the digital sphere, the exposure to risks come from the design of commercial practices on digital markets (what Helberger et al and Galli call 'architecture'), whereas the lack of resilience describes the lack of power of consumers vis-à-vis transnational companies. This relation can be understood as a relation of power in which the actors have different degrees of autonomy: companies have increased (hyper-)autonomy, whereas the consumers have decreased (hypo-)autonomy. Understanding vulnerability as a power relation, highlights the shortcomings of the EU Law approach which focuses solely on the hypo-autonomy of the consumer side, while neglecting the hyper-autonomy of companies.

29 Helberger et al., *supra* note 16, 187; also Galli, *supra* note 16, 203.
30 Galli, ibid, 204.
31 Put forward for financial services, see Domurath, *supra* note 2, 64.

a) Autonomy

While definitions of autonomy are numerous – oscillating in between liberty, self-rule, or free will,[32] I consider it useful to use Christman's conceptual distinction between individualistic and relational understandings of autonomy.[33] Both are concerned with the conditions for some kind of authenticity of will and action. I understand the discussions to be concerned with the conditions in which self-determination and authenticity can come about. Some authors put emphasis on the governance in one's actions and life by values, principles, or reflections that are truly their own as opposed to being guided by external or even manipulative forces.[34] Authenticity refers to a 'wholeheartedness' or 'truthfulness' connected to free will. It 'concerns the independence and authenticity of the desires (values, emotions, etc.) that move one to act in the first place.'[35] In this view, autonomy describes the possibility of being directed by considerations, desires, conditions, and characteristics that are not externally imposed, but which are part of one's authentic self.[36] The individualist approach emphasizes self-rule, authenticity (genuineness of values), and competence to relational thought. This does not necessarily mean that individuals need to be able to reflect on their subjective values in complete isolation from cultural and social context. In fact, Kymlicka argues that it is enough for a liberal notion of autonomy, 'piecemeal reflection' to enable individuals to engage critically with value formation.[37]

32 See for an exemplary overview of definitions, Gerald Dworkin, *The Theory and Practice of Autonomy* (Cambridge University Press 1988), 5; also: Andrew Sneddon, autonomy (Bloomsbury Academic, 2013), 2 ff.

33 John Christman, *Autonomy in Moral and Political Philosophy*, The Stanford Encyclopedia of Philosophy (2020), https://plato.stanford.edu/archives/fall2020/entries/autonomy-moral/.

34 John Christman, *Autonomy*, *in* The Oxford Handbook of the History of Ethics 691–709 (2013).

35 ibid. To what extent authenticity is required for autonomy, is highly debated. See, negatively: Sneddon, *supra* note 31, 7.

36 Christman, *supra* note 34. This view needs to be distinguished from moral philosophical viewpoints dealing with the responsibilities and obligations flowing from autonomy.

37 He does so within his argument that group rights are not logically opposed or in detriment to individual autonomy, see: Will Kymlicka, Multicultural Citizenship (1995).

Relational or social views on autonomy emphasize the specific environment in which self-governing agents find themselves. It is argued that the self has basic values which are filtered through social relationships. For example, in feminist studies, Mackenzie and Stoljar argue that personal and social relationships have constituent power over the development of people's identities and that the alienation following detachment from those relationships would undermine autonomy.[38] Thus, they shed light on the social conditions that can further or limits the ability to act effectively upon one's own values, emphasizing that the creation and exercise of autonomy is shaped by interpersonal relations and interactions. Social practices thus become constitutive elements of autonomy.[39] There is also a view that Christman calls 'procedural', which demands to look at the procedures by which individuals come to identify their values as their own in order to determine authenticity of value. This view is concerned with guaranteeing neutrality towards all conceptions of value.[40]

The way I see it, the disagreement between those views consists in the degrees of detachment from as well as the definition of 'external factors' for the constitution of autonomy. While the more individualistic view seems to operate on a rather sharp distinction between what is internal and external, the more relational or social view accepts that internal and external factors for autonomy cannot be neatly separated and that the boundaries between the two are porous. What they have in common is a shared concern for the conditions in which personal (maybe even authentic) values can emerge, flourish, and be owned. The conditions for the capacity for self-rule are the main concern, with debates surrounding the issue of to what extent self-rule can be socially mediated.

b) Hypo-autonomy: lack of power of consumers

This puts emphasis on the question of whether and to what extent the conditions for self-rule and determination actually exist in the digital sphere,

38 C Mackenzie and N (eds) Stoljar, *Relational Autonomy: Feminist Perspectives on Autonomy, Agency, and the Social Self* (Oxford University Press 2000).

39 For an overview of the discussions, see Christman, *supra* note 34.

40 Dworkin does not use the concept of autonomy, but it is clearly underlying his idea of liberalism as concerned with equality, see Ronald Dworkin, 'Liberalism' in Stuart Hampshire (ed), *Public and Private Morality* (Cambridge University Press 1978), 115.

namely to what extent consumers are actually autonomous. Different issues should be conceptually distinguished here.

We know that all consumers are considered to be in an inferior bargaining position due to information asymmetries and standard term contracts.[41] These are the very reasons for the regulation of consumer markets in the first place. Here, consumer autonomy is supposed to be intact, because the consumers have had time to reflect upon their values and choices as consumers, but the external condition of non-negotiable terms impede them to act in accordance with those choices. As a consequence, consumers are stuck with contracts terms that they did not choose. The regulatory approach here is to allow for the control of unfairness,[42] in order to ensure that the consumer who is left with no choice is at least not left with an obligation to adhere to unfair terms. Consumer autonomy is established ex post.[43]

There are however behavioural issues, which impede rational consumer decision-making, thereby leading to market failures.[44] There is a normative relation between autonomy and rationality. At times, consumer autonomy can be intact, but external conditions impede individuals from acting rationally in conformity with their self-determination and autonomously formed will. For example, consumers might not be able to deal with situations of pressure such as doorstep selling and, as a consequence, end up buying products and services that they did not want in the first place. Again, EU Law steps in.[45] Similarly, people affected by a serious illness could be considered vulnerable to particular advertising that misleadingly

41 Friedrich Kessler, *Contracts of Adhesion - Some Thoughts About Freedom of Contract*, Columbia Law Rev. 629–642 (1943).

42 Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, OJ L 95, 21.4.1993, 29–34.

43 See doctoral thesis of Candida Leone, on file with author.

44 See the 2011 Special Issue in the Journal of Consumer Policy as well as the introduction thereto: Hans-W. Micklitz, Lucia A Reisch & Kornelia Hagen, *An Introduction to the Special Issue on "Behavioural Economics, Consumer Policy, and Consumer Law,"* 34 J. Consum. Policy 271 (2011), http://proquest.umi.com/pqdlink?did=2436552091&Fmt=7&clientId=58117&RQT=309&VName=PQD.

45 Council Directive 85/577/EEC of 20 December 1985 to protect the consumer in respect of contracts negotiated away from business premises, OJ L 372, 31.12.1985, 31–33.

presents products as able to cure their illness,[46] precisely because – even though their autonomy is intact (including the wish to be cured), they are susceptible to a certain type of marketing that exploits their wish to be cured. This is precisely the approach of Article 5 (3) UCPD. In other instances, consumers do not always act rationally due to cognitive limitations. Here, autonomy could be considered impaired because preferences might be sup-optimal. This is the behavioural economics critique, which has, however not yet led to a change of regulatory approach.

In contrast, the concept of exceptional consumer vulnerability as currently included in the EU Law framework presupposes that vulnerable consumers are not autonomous due to their specific, personal characteristics such as age or mental infirmity. Those consumers are inhibited in their self-determination, because they are not able to develop autonomous will. For example, most legal orders restrict legal competence of minors. In addition, the UCPD, prohibits as unfair practices that exploit limited autonomy. The EU considered teenagers immature and credulous, which is why they can succumb to rogue marketing practices due to their lack of attention or reflection or risk-taking behaviour.[47] Therefore, the EU puts in place special protection measures in order to ensure that these consumers are protected from any possible negative consequences.

In the digital sphere, the autonomy of consumers is even more diminished: it is hypo-autonomy. This hypo-autonomy derives from the combination of mainly two issues: big data and the long-term character of consumer-business relations in the digital sphere. First, the increasing generation and accumulation of ever more data enables consumer data, combined with the use of algorithms and AI, into information usable for commercial purposes. The collected data can give insights into 'socio-demographic characteristics, such as age, gender or financial situation, as well as personal or psychological characteristics, such as interests, preferences, psychological profile and mood. This enables traders to learn more about consumers,

46 For example in an Italian case concerning 'slimming pills', see Autorità Garante della Concorrenza e del Mercato, Provvedimento n. 24607, PS6980 – *Xenalis Dimagranti*, ll.

47 European Commission, Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market, (2021/C 526/01), 36.

including about their vulnerabilities.'[48] With the possibility to infer increasingly fine-grained (and maybe even correct) consumer profiles from more and more collected data also come more possibilities to sell advertisements and products that are particularly tailored to exploit consumer biases and other vulnerabilities. Second, consumers' ongoing involvement in digital products and services make them increasingly susceptible to manipulation: 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'.[49] The more companies know about their customers, the more 'insidious' and subconscious their attempts of influence can become.

This is where the concept of digital vulnerability comes in. *Digital vulnerability* is more than just a situation or an 'unfortunate by-product' of economic activity in the digital sphere, but deliberately created,[50] sustained, and exploited for financial gain. It lies at the heart of capitalist logic that the systematically irrational behaviour of individuals will be exploited.[51] Engaging in 'nudging for profit' is following the economic incentive.[52] It is the very design of personalized products to respond to individual vulnerabilities. Nudging and discrimination as part of manipulation and exploitation are, thus, the problems most criticized in consumer research.[53] The critique puts emphasis on the effects of the 'industry's relentless search for experimental and creative digital marketing practices that seek to influence

48 European Commission, Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market, (2021/C 526/01), 36

49 Helberger et al., *supra* note 16, at 22. I do not agree, howevere, with Helbereger et al's claim that people move in and out of states of vulnerability. Especially with regard to algorithmic profiling, I think that the structuredness of the power relation with the company is so pervasive that 'digital vulnerability' is omnipresent and unflexible; or, at least, iindividuals move into stages of vulnerability more often than they move out of them.

50 Helberger and others (n 16), 19.

51 Jon D Hanson & Douglas A Kysar, *Taking Behavioralism Seriously: Some Problems of Market Manipulation*, 74 NYU Law Rev. 630–749 (1999), 635.

52 Calo, *supra* note 8,1001.

53 Philipp Hacker, 'Manipulation by Algorithms. Exploring the Triangle of Unfair Commercial Practice, Data Protection, and Privacy Law' [2021] European Law Journal 1; Calo, *supra* note 8; Tal Z Zarsky, 'Privacy and Manipulation in the Digital Age' (2019) 20 Theoretical Inquiries in Law 157; Karen Yeung, '"Hypernudge": Big Data as a Mode of Regulation by Design' (2017) 20 Information Communication and Society 118.

consumer behaviour'.[54] In this way, *digital vulnerability* also makes it clear that the hypo-autonomy of individuals is matched by increased autonomy of companies that create and exploit hypo-autonomy of individuals.

c) Hyper-autonomy: structural power of companies

The architectural aspect of vulnerability relates to the design of markets that brings about consumer vulnerability. In Helberger et al.'s view, the architectural character describes the fact that vulnerability is the very product of digital consumer markets; this relates to a type of 'situational monopoly' deriving from reduced choice for consumers, unequal bargaining power, and including the power of electronic devices.[55] For Galli, the architectural *layer* of vulnerability is based on four features:[56] horizontal and aggregate effects of data collection that enable access to individual consumers beyond individual data collection;[57] customization based on statistical (not necessarily truthful) prediction; usage over time, and the power concentration on digital markets. Both understandings of vulnerability thus stress that the way in which digital markets are *designed to* work by the very companies that trade and sell on those markets is leading to a universal vulnerability. Whether this is new or whether the digital sphere has only accentuated or shed light on existing consumer vulnerabilities on other markets[58] is not relevant here. What matters is that the way digital markets are made to work has given rise to acknowledging a *structural* aspect of vulnerability, namely the way in which companies generate and maintain structural asymmetries vis-à-vis their customers.

Here, the concept of digital vulnerability reflects the idea of structural power as established in Political Economy. According to Strange's seminal

54 Helberger et al., *supra* note 16, 15.

55 Helberger et al., *supra* note 16, 187.

56 Galli, *supra* note 16, 201 ff.

57 In this vein also: Salomé Viljoen, *A Relational Theory of Data Governance*, Yale Law Journal, 573–654 (2020).

58 See, for example, arguments in favour of a more universal concept of vulnerability of consumer son financial markets: Peter Cartwright, *supra* note 3; David Capper, *Protection of the Vulnerable in Financial Transactions – What the Common Law Vitiating Factors Can Do For You*, *in* Unconscionability in European Private Financial Transations - Protecting the Vulnerable 166–183 (Mel Kenny, James Devenney, & Lorna Fox O Mahony eds., 2010); Domurath, *supra* note 3.

definition, structural power describes the capacity of actors to shape and determine the structure of the global political economy within with states, their political institutions, economic enterprises, and professionals have to operate.[59] In the consumer realm, consumer manipulation is now the characterizing feature of consumer markets as market outcomes are determined by the ability of companies to control information, present choices and shape the setting in which market transactions occur.[60] Structural power is more than the power to decide how things are to be done. It includes the power to shape the frameworks within which all economic actors - states, individuals, corporate enterprises - relate to each other and among each other.

For the digital sphere, structural power describes the ability of companies to control data and information flows, present choices and shape the very setting for digital market transactions. Digital platforms are points of entry for the creation of new forms of private power in surveillance,[61] shaping the conditions of market entry, the scope for disruption and contestation, as well as the sources and manifestations of economic power, thereby replacing and rematerializing markets, all according to their own agendas and private interests of business expansion based on the commodification of data.[62] Kapczynski describes this as the monopoly power over information and markets, creating winner-takes-it-all dynamics and price discrimination through tailored offers and contract terms.[63] This structural power is relational because it increases or diminishes if one party also determined the surrounding structure of the relationship.[64] The more power digital companies have the more the power of consumers to have influence on their relation with that company diminishes.

What emerges is a picture of companies as hyper-autonomous actors not only in terms of their actions as architects of a highly exploitative and

59 Susan Strange, *States and Markets* (Bloomsbury Academic 2015/1988), 27.

60 Foreseen 20 years ago by Hanson and Kysar, *supra* note 51, 635.

61 Julie E Cohen, *Between Truth and Power - The Legal Constructions of Informational Capitalism* (Oxford University Press 2019), 235. She relies largely on Castell's seminal definition and conceptualization of 'informational capitalism', see Manuel Castells, *Rise of the Network Society* (Wiley-Blackwell 2010), 17-18.

62 ibid., 42.

63 Amy Kapczynski, 'The Law of Informational Capitalism The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power Between Truth and Power: The Legal Constructions of Informational Capitalism', Yale Law Journal, 1460 (2020).

64 Strange, *supra* note 59, 27.

opaque digital environment but also as regards the capacity to build this basically ubiquitous architecture in a more or less unrestrictive way. Consumers are unable to meet this power, being hypo-autonomous themselves. There is no global legal framework that forces these 'architectural companies' to take into account any external (outside of company business strategy) constraints. Business secrets, including algorithms, are fiercely protected under national, international, and EU Law. In this way, companies are not just autonomous in the sense of being to operate their business as they seem fit: beyond this, they also make the markets on which they act.

III. Interim conclusion 1

The conceptualizations of *digital vulnerability* emphasize a new phenomenon on consumer markets. The emergence of new marketing techniques based on large-scale data collection.

These techniques do not only exploit existing vulnerabilities but also *make* consumers vulnerable. I argue that this can be adequately understood as a power relation, in which the structural power of companies to make agreements with consumers but also create and design the very markets for those agreements is a sort of hyper-autonomy that is not matched by the hypo-autonomy of consumers, expressed as a defenceless vis-à-vis those practices.

Digital vulnerability puts our attention on the structural aspects of vulnerability in the digital sphere, thus enabling policies that focus on the supply side of digital consumer markets. This is an important policy agenda. However, as is, the concept of digital vulnerability does not go beyond the current emphasis on the protection of consumers from the negative consequences of their distorted economic behaviour. It is assumed that because of personalization that specifically targets vulnerabilities, consumers make economic decisions that they may come to regret afterwards. The regulatory focus is, thus, on the distorted expression of an otherwise intact personal will, which could emerge in a self-determined context but is changed to fit goals of economic gains at the moment the consumer enters into an economic relation with a provider of some digital product or service. It is protection ex post, after the formation of will and choice (however irrational it may be).

C. Privacy

I want to put forward for consideration that the concept of digital vulnerability could be stronger if it were to conceptualize the idea of privacy as the very foundation for any human action (including consumer choice).

To be sure, privacy does play a role in *digital vulnerability*. Helberger et al mention that a lack of privacy can be a potential source of vulnerability and that the GDPR suffers from a similar outdated approach as the UCPD; the former distinguishes between 'sensitive data' and non-sensitive data in a similar way as the latter distinguishes between vulnerable and non-vulnerable consumers.[65] And Galli sees privacy as the second layer of vulnerability.[66] Both accounts see privacy as an autonomy-enhancing value.[67] And both accounts see privacy as a possible source of vulnerability. Calo, in turn, formulated the relation between privacy and vulnerability in this way: the more vulnerability there is, the less privacy there is, and vice versa. In the latter sense, privacy acts as a shield that places barriers in the way of discovering vulnerability.[68] Here, the function of privacy is to minimize exploitation by hiding the vulnerabilities or by protecting information that makes individuals vulnerable.[69] Nevertheless, the concept of privacy is not thoroughly defined and it is not clearly understood how the relation between privacy and vulnerability unfolds.

In what follows, I will show that the relationship between privacy and vulnerability is determined by their concern with autonomy. What is more, I will argue that incorporating a thick understanding of privacy into the concept of digital vulnerability can help to balance the hypo-autonomy of consumers against the hyper-autonomy of companies in the digital sphere ex ante. This strengthening of the consumer position is possible because *thick privacy* allows us to see *why* consumers are less autonomous in the digital sphere than in other spheres of consumer action: because the hyper-autonomy of companies is based on large-scale surveillance and privacy-intrusions. These violations of privacy are the very basis of vulnerability, because they inhibit the *formation* of autonomous will, which then later have an impact on the *expression* of that will (distortion of economic beha-

65 Helberger et al., *supra* note 16, 190.
66 Galli, *supra* note 16, 199.
67 Helberger et al., *supra* note 16, 190.
68 Ryan Calo, *Privacy, Vulnerability, and Affordance*, 66 DePaul Law Rev. 591–604 (2017), 596.
69 ibid., 600.

viour). *Thick privacy* emphasizes the conditions for autonomy. Autonomy needs privacy. Privacy is a necessary conditions for autonomy because it protects a physical or – in the digital world – a mental space in which individuals can develop and reflect on values which they deem to be their own.

I. The value of privacy

Here, I follow those authors who attribute a distinct value to privacy as opposed to the ones who see privacy merely instrumental to other values. Already Brandeis and Warren, the arguably first ones to define the right to privacy, attribute a coherent and distinctive value to privacy which they conceptualize as the right to be left alone.[70] This stance was later defended by several authors. Bloustein, for example, saw a distinct value in privacy has– connected to human dignity - that would get lost if it wasn't mentioned.[71] Also Gavison sustains that privacy should be legally protected in itself because or even though serves different important functions (human aspirations).[72] And Inness attributes a distinct value to privacy because it embodies our respect for peoples are creators of their own plans of intimacy and emotional destinies. For her, intimacy is the core of privacy, which has to be distinguished from other interests such as the right to be let alone or the freedom from government intervention.[73]

Fried understands privacy as being important for a human space and argues that privacy is a moral value in itself that goes beyond being merely a tool for assuring another substantive interest.[74] It is rather the foundation without which other fundamental ends and relations (respect, trust, friendship, love) would simply not exist. Relationships build on common moral perceptions of personality, basic entitlements and duties vis-à-vis each other. Without privacy, the very integrity of humanity and personhood would be threatened and without privacy and we would not be human at all.[75]

70 Samuel D. Warren & Louis D. Brandeis, *The right to privacy*, 4 Harv. Law Rev. 193–220 (1890).
71 Edward J. Bloustein, *Privacy as an aspect of human dignity: an answer to Dean Prosser*, 39 New York Univ. Law Rev. 962 (1964).
72 Ruth Gavison, 'Privacy and the Limits of Law' (1984) 89 Yale Law Journal 421, 425.
73 Julie Inness, *Privacy, Intimacy, and Isolation* (Oxford University Press 1992), 74 ff.
74 Charles Fried, 'Privacy' (1968) 77 The Yale Law Journal 475, 477.
75 ibid., 477.

Privacy is essential to all human relationships because without respect for privacy, the minimal precondition for any relation would be missing.[76] For example, there would be no trust where there is no possibility of error that a private space provides.[77]

Gavison shows that scholars who argue that privacy does not have inherent value usually derive this argument from judicial decisions that usually do not protect privacy alone but in connection with another value and, thus, push them towards assuming no overarching value in itself.[78] However, she shows that the one does not logically follow from the other. Moreover, the instrumental view neglects the motivations for individual privacy claims.[79] Finally, as reductive accounts 'suggest that privacy is only a label used to protect other interests, logic would dictate that whenever a privacy question is discussed, the balancing should be among the "real" interests involved. Consequently, privacy is made redundant despite its usage.'[80]

For our purposes, it is important to see that the inherent, and if you wish: moral, value of privacy derives from the function of privacy. Privacy enables other values, such as autonomy, mental health, creativity, the capacity to create meaningful human relations, or even the formation of liberal citizens. These functions should not be understood in a modal way. Rather, these positive functions of privacy relate to the promotion of liberty, moral intellectual integrity, intimate relationships, and ideals of a free society in a law-like way, similarly to a *conditio sine qua non*.[81]

II. *Thin privacy* in EU Law: control rights

There are what I would call thin and thick accounts of privacy. The former operate more on the surface-level of observable behaviour, the latter provide context and deeper meaning to the concept of privacy. In the EU, the understanding of privacy is thin one. It is highly limited and, in the commercial sphere, is reduced to data management rights.

76 ibid., 484.
77 ibid., 486.
78 Gavison, *supra* note 72, 461-463.
79 ibid., 465.
80 ibid.,. 467.
81 Jeffrey L Johnson, 'A Theory of the Nature and Value of Privacy' (1992) 6 Public Affairs Quarterly 271, 280.

First of all, privacy protection does not have to be a concern for the commercial sector. The right to privacy as protected under Article 8 ECHR is not generally applicable in horizontal relations. While the ECtHR has carved out the right to privacy in the ECHR, arguably covering a wider range of interests, such as private and family life, home, and correspondence, right to one's imagine, identity and personal development, as well as the right to establish and develop relationships with others, the protection afforded under Article 8 ECHR does not have direct effect for the relations between consumers and companies that surveil them.

Second, in the commercial realm, privacy is understood in a limited way as data protection. The GDPR outsources the issue of privacy protection to the ePrivacy Directive 2002/58,[82] which focuses more narrowly on electronic communication and the use of cookies and other trackers. It is currently in the process of being reformed by the draft ePrivacy Regulation (ePR),[83] as part of the protection regime demanded by Article 7 ChFR, focusing on the confidentiality of electronic communications generally. The GDPR, in turn, regulates the use of personal data. It conceptualizes privacy merely as a set of control rights. The GDPR contains a catalogue of rights, which data subjects can exercise or not, such as the right to transparent information about data processing, Articles 11 through 15 GDPR, right to rectify wrong data, Article 16 GDPR, the so-called right to be forgotten, Article 17 GDPR, the right to restrict processing, Article 18 GDPR, or the right to object, Article 21 GDPR. Moreover, data collection and processing are only lawful if it is based on consent or necessity, Art 6 GDPR. Taken together, these provisions reflect a regulatory approach to privacy protection that is based on individual action by the data subject. It is the data subjects who have to give consent to data collection and processing and then take action in case there is wrong data or in case they want to object to data processing or erase data. Without such action, data collection and processing can and will proceed undisturbed. The approach to consent in the draft ePrivacy Regulation is the same, see Recital 18 ePR.

82 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

83 Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM/2017/010 final - 2017/03 (COD).

Even though onsent as the main legal basis for lawful data collection and processing has recently been strengthened in the case of *Meta v Bundeskartellamt* through stricter requirements for consent as a legal basis and for circumventing it by business 'necessity',[84] the interplay of consent and data rights in EU law reduces privacy to data control rights. They are personal data management rights. The protection under the GDPR can be called Do-It-Yourself protection,[85] which only gives weak power to individuals that cannot match the power of digital companies.[86] *The Meta*-judgment does not touch upon discussions to what extent the GDPR actually contains many pitfalls and hindrances to actual effective control.[87] The judgment about conceptual limitations of the GDPR comes *ante* the assessment of its effectiveness. This approach is in line with the general concern of the GDPR, which is not privacy or data protection per se, but rather the establishment of an internal data market. The GDPR does lay down rules for the protection of individual data (Article 1 (1) GDPR), but does so within the context of its aim to create an internal data market (Article 1 (3) GDPR). It includes rights that clearly serve the establishment of an internal market: for example, the right to data portability, which is inherently concerned with the movement of data from one provider to another. Recital 13 GDPR even states that the 'proper functioning of the internal market requires that the free movement of personal data within the Union is not restricted or prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.' This statement makes it clear that the internal market comes first; data protection second.

This outline shows that, in EU consumer law, privacy is understood in a narrow way. Data serves as a proxy for privacy and individuals are put in charge of its protection. The EU understanding comes close to

84 Case C-252/21 *Meta Platforms Inc. Meta Platforms Ireland Ltd, Facebook Deutschland GmbH v Bundeskartellamt*, ECLI:EU:C:2023:537.

85 Alec Wheatley, 'Do-It-Yourself Privacy: The Need for Comprehensive Federal Privacy Legislation With a Private Right of Action' (2015) 45 Golden Gate University Law Review; Tobias Matzner and others, 'Do-It-Yourself Data Protection—Empowerment or Burden?' in Serge Gutwirth, Ronald Leenes and Paul De Heert (eds), *Data Protection on the Move - Current Developments in ICT and Privacy/Data Protection*, vol 24 (2016).

86 Daniel J Solove, 'The Limitations of Privacy Rights' [2022] GW Law Faculty publications.

87 I. van Ooijen & Helena U. Vrabec, *Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective*, 42 J. Consum. Policy 91–107 (2019).

privacy as the control over information, more specifically how and to what extent personal data should be collected and processed for business purposes. Control is exercised through the granting or denial of consent and rights concerning rectification, erasure, mobility, or objection. This is a thin understanding of privacy in terms of control rights is concerned with authorization as the variable that decides on the lawfulness of publication of information. Privacy gives the right to control information, as Westin claimed in 1967,[88] meaning the individual right to determine when, how and to what extent information about them is communicated. This includes the right to withhold or conceal information (privacy as secrecy).[89]

III. *Thick privacy*: substantive dimensions

There is a spectrum of thicker accounts of privacy. On one end of the spectrum, we can locate ideas of privacy as clear boundary-setting between a private self and public intrusion. On the other end, emphasis is put on the context-specific construction of a private sphere.

An example of the first group is the Warren and Brandeis' right to be left alone,[90] which draws a strict line separating private and public behaviour. They are not interested in what it is that precisely makes certain behaviour private or public. What matters for them is the idea that 'something private' is being 'made public.' While emphasis is on the movement from the private into the public without consent, thus basing themselves in the idea of control, it could provide grounds for a thicker understanding of privacy because it is absolute. In the context of the rise of 'mass media and newspaper enterprise, instantaneous photographs, gossip as trade at the end of the 19th century, Warren and Brandeis' privacy is the necessary 'retreat from the world'.[91] It includes the idea of an inviolate personality.[92] In a similar vein,

88 This is probably the most wide-spread understanding of privacy. Fundamentally: A. Westin, *Privacy and Freedom* (London: The Bodley Head 1967).

89 See R. Posner, "The Right of Privacy" 12. *Georgetown Law Review* 1977, p 393. For an overview of different definitions, see D. Solove, "Conceptualizing Privacy" 90. *California Law Review* 2002,1087.

90 Warren and Brandeis, *supra* note 70.

91 ibid., 195-196.

92 ibid., 205.

other authors define privacy as the limited access to a person.[93] They share a concern for a certain boundary that needs to be defended. Privacy refers to the right to determine the boundaries of an own private – as opposed to public – space. This approach can be called defensive because of its role in protecting a personal space of liberty in which the very self can flourish.

An even thicker account of privacy is provided by Cohen who defines privacy as freedom from surveillance.[94] She sees privacy as foundational for informed and reflective citizenship on the one hand and the capacity for innovation on the other. For her, privacy protects 'the situated practices of boundary management through which the capacity for self-determination develops.[95] While the idea that privacy protects the space for the development of the liberal self has an aspect of boundaries to it,[96] Cohen's concept of privacy is thicker because she is concerned with shelter emergent subjectivity from efforts of commercial and governmental actors to render individuals transparent and predictable'.[97] Surely, privacy as a shield is about control of those boundaries, but it is also about the defence and preservation of a space in which the will to control can even develop. As 'emergent subjectivity' exists in the space between the experience of autonomy and social shaping, Cohen acknowledges that the 'self' is socially constructed.

Similarly, Solove argues that privacy cannot and should not be defined in a static way, but always in relation to a specific context. Privacy, in this view, refers to the practices (activities, customs, norms) that are the product of history and culture.[98] It cannot be understood a priori but only in specific contexts of social practices. The protection of privacy implies the protection of those social practices from disruption. Against the backdrop of historically changing conceptions of privacy, the value of privacy in each and every specific situation is also changing. For Solove, the value of privacy *in the context of large-scale surveillance* lies in the protection from

93 Hyman Gross, *The Concept of Privacy,* 42 New York Univ. Law Rev. Also Gavison, *supra* note 73.
94 Julie E. Cohen, *What privacy is for*, 126 Harv. Law Rev. 1904–1933 (2013), 1905.
95 ibid., 1905. also: Cohen, "Configuring the Networked Self: Law, Code, and the Play of Everyday Practice" *Gergetown Law Faculty Publications and Other Works*, 2012, p 149.
96 Cohen, *supra* note 94.
97 ibid., 1905.
98 Daniel J Solove, 'Conceptualizing Privacy' (2002) 1087 The Individual and Privacy: Volume I 333, 1092-1093

a systemic oppressiveness that suffocates the exercise of power that renders people vulnerable and helpless.[99]

Acknowledging the pervasiveness of the digital surveillance architecture, Ienca and Andorno introduce the concept of mental privacy as a 'neuro-specific' right that copes with possible misuses of neurotechnology and its threat to fundamental liberties associated with individual decision-making.[100] To them, privacy protection in this context implies the recognition of a negative right to cognitive liberty that protects individuals from the coercive and unconsented used of neuro-technologies as well as the right to mental privacy and the right to psychological continuity. The right to mental privacy protects 'private or sensitive information in a person's mind from unauthorized collection, storage, use, or even deletion in digital form or otherwise, thus protecting not only *expressed information* but also the *generation* of such information. The right to psychological continuity, in turn, protects the 'mental substrates of personal identity from unconscious and unconsented alteration by third parties' through the use of neuro-technologies. Their idea goes significantly beyond the ideas expressed above (thin privacy) as it incorporates a concern for the pervasiveness of new technologies. In this way, it gives shape to the concern shared with Cohen and Solove about the mental effects of large-scale surveillance.

To my mind, Ienca and Andorno synthesize the interpretations of privacy specifically for the digital sphere. It is the probably thickest of all accounts of privacy because it does not merely deal with the expression of internal will but also with the possibilities of its formation. It gives another name to Cohen's protection of emergent subjectivity. Moreover, it shows that accounts such as Fried's or Inness' – which are concerned with attributing inherent value to privacy - are very well applicable in the digital sphere. Despite Solove's critique of attempting of finding an overarching definition, Ienca and Andorno's critique of dismantling of intimacy or other conditions for any human relation and activity is spot on in the context of large-scale surveillance. In my view, their ideas can be reformulated in Solove's terms not as overarching definitions but as a concern for the preservation of a shelter for human flourishing *within the specific context* of large-scale supervision in the political economy of informational capitalism. Both Fried's and Inness' concern for the inherent function of privacy

99 ibid., 1149 ff.

100 Marcello Ienca & Roberto Andorno, *Towards new human rights in the age of neuroscience and neurotechnology*, 13 Life Sci. Soc. Policy 1–27 (2017).

for intimate human relationships and Cohen's freedom from surveillance as a pre-requisite for 'protected zones of personal autonomy aim at giving room to productive expression and development to flourish'.[101] Mental privacy is the specific privacy that is protected by freedom from surveillance.

IV. Privacy and autonomy

There is a necessary connection between privacy and autonomy because privacy is pivotal for autonomy. I have elaborated on this connection in more detail elsewhere, based on the model of informed consent by Faden and Beauchamp,[102] so I will confine the following to a summary of the points that are important for this contribution. To Faden and Beauchamp, autonomous action must be intentional, based on understanding, and free from controlling influences.[103] Intention arguably develops in condition of privacy because it is concerned with the formation of authentic will, while the freedom from manipulation concerns the expression of will. Faden and Beauchamp are weary of including authenticity of will as an additional requirement for autonomous action because they believe that it would narrow down the scope of actions protected by a principle of respect for autonomy.[104] For them, it makes sense to define 'autonomy' broadly and not include too many limiting parameters (such as authenticity). Their concern is, thus, with casting a broad net in order to lead to broad protection of what can be considered autonomous action.

For our purposes it is however useful to include a notion of authenticity into the 'intention' parameter of their informed consent theory. It allows us to cast a wide net over what would have to be protected in large-scale surveillance. For the aim of highlighting the importance of privacy for autonomy, it makes sense to include authenticity into the conceptual framework of what *intention* is, because in case of its absence, we can determine a violation of the conditions for autonomous action and informed consent. Here, including privacy conditions leads to a wider 'surface' to catch more

101 Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 Stanford Law Rev. 1373 (2000),1377.

102 Irina Domurath, 'Plaform Economy and Individual Autonomy' (2022) 30 European Review of Private Law, with reference to Ruth R Faden and Tom L Beauchamp, *A History and Theory of Informed Consent* (Oxford University Press 1986).

103 Ruth R Faden and Tom L Beauchamp, *A History and Theory of Informed Consent* (Oxford University Press 1986), 238.

104 ibid., 265.

possible violations. In the end, this result is in line with the goal of broad the protection sought by Faden and Beauchamp (who made their argument before the emergence of pervasive new technologies).

The connection between privacy and autonomy is either explicit or underlying the above-mentioned definitions of privacy. In the defensive accounts of privacy as a space of non-interference, the protection from any type of intrusion is considered incompatible with the freedom associated with a personal space in which the self can develop and flourish. Also Westin is concerned with this space. He sees the preservation of autonomy goal of privacy protection, a release from role-playing, and the possibility of having time for self-evaluation and for protected communication.[105] Autonomous individuals can exist only when there is the possibility of establishing a boundary between the self and their surroundings. Total transparency – the complete lack of privacy –signifies the disappearance of the boundary between the self and its surrounding; a 'transparent self' cannot exist because individuation needs a certain amount of concealment from the environment.[106]

A more substantive connection between privacy and autonomy can be found in Cohen's understanding of privacy regards freedom from surveillance. Here, privacy as the absence of surveillance is foundational to the practice of informed and reflective citizenship, and therefore an indispensable structural feature of liberal democratic political systems.[107] To her, a lack of privacy means a reduced scope for self-making (along liberal or other lines) through the development of subjectivity that is shaped by social and communal values.[108] She focuses on the conditions for 'meaningful autonomy in fact'.[109] Thus, the right to be left alone must, in a political economy of informational capitalism that is based on large-scale surveillance, comprise the right to be left alone *mentally*. It implies the right to not merely control, but close off a mental space for any intervention or influence of any kind, including nudging and other attempts of behavioural manipulation. It is precisely this space free from intervention and observation that is needed for play, experiments, successes and failures as necessary

105 A. Westin, *Privacy and Freedom* (London: The Bodley Head 1967).
106 Ida Koivisto, *The Anatomy of Transparency: The Concept and its Multifarious Implications*, EUI Work. Pap. MWP 1–22, 20 (2016).
107 Cohen, *supra* note 94, 1905.
108 ibid., at 1911.
109 Cohen, *supra* note 101.

for the development of individual personalities, which, in turn, is the basis for any human interaction, be it personal, social, economic, or political.

This does not mean that individuals need to be completely disconnected from their surroundings in order to be autonomous. For our purposes, it is not important whether autonomy thrives only in the possibility of complete seclusion from any societal forces or whether autonomy is constitutively shaped by interpersonal relations and interactions, because large-scale surveillance undermines both, the secluded individual and the socially and culturally shaped individual. Emphasizing the possibility for a mental space as a necessary condition for autonomy rather than the conditions under which individuals acquire their identity makes this clear. If we regard individuals only as autonomous in the complete absence of any influence – the broader protection would be afforded here -, autonomy is eroded because there is no mental space under large-scale surveillance. If we regard individuals as socially constituted and shaped, autonomy is also eroded because there is no mental space either for developing basic autonomy. There is nothing that social factors could even influence and help to shape. Big data analyses, data mining, and deep data are ever more intruding upon the internal space where freedom of thought, free will, and individual autonomy can develop. Surveillance deprives private autonomy of its very foundation because it runs counter to the idea of a mental space for its development.

V. Interim conclusion 2

Privacy has an intrinsic value as the basis for individual autonomy. The current EU Law framework falls short of this understanding because it outsources privacy-concerns to the public sphere in which states and public authorities must be held accountable for privacy intrusions, whereas only giving data management rights to individuals in the commercial sphere. Those rights merely serve to control data flows, giving consumers very little power vis-à-vis companies who collect, exploit, and sell that data. In this way, EU Law incorporates a thin understanding of privacy.

In contrast, the concept of thick privacy draws our attention to large-scale surveillance on which digital business strategies are based. Understood as freedom from surveillance or mental privacy, *thick privacy* for the digital sphere emphasizes that individual autonomy is not merely attacked by manipulation, but is structurally and inherently eroded. Acknowledging

that privacy – including mental privacy – is a necessary conditions for autonomy and the formation and exercise of any meaningful informed consent in practice, shows that the mere monitoring of consumer behaviour is a violation of privacy that can inhibit consumer autonomy to develop in the first place. As a consequence, the conditions for informed consent – the basis of consumer dealings in the digital sphere – are not met.

D. Conclusion: digital vulnerability and thick privacy

Digital vulnerability is a new type of consumer vulnerability related to the emergence of new digital technologies. Hitherto, it describes the potential for harm through the adaptive persuasive systems employed in digital or algorithmic marketing. *Digital vulnerability* has the potential to move EU law away from its static understanding of consumer vulnerability in variation from the benchmark consumer standard to a more substantive understanding of vulnerability in the digital economy. This can be evidenced by the proposals put forward, for example by Helberger et al. They suggest a variety of changes based on *digital vulnerability* intended to improve the information paradigm by implementing an obligation for personalized privacy notices, consent as a process, as well as more efficient teaching and training programmes.[110] Moreover, they show that the structural asymmetries between companies and consumers in the digital economy (digital asymmetry) can qualify as forbidden 'aggressive practices' under Articles 8 and 9 UCPD, while being subject to a last resort fairness check under Article 5 (1) UCPD.[111] Similarly, Galli argues that Article 5 (1) and (2) UCPD create new professional duties and obligations of professional diligence, such as privacy by design, and that the digital-choice environment could qualify as 'undue influence' under Article 9 UCPD.[112]

To my mind, these proposals do not go far enough. The concept of digital vulnerability can do more than enable new interpretations. In fact, the mentioned proposals become substantially weaker as soon as there is talk of 'broader societal developments' that 'have to be taken into account'. For example, Helberger et al, when advancing better media literacy proposals, acknowledge that 'not including a broader social perspective and not ad-

110 Helberger et al., *supra* note 16, 41 ff.
111 ibid., 49 ff.
112 Galli, *supra* note 16.

dressing the inequalities of power and knowledge mentioned … renders this effort insufficient for protecting consumers in the online environment.'[113] But this is not followed by clarifications about how those inequalities of power and knowledge could and should be addressed.

Viewing vulnerability as a power relation, shifts our focus towards the main constituent parameter of this power asymmetry: autonomy asymmetry. On the one hand, there is the *hyper*-autonomy of digital companies: the structural power to determine not only their dealings with consumers but also the environment in which these dealings take place. Companies are the ones who make the very markets on which they all other market players interact. They make those markets through large-scale surveillance, collecting vast amounts of data, and turning profits through personalization. On the other hand, there are the *hypo*-autonomous consumers, unable to negotiate their dealings with companies and certainly not to build the markets on which they interact with companies.

Adopting the notion of *thick privacy* – understood as mental privacy and freedom from surveillance - for the concept of digital vulnerability would give substance to this power relation. While both Helberger et al and Galli do give a lack of privacy a role to play in the creation and manifestation of digital vulnerability, both accounts under-conceptualize privacy. It is however here, where the concept of digital vulnerability could unfold its potential. Privacy impacts upon digital vulnerability precisely because it secures the conditions for autonomy. Privacy protects autonomy. Digital vulnerability reflects diminished consumer autonomy.

If the literature on digital vulnerability made it clear that privacy needs to be understood in a thick way, privacy intrusions through large-scale surveillance could be adequately included into the concept of digital vulnerability. In Helberger et al.'s version, the incorporation of *thick privacy* would emphasize the state of universal defenceless in exposure to power imbalances. This defencelessness would not – as they claim - merely be precipitated by the automation of commerce, datafied selling relationships and general digital architecture, but would specifically derive from large-scale surveillance. Adopting a thick understanding of privacy would explain why the digital architecture does in fact lead to vulnerability: because privacy is invaded structurally through mental monitoring, measuring, and manipulating. In Galli's layered digital vulnerability, the acknowledgement of *thick privacy* would let collapse the distinction between the foundational layer of

113 Helberger et al., *supra* note 16, 44.

the architecture of algorithmic marketing and the second layer of privacy. The large-scale invasion of privacy is part of the architecture of algorithmic marketing.

Thick privacy changes the focus of both the digital vulnerability concept and the consumer vulnerability framework in EU Law away from the manipulation of behaviour (the expression of autonomy) towards a much more subversive change of thinking and manipulation of will (the formation of autonomy). Large-scale surveillance – this is the contribution of *thick privacy* – impedes self-determination at the most basic level. The focus on the economic distortion of consumer behaviour through manipulation comes in at a later stage, when avoiding economic and financial harm from the subversively manipulated will of consumers. *Thick privacy* in a context of surveillance capitalism makes it clear that economic and financial harm in terms of behavioural manipulation is merely a symptom of the underlying harm to the formation of self-determination and free will. In this way, the concept has the potential to balance the hypo-autonomy of consumer against the hyper-autonomy of companies. Thick privacy can be used as a sword[114] also by consumers because it makes it clear that it is large-scale surveillance and data collection that makes them vulnerable. In this way, the violation of *thick privacy* thus becomes the root of digital vulnerability. Adopting a thick idea of privacy within a concept of digital vulnerability (and hopefully into EU Law) would thus shift our focus away from emphasizing the danger for manipulation of consumer behaviour to a state prior to the actual decision-making, namely the formation of consumer will.

114 Calo, *supra* note 68.