PREFACES

Enforcing and Expanding Legal Protections for Vulnerable Subjects

Frank Pasquale

Technological advance is almost always a double-edged sword. The same AI that can propose different chemical compounds for medicinal purposes can also suggest new poisons. Advertising targeting software may be immensely useful, but may also take advantage of vulnerabilities (by, for example, marketing cosmetics to a person when it calculates they are feeling most unattractive). Generative AI creates an enormous range of useful images, but also dramatically reduces the cost of disinformation.

Is there a way to encourage the positive side of digital advance, while curbing its negative effects? If so, law is among the most important tools for achieving this end. In *The New Shapes of Digital Vulnerability in European Private Law*, Camilla Crea and Alberto De Franceschi have assembled a remarkable set of authors to chart the path forward. The authors in this volume both propose expanded enforcement of extant law, and postulate important new protections. While I cannot convey the breadth of their contributions in a brief preface, I describe below a set of perspectives in the volume that illustrate one particular achievement of this collection – its simultaneously solid grounding in present controversies and ambitious aspirations toward a better future.

Emilia Mišćenić has starkly laid out the stakes of the present inquiry in her chapter, *Information, Transparency and Fairness for Consumers in the Digital Environment.* As she observes, "Despite the existing legal framework, businesses are only purportedly complying with legal rules. More often than not, they are circumventing or ignoring the requirements of EU consumer law related to mandatory information duties and transparency." This is an important diagnosis, justifying further inquiry into both improved enforcement and reform of present legal authorities.

In terms of law reform, Mateja Durovic and Eleni Kaprou recognize that "digital asymmetry captures the position of imbalance between traders and consumers online, alongside the embedded vulnerability of consumers." They argue in *The New Concept of Digital Vulnerability and the European Rules on Unfair Commercial Practices* that "more holistic and extensive

reform of the [Unfair Commercial Practices Directive] will be required to thoroughly adapt consumer law regulations to the fluctuating digital economy." This is an important level-setting, establishing the stakes of vulnerability-related legislation and the importance of advancing it.

Federica Casarosa and Hans-W. Micklitz expertly state the case for caution with respect to online dispute resolution systems, especially with respect to the disabled and impoverished. Their chapter *Addressing Vulnerabilities in Online Dispute Resolution* recognizes both the uses and shortcomings of digital literacy approaches. They articulate three dimensions of digital asymmetry which must be at the core of future legislation and enforcement in the area. First there is relational asymmetry, "due to the position [consumers] have in a complex digital environment where equal interaction is made impossible." The old problem of "one-shot" versus "repeat players," noted in Marc Galanter's *Why the Haves Come Out Ahead*, is profoundly exacerbated in massive platforms which are older than a fair number of their users—and more powerful than nearly all of them. Second, there is architectural asymmetry, which is only belatedly and partially addressed by restrictions on dark patterns and similar forms of manipulation via interface. Third, they analyse the problem of knowledge-based asymmetry, where "the trader benefits from detailed insights about the consumer while the consumer often knows - or understands - very little about how the trader and the service operate." Large platfoms may base their calculations on billions of transactions, while consumers have far less information—and, in concentrated commercial environments, few "exit" options to alternative providers.

Recognizing this knowledge-based asymmetry, Irina Domurath's philosophically sophisticated chapter articulates the importance of privacy to help level the informational playing field. Many forms of manipulation are based on intimate knowledge of a consumer or worker. Privacy law is not simply about informational self-governance, but also helps reduce the ability of other entities to erode the data subject's autonomy. Domurath proposes "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)." This is a thought-provoking challenge to surveillance capitalism, logically extending Shoshana Zuboff's critique of behaviorism by deeply considering the foundations of the philosophy of action. Real human action (or human agency, in Charles Taylor's framing), rather than mere conditioned response, is premised on free

will, which is in turn dependent on some Goffman-ian "off-stage" space to reflect and plan free of any entity's prying eyes or sensors.

To be sure, critics of liberal individualism might characterize such a space as a fantasy. As Hans-Georg Gadamer recognized, we are always already socially formed in our aspirations and ideals. Nevertheless, we should also recognize that, as Jordan Stein has argued, a fantasy "picks us up and dusts us off and allows us to say to ourselves…I am not (or, as the case may be, I am) that kind of person, this action is not (or, again, is) part of the pattern, often called a personality, that adds up to me as the person I recognize myself to be."[1] The fantasy of self-governance beyond the scope of market imperatives may operate as an ever-receding, and yet still hope-inspiring, horizon of vulnerability studies. Certainly no one can blame today's oft-manipulated consumers for chasing such a dream, however often the grim realities of online commerce dash its realization.

Fabrizio Esposito's conception of "hyper-engaging" practices as particularly manipulative nudges (in his chapter *Investigating Digital Vulnerability with Theories of Harms*) illuminates the stakes of such aspirations in a particularly perceptive manner. The work of thinkers ranging from Jonathan Haidt (*The Anxious Generation)* to Lauren Berlant (particularly with respect to their theory of "cruel optimism") should motivate sophisticated commentators to reconsider liberal scholars' almost blanket rejection of critical theories of false consciousness. Left unresisted, hyper-engagement ultimately defeats more grounded, authentic, and valid aspirations.[2] Moreover, new technology is constantly expanding the potential reach of hyper-engagement. For example, as Niti Chatterjee and Gianclaudio Malgieri argue, the type of wearables marketed for metaverse engagement could easily "exacerbate existing areas of concern, transforming minor vulnerabilities into major threats." Along with Shabahang Arian in this volume, they presciently advance the digital vulnerability field into virtual reality.

Mateusz Grochowski's chapter also skillfully extends the scope of aspiration in the field of digital vulnerability. He convincingly argues that consumer protection laws must move beyond a purely economic focus, to address non-economic experience (including emotional and social well-be-

1 Jordan Alexander Stein, *Fantasies of Nina Simone* (Duke University Press, 2024), 11.

2 David Golumbia and Frank Pasquale, "From Public Sphere to Personalized Feed: Corporate Constitutional Rights and the Challenge to Popular Sovereignty," in *Human Rights after Corporate Personhood*, edited by Jody Greene & Sharif Youssef (Toronto: Univ. of Toronto Press, 2020).

ing). Grochowski observes that "EU consumer law has never developed a systematic framework for including non-economic interests and non-economic harm," despite an "expansion of the digital economy" that has "made this deficit particularly vivid and troublesome." This insight should be taken seriously by EU policymakers, particularly as the field of affective computing advances to develop more sophisticated methods of simulating and stimulating emotions.[3] But these same policymakers deserve credit for advancing regulation in a way that opened up space for legal academic consideration of the proper scope and force of consumer protection law.

This volume demonstrates a remarkable symbiosis between policy-oriented legal academic work, and more theoretical and philosophical scholarship. Because Europe has taken on the challenge of digital vulnerability in its privacy and consumer protection laws, it has sparked a number of fascinating inquiries into the nature of manipulation, fair trade, and commercial ethics. Meanwhile, because of the existence of this substantial body of literature, those developing new regulations and applying them are privy to deeply considered analyses of the strength and limits of the vulnerability concept. This is a virtuous cycle to which the present volume makes a sterling contribution. I congratulate the editors and authors on their remarkable capacity to refine our normative understanding of asymmetries of power and harm in online contexts, while proposing concrete advances in the legal regime meant to address these asymmetries.

3 Frank Pasquale, "Affective Computing at Work: Rationales for Regulating Emotion Attribution and Manipulation," in *Artificial Intelligence, Labour and Society*, edited by Aida Ponce del Castillo (Brussels: ETUI Press, 2024).