MAKING VULNERABILITY: PLATFORMS AND THEIR AFFORDANCES

Sherry Tseng[*]

TABLE OF CONTENTS

[*] Georgetown Law J.D. 2024; University of Pennsylvania B.A./M.A. 2020.

INTRODUCTION

The law often treats vulnerability as a binary status: a person or a group is vulnerable based on their fulfillment of certain conditions. Those deemed vulnerable are thus afforded heightened legal protections.[1] The Children's Online Privacy Protection Act, for example, imposes stricter requirements on the collection of personal information of those under the age of thirteen.[2] Several federal and state laws safeguard against elder abuse.[3] And the doctrine of contractual incapacity gives those with mental disabilities a legal defense to their contractual obligations.[4]

But vulnerability is neither an *a priori* nor a dichotomous status. A person and/or group can be *made* vulnerable to varying degrees. This is increasingly true in digitally mediated environments. Algorithms interfere with our decision-making abilities[5] and social robots engage our emotions to induce disclosure of sensitive information.[6]

The goal of this Note is to explore the relationship between platforms and user vulnerability and consider whether and how the law should respond. To do so, it brings three areas of study into conversation and assigns each area a functional role, each mapping onto the three Parts. Part I discusses the conceptual contribution of vulnerability theory. While the literature is rich in discussions on the influence of digital technology on autonomy,[7] I take vulnerability as

---

[1] *See* Martha Albertson Fineman, *The Vulnerable Subject: Anchoring Equality in the Human Condition*, 20 YALE J.L. & FEMINISM 1, 8 (2008) [hereinafter Fineman, *Anchoring Equality*]. *See generally* Martha Albertson Fineman, *The Vulnerable Subject and the Responsive State*, 60 EMORY L.J. 251 (2010) [hereinafter Fineman, *The Vulnerable Subject*].

[2] Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–06 (2012).

[3] *See Elder Abuse and Elder Financial Exploitation Statutes*, U.S. DEP'T OF JUST., https://www.justice.gov/elderjustice/prosecutors/statutes [https://perma.cc/KP4D-NQ9Y].

[4] *See* Sean M. Scott, *Contractual Incapacity and the Americans with Disabilities Act*, 123 DICK. L. REV. 253, 257–62 (2020).

[5] *See generally* Daniel Susser, Beate Roessler & Helen Nissenbaum, *Technology, Autonomy, and Manipulation*, 8 INTERNET POL'Y REV. (2019); SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER (2018).

[6] *See* Woodrow Hartzog, *Unfair and Deceptive Robots*, 74 MD. L. REV. 785, 791–96 (2015).

[7] *See, e.g.*, Daniel Susser, Beate Roessler & Helen Nissenbaum, *Online Manipulation: Hidden Influences in a Digital World*, 4 GEO. L. TECH. REV. 1 (2019); Tal Z. Zarsky, *Online Privacy, Tailoring, and Persuasion*, *in* PRIVACY AND TECHNOLOGIES OF IDENTITY—A CROSS-DISCIPLINARY

the entry point. Doing so scaffolds two ideas. First, because the law recognizes vulnerability as meriting a response, spotlighting vulnerability rather than autonomy gives us a better opening to demand legal protection.[8] Second, vulnerability theory reframes the interest warranting protection from a designated static category to a relational, context-dependent condition that admits of degrees. This gives us a thicker description of the problem. Feminist theory marries vulnerability to a *relational* account of autonomy. The harm then is not threats to traditional notions of autonomy, which are predicated on atomistic conceptions of selfhood, but to socially constituted capacities. Pressures on these capacities lead to what I call "imposed vulnerability."

Part II draws from platform studies to offer a descriptive claim. I locate the platform as a distinct actor that imposes vulnerability. Many have written about the contributions of different features of digital environments, such as data flows and technology design, to impairing autonomy,[9] but few have offered a detailed account of the unique role of *platforms*.[10] This Note builds on those accounts and bridges them to vulnerability. Platforms are not just a new economic model. They are also much more than the facilitators of data flows. Rather, as the architects of the information economy, they decide what information can constitute data and what choices are available in the first place, limiting the possible forms that the self takes in the digital world. In doing so, they constrain the range of options necessary for the full development and exercise of relational autonomy and impose vulnerability on the self.

Finally, building on the conceptual and descriptive claims, Part III looks to the Commission's Section 5 authority to regulate unfair or deceptive trade acts or practices. Examination of case law and legislative history shows whether and how the Commission might

---

CONVERSATION 209 (Katherine J. Strandburg & Daniela Stan Raicu eds., 2006).

[8] *See* Fineman, *The Vulnerable Subject*, *supra* note 1. The law also recognizes autonomy as independently deserving of legal protection, but has placed far more legal restraints on autonomy per se. *See, e.g.*, Dobbs v. Jackson Women's Health Org., 597 U.S. 215, 257 (2022) (rejecting "attempts to justify abortion through appeals to a broader right to autonomy").

[9] *See infra* Part II.A.

[10] *See* Julie E. Cohen, *Infrastructuring the Digital Public Sphere*, 25 YALE J.L. & TECH. 1 (2023) [hereinafter, Cohen, *Infrastructuring*]; Julie E. Cohen, *Platforms, Data Infrastructures, and Infrastructure Stacks*, *in* GLOBAL GOVERNANCE BY DATA: INFRASTRUCTURES OF ALGORITHMIC RULE (Fleur Johns, Gavin Sullivan & Dimitri van den Meerssche, eds., forthcoming 2024) [hereinafter Cohen, *Infrastructure Stacks*].

be able to wield its authority to address the power of platforms to render users vulnerable.

I. VULNERABILITY

In 2013, marketing firm PHD published a study that claimed that women tend to feel less attractive on Monday mornings.[11] The study advised advertisers to target ads towards women on Monday mornings because those were their "prime vulnerability moments."[12] The marketing study was met with outrage: PHD had, in effect, suggested targeting, if not exploiting, women at their most vulnerable in the pursuit of profit.[13]

But what does it mean for women to be in their "prime vulnerability moments"? Women on Monday mornings are, after all, not typically understood as a particularly vulnerable demographic group. This Part offers a theoretical framework of vulnerability. It departs from the traditional view of vulnerability as a binary label and instead draws from vulnerability theory to frame it as iterative layers of both ontological conditions and social arrangements.

Traditionally, vulnerability refers to the state of being more open to harm and dependent on others to safeguard against harm on the basis of belonging to certain demographic groups.[14] This "labels" approach has been intensely critiqued;[15] in response, Florencia Luna

---

[11] PHD Media, *New Beauty Study Reveals Days, Times and Occasions When U.S. Women Feel Least Attractive*, PR NEWS WIRE (Oct. 2, 2013, 10:00 AM), https://www.prnewswire.com/news-releases/new-beauty-study-reveals-days-times-and-occasions-when-us-women-feel-least-attractive-226131921.html [https://perma.cc/6QZC-96M4].

[12] *Id.*

[13] *See, e.g.*, Rebecca J. Rosen, *Is This the Grossest Advertising Strategy of All Time?*, THE ATLANTIC (Oct. 3, 2013); https://www.theatlantic.com/technology/archive/2013/10/is-this-the-grossest-advertising-strategy-of-all-time/280242/ [https://perma.cc/2Q87-RWMP]; Sam Jasenosky, *Advertisers Target Women's Insecurities*, THE MINNESOTA DAILY (Oct. 15, 2013), https://mndaily.com/259010/uncategorized/advertisers-target-women-s-insecurities/ [https://perma.cc/NWE9-D65F].

[14] *See* Florencia Luna, *Elucidating the Concept of Vulnerability: Layers Not Labels*, 2 INT'L J. FEMINIST APPROACHES TO BIOETHICS 121, 123–25 (2009).

[15] Among the critiques is that vulnerability "stereotypes whole categories of individuals, without distinguishing between individuals in the group who indeed might have special characteristics that need to be taken into account and those who do not." Carol Levine, Ruth Faden, Christine Grady, Dale Hammerschidt & Lisa Eckenwiler, *The Limitations of "Vulnerability" as a Protection for Human Research Participants*, 4

proposed an interpretation of vulnerability as layers.[16] In her view, vulnerability is a relational and context-dependent *layer* that exists in multiplicities and along different axes, and can be acquired and removed.[17] Constructed this way, a person is not categorically vulnerable, but can be rendered more or less vulnerable. They depend on others to protect them from harm and can be made more or less dependent.

In tracing the origins of such vulnerability, philosophers point to the dependence that arises from our embodied selves.[18] The body is the site of encounter with material dependencies, such as cognitive formation, illness, or disease. It is also the vehicle through which we experience our emotions and emotional needs, whether that be grief, isolation, or care. As such, it exists in a state of dependence that looks to individuals as well as social, economic, and cultural networks and institutions for support.[19] Vulnerability is thus universal.

Take Person A, who is of reproductive age in the top 10% of household income. If they become pregnant, they are vulnerable because they may face pregnancy complications and depend on social and medical support to meet their emotional and bodily needs. Compare them with Person B, who is a teenager of reproductive age in the bottom 10% of household income in a state that criminalizes abortion. Between the two, Person A is more likely to have access to a range of options for early and regular maternal care, while Person B is more likely to rely on the state for maternal healthcare coverage.[20] Person B then not only has the same layer of vulnerability arising from their emotional and bodily needs as Person A, but also acquires additional layers from their added dependence on the state's decisions on what public health insurance covers.

That vulnerability is universal implicates our understanding of autonomy. More precisely, if vulnerability is universal and humans

---

AM. J. BIOETHICS 44, 47 (2004). Another is that there are so many groups labeled vulnerable that by now, nearly *everyone* is vulnerable. *Id.* at 46.

[16] Luna, *supra* note 14.

[17] Florencia Luna, *Identifying and Evaluating Layers of Vulnerability—A Way Forward*, 19 DEVELOPING WORLD ETHICS 86, 88 (2018).

[18] *See* Wendy Rogers, Catriona Mackenzie & Susan Dodds, *Why Bioethics Needs a Concept of Vulnerability*, 5 INT'L J. FEMINIST APPROACHES TO BIOETHICS 11, 24 (2012); Catriona Mackenzie, *The Importance of Relational Autonomy and Capabilities for an Ethics of Vulnerability*, *in* VULNERABILITY: NEW ESSAYS IN ETHICS AND FEMINIST PHILOSOPHY 35 (Catriona Mackenzie, Wendy Rogers & Susan Dodds eds., 2013).

[19] *See* Fineman, *Anchoring Equality*, *supra* note 1, at 10.

[20] *See* Arline T. Geronimus, *Teenage Childbearing and Personal Responsibility: An Alternative View*, 112 POL. SCI. QUARTERLY 405 (1997).

are capable of autonomy, then autonomy cannot be understood in terms of a purely isolated and atomistic self.[21] Feminist theorists provide an alternative: relational autonomy, which imagines autonomy as a socially constituted capacity that relies on relationships rather than isolation.[22] Our selves are formed and revised by our connections with others.

The intersubjective character of autonomy is based on at least two principles. First, our sense of self is deeply intertwined with the recognition by others that our decisions and choices belong to an autonomous person—that is, they are *ours*.[23] This is because such recognition sustains important functions of our psychologies, such as self-trust, self-respect, and self-esteem.[24] Nonrecognition or misrecognition can thwart the development of those functions.[25] Should Person B wish to terminate their pregnancy but be unable to do so due to the state's laws, their "decision" to continue the pregnancy is not *theirs*. Rather, their pregnancy is an *imposed* condition that leaves them susceptible to intense stigma and misrecognition.[26]

Second, many of our capabilities and competencies are mediated by others in our social activities and practices.[27] If Person B is pushed out of school, as many teenage parents often are,[28] they can no longer

---

[21] *See* Fineman, *Anchoring Equality*, *supra* note 1, at 10 ("[The liberal subject] is indispensable to the prevailing ideologies of autonomy, self-sufficiency, and personal responsibility, through which our society is conceived as constituted by self-interested individuals with the capacity to manipulate and manage their independently acquired and overlapping resources.").

[22] Jennifer Nedelsky, *Reconceiving Autonomy: Sources, Thoughts and Possibilities*, 1 YALE J. L. & FEMINISM 7, 12 (1989) ("If we ask ourselves what actually enables people to be autonomous, the answer is not isolation, but relationships—with parents, teachers, friends, loved ones—that provide the support necessary for the development and experience of autonomy."). *See generally* Joel Anderson & Axel Honneth, *Autonomy, Vulnerability, Recognition, and Justice*, *in* AUTONOMY AND THE CHALLENGES TO LIBERALISM: NEW ESSAYS 127 (2005).

[23] Mackenzie, *supra* note 18, at 44.

[24] *Id.* at 44–45.

[25] *Id.*

[26] *See* Elizabeth Yardley, *Teenage Mothers' Experience of Stigma*, 11 J. YOUTH STUD. 671 (2008) ("Teenage mothers are often perceived as a homogenous group of immature, irresponsible, single, benefit-dependent, unfit parents who deviate from ideals of motherhood.").

[27] Joel Anderson, *Autonomy and Vulnerability Entwined*, *in* VULNERABILITY: NEW ESSAYS IN ETHICS AND FEMINIST PHILOSOPHY 134, 146–51 (Catriona Mackenzie, Wendy Rogers & Susan Dodds eds., 2013).

[28] *See also* Linda Mangel, *Pregnant and Parenting Students Are Still Being Pushed Out of School*, AM. CIV. LIBERTIES UNION (Mar. 31, 2011),

move through the world as a student nor can they participate in the social aspects of school.

Closely related is the freedom of association. The social support necessary to our capacities as autonomous beings must not be coerced. The development and exercise of relational autonomy demands an equality of access to a range of options.[29] One must be positioned to genuinely *choose* their decisions and social activities and like so, be able to choose the social relations they form. It is only on this basis that one can legitimately claim genuine recognition of their actions as *theirs* and participate in social activities and practices that reflect *them*.

There is, however, a thin line between the degree of vulnerability necessary to cultivate relational autonomy and that at which vulnerability becomes problematized. Unjust social arrangements can make us excessively vulnerable by rendering us dependent on others to the point that they erode our relational autonomy.[30] Under such conditions, just as Person B was made to depend on the government's decision to criminalize abortion, we are made to depend on others in such a way that our recognition and social competencies are no longer the product of our choices and decisions. Such arrangements result in what I call "imposed vulnerability."

In sum, vulnerability consists of iterative layers of both ontological conditions and social arrangements. Whether it is problematized turns on whether those iterative layers and their interactions may thwart the development and exercise of one's relational autonomy. This Note is concerned with imposed vulnerability. The next Part outlines how platforms may contribute to imposed vulnerability, ultimately to lay the ground to assess how the law might respond.

II. THE ROLE OF PLATFORMS IN IMPOSED VULNERABILITY

The effects of digital environments on user autonomy are well-documented in the literature. Most of the scholarship has centered on certain aspects of digital environments. Part II.A overviews these aspects; scholars thus far have focused on data flows and technical designs. Part II.B steps back. It examines the underlying architecture—the platform—that defines and limits the very capabilities that make data flows and technical designs possible. Borrowing from science and technologies studies, it frames the platform as a distinct actor that bends human activity to conform with

---

https://www.aclu.org/news/smart-justice/pregnant-and-parenting-students-are-still-being-pushed-out [https://perma.cc/VZ73-WSJ6].

[29] Mackenzie, *supra* note 18, at 45.

[30] *Id.* at 43.

and in the service of its own interests. In doing so, it renders users dependent on its choices for how they are recognized and what they can participate in, imposing another layer of vulnerability.

A. DATA FLOWS AND DESIGN INTERFACES

It is fairly widely recognized among academics that our online activities are not merely our autonomously-formed offline activities transposed into their digital forms. As many have discussed, the modern consumer is mediated by both intense data collection practices and design choices.[31]

First, large-scale commercial surveillance, together with profiling methods, seeks to shape user preferences and decisions.[32] Firms collect massive troves of data from wearables to cookies to behavioral biometrics.[33] Equipped with this information and the derived inferences,[34] they acquire a "capacity for social control through their asymmetrical power over consumer data."[35] The incorporation of behavioral economics into marketing strategies illustrates this power. Firms use the information collected and insights gleaned to identify consumers' cognitive and affective susceptibilities.[36] This subsequently allows advertisers to target advertisements in a way and at a time when consumers are their most susceptible.[37] Political actors have further used and abused the advertising interface in similar ways for political gain.[38]

---

[31] *See, e.g.*, Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995, 1003–04 (2014); Susser, Roessler & Nissenbaum, *supra* note 5, at 14.

[32] *See generally* ZUBOFF, *supra* note 5.

[33] *See* Jonathan R. Mayer & John C. Mitchell, *Third-Party Web Tracking: Policy and Technology*, 2012 IEEE SYMP. ON SEC. & PRIV. PROC. 413, 415 (2012).

[34] *See, e.g.*, Charles Duhigg, *How Companies Have Learned Secrets*, N.Y. TIMES (Feb. 16, 2012), https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html [https://perma.cc/SV29-KYWJ]; *See generally* Alicia Solow-Niederman, *Information Privacy and the Inference Economy*, 117 NW. U. L. REV. 357, 359–68 (2022) (detailing the inference economy).

[35] Anthony Nadler & Lee McGuigan, *An Impulse to Exploit: The Behavioral Turn in Data-Driven Marketing*, 35 CRIT. STUD. MEDIA COMM'N 151, 151 (2018).

[36] *See id.*

[37] *See id.*

[38] ANTHONY NADLER, MATTHEW RAIN & JOAN DONOVAN, WEAPONIZING THE DIGITAL INFLUENCE MACHINE: THE POLITICAL PERILS OF ONLINE AD TECH, DATA, & SOC'Y 27–38 (2018).

Design choices in user interfaces have also amplified firms' capacities to mold user decisions to their liking. As many have written, they do so by constructing choice architectures that obscure the full range of available options and/or hamper users' efforts to act on their actual preferences.[39] Further, because these designs may also use Big Data, they create a choice environment to personalize our decision-making contexts.[40]

Daniella DiPaola and Ryan Calo linked these ideas to what they term "socio-digital vulnerability," which is the "susceptibility of individuals and groups within mediated environments to decisional, social, or constitutive interference."[41] In their view, problematic treatment of data, social robots, and interface designs have reconfigured the way we form and act on our preferences, our social interactions, and fundamental notions of selfhood.[42] Socio-digital vulnerability is then the umbrella term to encapsulate these harms.[43]

But data flows and design interfaces are just two *features* of digital environments that firms leverage. How they can be executed depends on the character of the environments themselves and their affordances. Karen Levy and Solon Barocas identified platforms as sites that can structure discriminatory interactions because of their role in designing encounters.[44] More recently, Julie Cohen examined the role of "platformized systems."[45] Taking an infrastructural lens, she argued that platforms function as infrastructures that "facilitate, undergird, shape, and normalize the conditions of possibility for human activity over spaces and across scales."[46] In doing so, platforms configure the very form that online communication can take. Optimization algorithms, for instance, modulate users' content feeds according to their preferences, which could be either independently formed or artificially shaped to satisfy the

---

[39] *See generally* Jamie Luguri & Lior Jacob Strahilevitz, *Shining A Light on Dark Patterns*, 13 J. LEGAL ANALYSIS 43 (2021) (evidencing the power of dark patterns).

[40] Karen Yeung, *'Hypernudge': Big Data as a Mode of Regulation by Design*, 20 INFO., COMMC'N & SOC'Y 118 (2017); *see also* Daniel Susser, *Invisible Influence: Artificial Intelligence and the Ethics of Adaptive Choice Architectures*, 2019 AAAI/ACM CONF. ON AI, ETHICS, AND SOC'Y PROC. 403 (2019) (detailing the use of artificial intelligence and machine learning to tailor choice architectures to users).

[41] Danielle DiPaola & Ryan Calo, *Socio-Digital Vulnerability*, https://ssrn.com/abstract=4686874 [https://perma.cc/4MEF-RLCS].

[42] *Id.* at 10.

[43] *Id.*

[44] Karen Levy & Solon Barocas, *Designing Against Discrimination in Online Markets*, 32 BERKELEY TECH. L.J. 1183, 1203 (2017).

[45] *See generally* Cohen, *Infrastructuring*, *supra* note 10.

[46] *Id.* at 16.

engagement imperative.[47] Software development kits condition app development on data exchanges formatted according to standardized protocols.[48] And advertising dashboards, which platforms control, auction ad placements based on proprietary data analytics, thereby determining which ads are fed to which users.[49]

In the following Section, I sketch out other ways that platforms structure and circumscribe the modes of online communication available to us. Attention to the environments reveals that threats to autonomy—the imposition of vulnerability via threats to relational autonomy—begins *before* data flows and *before* choice architectures nudge. They begin at the very construction of data and of choices available to us. In this respect, while improper data flows and manipulative choice architectures make up a set of layers of imposed vulnerability, platformized environments make up another.

B. COOKING THE DATA: PLATFORMS AS ARCHITECTS OF THE INFORMATION ECONOMY

In *The Politics of 'Platforms*,*'* Tarleton Gillespie offered a discursive treatment of the term "platform." The term's various connotations expose its functions and contributions. On one view, platforms trumpet themselves as neutral loci of exchange and communication. Facebook, for example, connects users to each other, as well as users to web developers; YouTube bridges content creators to viewers; Amazon links businesses to customers. In this way, platforms have a place in addressing our baseline vulnerabilities.[50] Another view presents platforms not as mere intermediaries but as agents in their own right.[51] Their methods of "facilitating" encounter are imbued with underlying logics that serve their own interests. YouTube connects users to the extent that it can

---

[47] *Id.* at 17–18.

[48] *Id.* at 21–22.

[49] *Id.* at 22–25.

[50] *See also* Jessica N. Fish, Lauren B. McInroy, Megan S. Paceley, Natasha D. Williams, Sara Henderson, Deborah S. Levine & Rachel N. Edsall, *"I'm Kinda Stuck at Home With Unsupportive Parents Right Now": LGBTQ Youths' Experience with COVID-19 and the Importance of Online Support*, 67 J. ADOLESCENT HEALTH 450 (2020) (highlighting the role of social in offering in online support to LGBTQ youth); Claire Cain Miller, *For One Group of Teenagers, Social Media Seems a Clear Net Benefit*, N.Y. TIMES (May 24, 2023), https://www.nytimes.com/2023/05/24/upshot/social-media-lgbtq-benefits.html [https://perma.cc/U7FK-TGTE].

[51] Tarleton Gillespie, *The Politics of 'Platforms*,' 12 NEW MEDIA & SOC'Y 347, 352–55 (2010).

leverage such connections to maximize advertising revenue,[52] and Facebook links web developers to users to the extent that they allow for further collection and centralization of external web data.[53] Relatedly, they also police and constrain those encounters to eschew or resist regulatory scrutiny.[54]

This Section dissects the latter view and the related body of work. It draws on science and technology studies to examine how the architectural work of platforms might extend past meeting our baseline vulnerabilities. Excavating the embedded social processes illustrates platforms' potential contributions to imposed vulnerability. More precisely, their participation in datafication and interoperability systems structure—and circumscribe—the relationships we can have with others. The upshot is that we may be rendered excessively dependent on platform affordances for the development and exercise of our relational autonomy.

1. *Datafication of Behavior*

Start with datafication. As scholars have mentioned, platforms have engaged in a massive project of commercial surveillance and transformation of human activity into monetizable data at an unprecedented scale.[55] Critically, the obtained data is not "raw" data that present users as digitized clones of their offline selves. Rather, data comes "cooked" by normative and cultural judgments.[56] It is

---

[52] *See id.* at 353.

[53] Anne Helmond, *The Platformization of the Web: Making Web Data Platform Ready*, SOC. MEDIA + SOC'Y, 1 (2015).

[54] *See* Katharine Trendacosta, *Unfiltered: How YouTube's ContentID Discourages Fair Use and Dictates What We See Online*, ELEC. FRONTIER FOUND. (Dec. 10, 2020), https://www.eff.org/wp/unfiltered-how-youtubes-content-id-discourages-fair-use-and-dictates-what-we-see-online [https://perma.cc/H3UV-EDU6] (illustrating how YouTube's automated copyright filter has "replaced legal fair use of copyrighted material with its own rules"); Josh Taylor & AAP, *Facebook Shuts News Tab After Meta Vows to Stop Paying Australian Publishers for Content*, THE GUARDIAN (Apr. 1, 2024, 7:53 PM), https://www.theguardian.com/media/2024/apr/02/facebook-shuts-news-tab-after-meta-vows-to-stop-paying-australian-publishers-for-content [https://perma.cc/L353-GME2]; *see also* ÁNGEL DÍAZ & LAURA HECHT-FELELLA, BRENNAN CTR. FOR JUSTICE, DOUBLE STANDARDS IN SOCIAL MEDIA CONTENT MODERATION 3 (2021) (detailing how social media platforms regulate content to "facilitate a favorable regulatory environment," resulting in disparate impacts on marginalized groups).

[55] *See supra* Part II.A.

[56] JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM 64 (2019); *see* LISA

filtered by the choices of categorization, measurement, and storage that system designers make.[57]

But datafication is premised on something more than methods of data cleaning. Datafication operates on *human activity*; it acts as behaviorists, taking only tangible behavior as input. In doing so, it conflates selfhood with its material manifestations. It collects behavioral and physiological data and aggregates the information to presumably shed light on our mental states. Our preferences are defined by the webpages we click and the amount of time we spend on them. The strength of our relationships is determined by the time we spend on others' profiles. And our thought processes are reflected in our search history. In 2017, as Facebook itself stated, "[b]y monitoring posts, pictures, interactions, and internet activity in real-time, [the company] [could] work out when young people feel 'stressed', 'defeated', 'overwhelmed', 'anxious, 'nervous', 'stupid', 'silly', 'useless', and like a 'failure.'"[58]

Scholarship and commentators have tended to adopt language that entrenches this presumption. Datafication, as they explain, is the quantification of the entirety of human life.[59] Large-scale commercial surveillance collects personal information that encompasses the totality of the self.[60] In this way, firms know us perhaps better than we ourselves do.[61]

Behaviorism, however, offers only a simplified account of the self. Indeed, it had long been debated in literatures in psychology, communication studies, and philosophy of mind. Evaluating the behaviorist argument, these literatures have concluded that our behaviors are not coextensive with our mental states, nor can our

---

GITELMAN & VIRGINIA JACKSON, "RAW DATA" IS AN OXYMORON 2 (Lisa Gitelman, ed., MIT Press 2013).

[57] COHEN, *supra* note 56, at 64.

[58] Michael Nunez, *Facebook Handed Over Data on 'Insecure' and 'Overwhelmed' Teenagers to Advertisers*, GIZMODO (May 1, 2017), https://gizmodo.com/facebook-handed-over-data-on-insecure-and-overwhelmed-t-1794800092 [https://perma.cc/RV84-5YLG].

[59] Ulises A. Mejias & Nick Couldry, *Datafication*, 8 INTERNET POL'Y REV., 1 (2019).

[60] *See, e.g.*, Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934 (2013) (describing surveillance as "total"); Sarah Myers West, *Data Capitalism: Redefining the Logics of Surveillance and Privacy*, 58 BUS. & SOC'Y 20, 21 (2019) ("Nearly every routine aspect of our lives today produces a digital trace...").

[61] James Carmichael, *Google Knows You Better Than You Know Yourself*, THE ATLANTIC (Aug. 19, 2014), https://www.theatlantic.com/technology/archive/2014/08/google-knows-you-better-than-you-know-yourself/378608/ [https://perma.cc/9FZV-YCHY].

mental states be defined solely in terms of our behavioral dispositions.[62] Accordingly, a prevailing functionalist view has emerged that mental states, consciously or subliminally, scaffold behavior rather than the other way around.[63] Mental states do not map onto behaviors by a one-to-one ratio, such that different individuals may behave in the same way yet hold different mental states.[64]

These ideas are not foreign to the law, which has long recognized the divergence between behavior and mental states and that selfhood is a composite, however arranged, of the two. We see this in the acknowledgment of mixed motives in antidiscrimination law, different *mens rea* standards in criminal law, and negligence and intentional torts as separate legal actions. What is clear from this brief synthesis is that our behaviors are not equivalent to our mental states, nor are they necessarily capable of shedding light on our mental states.

By building digital profiles based on our behavioral patterns, platforms return us to the behavioral view. Three corollaries follow from this. First, partiality towards quantified representations diminishes, if not eliminates, the subjective, narrative form as an epistemic tool. By defining us in terms of quantifiable, discrete acts, platforms blur the distinctions between causal and correlative relationships for our behavior, as well as those between justificatory and explanatory reasons. They also collapse the multiple reasons that may exist for a given set of behaviors. However, because our mental states and phenomenological experiences are not completely reducible to behavior, they are excluded from our digital personas.[65]

Consider Facebook's Like button. The button was introduced in 2009 as a shortcut for users to succinctly engage with online content.[66] Its popularity was evident: four years later, there were 4.5

---

[62] *See generally* Hillary Putnam, *The Meaning of 'Meaning,'* 2 MIND, LANGUAGE AND REALITY 131 (1975); Ned Block & Jerry Fodor, *What Psychological States Are Not*, 81 PHILOSOPHICAL REV. 159 (1972); Marshall H. Segall, Walter J. Lonner & John W. Berry, *Cross-Cultural Psychology as a Scholarly Discipline: On the Flowering of Culture in Behavioral Research*, 53 AM. PSYCHOLOGIST, 1101 (1998).

[63] For a brief overview of functionalism, see Thomas Polger, *Functionalism*, INTERNET ENCYC. PHIL. https://iep.utm.edu/functism/ [https://perma.cc/6HFJ-JR62].

[64] *Id.*

[65] I am not arguing that behavior is not relevant at all to our self-constitutions, only that behavior is not our complete self-constitutions.

[66] Carolin Gerlitz & Anne Helmond, *The Like Economy: Social Buttons and the Data-Intensive Web*, 15 NEW MEDIA & SOC'Y 1348, 1352 (2013).

billion likes per day.[67] The ambiguity of the icon, however, leaves open a mix of uses. One study found a range of motives for clicking the Like button, such as genuinely liking the post's content, acknowledging that the user viewed the post, signaling social support for the author, and storing the post for later retrieval.[68] Another concluded that Liking behavior was tied to goals, such as maintaining social ties and preserving self-presentation.[69] Yet this array of motives is not captured by the phatic nature of the Like button.

Second, what behavior is collected is contingent on the language made available by the platforms. For example, in 2016, Facebook rolled out new reactions, including "love," "haha," "wow," "sad," and "angry," users could use in addition to the Like button.[70] What was *not* added was the "yay" and "confused" responses.[71] In a blog post, Facebook explained that its omission of "yay" and "confused" was informed in part because they were difficult to internationalize, and more reactions would make consumption of content on the News Feed more difficult.[72] Users were thus confined to expressing emotions online to the extent that those emotions comported with what Facebook deemed permissible.[73]

---

[67] Josh Constine, *Facebook's Growth Since IPO In 12 Big Numbers*, TECHCRUNCH (May 17, 2013, 1:43 PM), https://techcrunch.com/2013/05/17/facebook-growth/?guccounter=1 [https://perma.cc/S62K-F7JG].

[68] *See* Rebecca A. Hayes, Caleb T. Carr & Donghee Yvette Wohn, *One Click, Many Meanings: Interpreting Paralinguistic Digital Affordances in Social Media*, 60 J. BROADCASTING & ELEC. MEDIA 171, 178–79 (2016).

[69] Erin M. Sumner, Luisa Ruge-Jones & Davis Alcorn, *A Functional Approach to the Facebook Like Button: An Exploration of Meaning, Interpersonal Functionality, and Potential Alternative Response Buttons*, 20 NEW MEDIA + SOC'Y 1451, 1459–61 (2017); *see also* Jiyoung Chae, *Explaining Females' Envy Toward Social Media Influencers*, 21 MEDIA PSYCHOLOGY 246 (2018) (comparing the use of social media for relevant practical information with its use for social comparison).

[70] Casey Newton, *Facebook Rolls Out Expanded Like Button Reactions Around the World*, THE VERGE (Feb. 24, 2016, 8:00 AM), https://www.theverge.com/2016/2/24/11094374/facebook-reactions-like-button [https://perma.cc/V4A8-2848].

[71] *See id.*

[72] Geoff Teehan, *Reactions: Not Everything in Life Is Likable*, DESIGN AT META (Feb. 24, 2016), https://medium.com/designatmeta/reactions-not-everything-in-life-is-likable-5c403de72a3f [https://perma.cc/W9T4-8E2J].

[73] *See also* Pamela Wisniewski, Karla Badillo-Urquiola, Zahra Ashtorab & Jessica Vitak, *Happiness and Fear: Using Emotions as a Lens to Disentangle How Users Felt About the Launch of Facebook Reactions*, 3 ACM TRANS. SOC. COMPUT. 1 (2020) (finding that the new reactions

Third, algorithms program our behavioral patterns in a way that prioritizes certain behavior over others. [74] One study found that a "share" weighed around the same as two "comments," and a "comment" weighed around the same as seven "likes."[75] Just one year after it introduced the new reactions, its algorithm weighed the "angry" emoji five times more than its Like button.[76] The justification was that "angry" emojis were more likely to be used in response to controversial posts, which fueled user consumption.[77]

The upshot of the focused attention on our behavior is that datafication restricts the range of available options and thus, imposes vulnerability. Our online decisions are not *ours* per se but are bent by the ways in which platforms limit the realm of possibilities. In particular, they do so by constraining both our own self-representations and our social relationships. On the former, datafication forbids us from deploying narrative, epistemic tools and reduces us to platform-defined permissible behavioral states. The little regard to the subjective mental and phenomenological states that scaffold our behavior in turn leads to misrecognition or nonrecognition of our decisions.

In Facebook's case, as one Facebook spokesperson stated, "[p]eople are placed into interest categories based on their activity on Facebook, including the pages they like or the ads they click on."[78] The effect is that people are pigeonholed as expressing certain interests, such as "telenovela," "cancer awareness," or even "oxygen."[79] While some of these categories may accurately reflect

---

still contained several design constraints, such as the inability of users to express conflicting emotions).

[74] *See also* Cohen, *Infrastructuring*, *supra* note 10, at 17 (discussing optimization algorithms).

[75] Cheonsoo Kim & Sung-Yun Yang, *Like, Comment, and Share on Facebook: How Each Behavior Differs from the Other*, 43 PUB. RELS. REV. 441 (2017), http://doi.org/10.1016/j.pubrev.2017.02.006.

[76] Jeremy B. Merrill & Will Oremus, *Five Points for Anger, One For a 'Like': How Facebook's Formula Fostered Rage and Misinformation*, WASH. POST (Oct. 26, 2021, 1:04 PM), https://www.washingtonpost.com/technology/2021/10/26/facebook-angry-emoji-algorithm/ [https://perma.cc/8SJZ-UHB4].

[77] *Id.*

[78] Colin Lecher, *How Big Pharma Finds Sick Users on Facebook*, THE MARKUP (May 6, 2021, 8:00 AM), https://themarkup.org/citizen-browser/2021/05/06/how-big-pharma-finds-sick-users-on-facebook [https://perma.cc/JSH7-JKJZ]; *see also* Kelly Cotter, Mel Medeiros, Chakyung Pak & Kjerstin Thorson, *"Reach the Right People": The Politics of "Interests" in Facebook's Classification System for Ad Targeting*, BIG DATA & SOC'Y 1, 8 (2021).

[79] Lecher, *supra* note 78; Angie Waller & Colin Lecher, *Facebook Promised to Remove "Sensitive" Ads. Here's What It Left Behind*, THE

the interests and preferences of users, not all do. In Russia, Facebook tagged 65,000 users as having an interest in "treason."[80] And it labeled members and allies of the LGBTQ+ community as having an interest in "transgenderism," a derogatory term used by anti-transgender activists.[81] Although there is little public evidence of how Facebook designates interest categories,[82] what is clear is that it does so irrespective of the reasons underlying those behaviors.

Feeds are then ordered and curated according to what the company thinks of our "interests" based on our behaviors.[83] For example, advertisers targeted a drug to treat a chronic pulmonary disease to those interested in "oxygen" and an ad with a woman in a bikini asking teens if they were "summer ready", to those interested in "extreme weight loss."[84] By curating our feeds according to these interest categories built from our behavior, platforms restrict the sorts of online behaviors available to us at all. The decision to click on those ads are not necessarily *ours* but are imposed by the limited range of options available.

The same can be said of social relationships. Facebook repeatedly recommended political groups, ranging from "Joe Biden Is Not My President," "Philly for Elizabeth Warren," or "Liberty lovers for Ted Cruz" based on interest categories.[85] In one specific

---

MARKUP (May 12, 2022, 9:37 AM), https://themarkup.org/newsletter/citizen-browser/facebook-promised-to-remove-sensitive-ads-heres-what-it-left-behind [https://perma.cc/2NZT-D746].

[80] Marrian Zhou, *Facebook Removes 'Treason' as Keyword for Users' Interests*, CNET (July 11, 2018, 11:31 AM), https://www.cnet.com/tech/tech-industry/facebook-removes-treason-as-keyword-for-users-interests/ [https://perma.cc/QMT2-W6DK].

[81] Cotter, Medeiros, Pak & Thorson, *supra* note 78, at 8.

[82] Lecher, *supra* note 78.

[83] This might extend beyond "interest categories." The Washington Post compiled a list of 98 data points including a user's age, likelihood of engaging in politics, and ownership of a timeshare. Caitlin Dewey, *98 Personal Data Points that Facebook Uses to Target Ads to You*, WASH. POST (Aug. 19, 2016, 10:13 AM), https://www.washingtonpost.com/news/the-intersect/wp/2016/08/19/98-personal-data-points-that-facebook-uses-to-target-ads-to-you/ [https://perma.cc/9DDZ-X6ZJ].

[84] Lecher, *supra* note 78; Eden Gillespie, *Facebook Approves Ad Targeting Teens Interested in "Extreme Weight Loss,'* SBS NEWS (Feb. 22, 2022, 5:26 PM), https://www.sbs.com.au/news/the-feed/article/facebook-approves-ad-targeting-teens-interested-in-extreme-weight-loss/htqzci573 [https://perma.cc/6X29-V4YZ].

[85] Corin Faife & Alfred Ng, *After Repeatedly Promising Not To, Facebook Keeps Recommending Political Groups to Its Users*, THE MARKUP (June 24, 2021, 8:00 AM), https://themarkup.org/citizen-

case, researchers created a fake profile of a person interested in politics, Christianity, and Donald Trump.[86] Two days after "she" joined, she was met with recommendations to join QAnon groups and her feed was filled with a "barrage of extreme, conspiratorial, and graphic content."[87] In both cases, the range of permissible user activity depended on Facebook's decisions to decide what sort of social relationships were available for them to enter into.[88]

The broader consequence is that excessive dependence on platform affordances for our recognition and social participation allows us little opportunity to explore different possibilities for who we might be. By limiting our options based on categories formed by our behavioral dispositions, they foreclose curiosity, experimentation, and play. [89] In turn, that keeps us from the exploration, whether that be exploration that affirms or challenges our preferences; necessary for us to cement our understanding of ourselves.

2. *APIs and Social Plugins*

Platforms also structure our interactions through their interoperability systems. Many platforms rely heavily on partners and third-party developers as channels to extend their services and supercharge their bottom lines.[90] Part of this reliance is executed through application programming interfaces (APIs)—interfaces that

---

browser/2021/06/24/after-repeatedly-promising-not-to-facebook-keeps-recommending-political-groups-to-its-users [https://perma.cc/AF3S-CGB7].

[86] Brandy Zadrozny, *'Carol's Journey': What Facebook Knew About How It Radicalized Users*, NBC NEWS (Oct. 22, 2021, 6:31 PM), https://www.nbcnews.com/tech/tech-news/facebook-knew-radicalized-users-rcna3581 [https://perma.cc/D6G8-D87R].

[87] *Id.*

[88] *See also* Paul Barrett, Justin Hendrix & Grant Sims, *How Tech Platforms Fuel U.S. Political Polarization and What Government Can Do About It*, BROOKINGS INST. (Sept. 27, 2021), https://www.brookings.edu/articles/how-tech-platforms-fuel-u-s-political-polarization-and-what-government-can-do-about-it/ [https://perma.cc/5HHS-4S5H].

[89] *See also* Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1425 (2000) ("The opportunity to experiment with preferences is a vital part of the process of learning, and learning to choose, that every individual must undergo."); JULIE E. COHEN, *Reimagining Privacy, in* CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY PRACTICE (2012) (framing privacy as the ability of individuals and communities to evolve subjectivities).

[90] *See* Helmond, *supra* note 53.

facilitate communication and interaction between the application and a platform—and social plugins—social buttons that developers can add to their website.[91] These tools are crucial to platforms and their technological and economic growth. They cross-fertilize resources to allow developers to build on top of platforms, while expanding the reach of platforms' functionalities.

First, APIs open up the exchange of data between third-party applications and the platforms but do so as "boundary resources."[92] In particular, they police both the scope and nature of what data is included. As to scope, platforms decide what applications can access the APIs. The power to do so gives platforms leverage to stymie opportunities available to their rivals, while enhancing those of their partners.[93] For example, there have been many documented instances in which Meta denied API access to entities it considered rivals. In 2013, Meta shut down API access to Vine, an emerging rival in video-sharing services.[94] In the same year, it blocked access to other social networks, such as Path[95] and Circle,[96] and messaging services, such as MessageMe and Voxer.[97] Further, between 2011 and 2018, Meta allegedly limited use of its APIs solely to developers who agreed to not develop competing products or promote competitors.[98]

As to nature, platforms structure the lexicon of the ecosystem that developers build on. By exposing slivers of their underlying architecture, they demand that developers conform to the permissible

---

[91] AMRIT TIWANA, PLATFORM ECOSYSTEMS: ALIGNING ARCHITECTURE, GOVERNANCE, AND STRATEGY 6 (2014); Gerlitz & Helmond, *supra* note 66, at 1352.

[92] Ahmad Ghazawneh & Ola Henfridsson, *Balancing Platform Control and External Contributions in Third-Party Development: The Boundary Resources Model*, 23 INFO. SYS. J. 173 (2013).

[93] *See* Robert Bodle, *Regimes of Sharing: Open APIs, Interoperability, and Facebook*, 14 INFO., COMMC'N & SOC'Y 320, 322–23 (2011).

[94] Mark Scott, *Documents: Zuckerberg Allegedly Blocked Rivals from Accessing Facebook Data*, POLITICO (Dec. 5, 2018, 5:35 PM), https://www.politico.eu/article/mark-zuckerberg-six4three-facebook-data-damian-collins-internal-documents/ [https://perma.cc/NE68-Z5AW].

[95] Josh Constine & Mike Butcher, *Facebook Blocks Path's "Find Friends" Access Following Spam Controversy*, TECHCRUNCH (May 4, 2013, 6:04PM), https://techcrunch.com/2013/05/04/path-blocked/ [https://perma.cc/9MEW-ZRSP].

[96] Complaint, Fed. Trade Comm'n v. Facebook, Inc., No. 20-03590, at 154 (D.D.C. Jan. 13, 2021) [hereinafter Facebook Complaint].

[97] Kim-Mai Cutler, *Facebook Brings Down The Hammer Again: Cuts Off MessageMe's Access to its Social Graph*, TECHCRUNCH (Mar. 16, 2013, 12:20 AM), https://techcrunch.com/2013/03/15/facebook-messageme/ [https://perma.cc/R6H3-QDXV].

[98] Facebook Complaint, *supra* note 96, at 136.

interactions.[99] In this way, platforms choreograph the social relations enabled by the applications built atop them: standardized protocols, shared with developers, are used to attract them to the platform's ecosystem.[100] One example is Facebook's use of Open Graph. Open Graph is a protocol that standardizes data formats on the web, such that external web pages organize their information in the same way Facebook does.[101] By doing so, companies can integrate user activity on those pages to Facebook's own social graph, which is a representation of users and their connections to other users and objects on Facebook.[102] As such, platforms "decentralize data production"[103] while modulating the activity of the developers.

Social Plugins, such as the Like button, do similar architectural work. Now distributed across the Internet, the Like button can be placed to advertised products, recipe pages, dating apps, and YouTube videos. The button exchanges formatted data between the developer and the platform.[104] The consequence is that as the button creates *more* data—e.g., about the number of hits, and demographic data on the likers—that new data is transmitted back to Facebook.[105]

The connection to vulnerability is clear. Platforms impose vulnerability via their APIs and social plug-ins. What user data is collected depends on the platform's own competitive interests. In Facebook's case, consumer behaviors on competitor sites, having been cut off, are precluded from informing the options available to users. For example, Path was designed as a social media platform for users' closest fifty friends.[106] Presumably, because of the narrower social graphs, users would be less susceptible to pressures of self-presentation (or at least, susceptible to qualitatively different types

---

[99] *See* Fernando N. Van der Vlist, Anne Helmond, Marcus Burkhardt & Tatjana Seitz, *API Governance: The Case of Facebook's Evolution*, SOC. MEDIA + SOC'Y 1, 3–5 (2022).

[100] *See* Bodle, *supra* note 93, at 325.

[101] Van der Vlist et al., *supra* note 99, at 11; *see A Guide to Sharing for Webmasters*, META FOR DEVELOPER, https://developers.facebook.com/docs/sharing/webmasters/ [https://perma.cc/E4MW-BV2S]. For a deeper dive into Open Graphs, *see The Open Graph Protocol*, https://ogp.me/ [https://perma.cc/33HY-VP4P].

[102] Gerlitz & Helmond, *supra* note 66, at 1352.

[103] Helmond, *supra* note 53, at 5.

[104] *See* Gerlitz & Helmond, *supra* note 66, at 1352.

[105] *Id.* at 1353.

[106] Mike Isaac, *New Social Network Path = iPhone + Instagram + Facebook – 499,999,950 Friends*, FORBES (Nov. 14, 2010, 9:49 PM), https://www.forbes.com/sites/mikeisaac/2010/11/14/new-social-network-path-iphone-instagram-facebook-499999950-friends/?sh=71699cdd48e9 [https://perma.cc/Q4DN-XZCV].

of pressures).[107] Thus, the activity a user would be involved in on Path might be different from what they would engage in on Facebook. However, that activity on Path would not be used to inform interest categories which in turn structure the available behavior.

Similarly, such interoperability systems illustrate the limits of behavioral data[108] on third-party sites and applications. They dictate what types of behavior are accessible in accordance with their own interests and forbid non-conforming behaviors, making users dependent on what those APIs and social plug-ins are designed to permit. As users move through the Internet, much of which is connected to Facebook, they are limited to the language provided by Facebook. In turn, the data that flows from those sites and applications, which necessarily conform to Facebook's own standardized protocol, are used to constrain the range of options available on the service itself.

***

Platforms are hardly mere intermediaries or facilitators of encounter. Nor are they only responsible for what many have called manipulative data flows and choice architectures that threaten autonomy. Instead, what encounters are permissible for users—and thus, what social relations we may have and the bases of those relations—are contingent on the decisions made by platforms.

III. PLATFORMIZATION AS AN UNFAIR ACT

The work done by the conceptual shift from autonomy to imposed vulnerability in Part I is important because it poses the harm as one that the law has recognized as meriting legal protection. Yet, imposed vulnerability by platforms cannot be solved by an isolated or discrete area of law. It demands the symbiotic work of multiple areas of law. This Part considers one proposal: the Federal Trade

---

[107] *See also* Michael A. DeVito, Jeremy Birnholtz & Jeffrey T. Hancock, *Platforms, People, and Perception: Using Affordances to Understand Self-Presentation on Social Media*, PROC. ACM CONF. ON COMPUT. SUPPORTED COOPERATIVE WORK AND SOC. COMPUT. 740 (2017) (detailing different self-representation strategies across different social media); Xiaoyun Huang & Jessica Vita, *"Finsta Gets All My Bad Pictures": Instagram Users' Self-Presentation Across Finsta and Rinsta Accounts*, 6 PROC. ACM HUM.-COMPUT. INTERAC. 1 (2022) (same but within the same social media platform). *See generally* Erving Goffman, *Presentation of Self in Everyday Life*, *in* THE PRESENTATION OF SELF IN EVERYDAY LIFE 17–25 (1959).

[108] *See supra* Part II.B.1.

Commission's authority to regulate "unfair or deceptive acts or practices." Part III.A offers a brief discussion of the appeal of the Commission. The remaining Sections detail how the Commission's statutory authority may or may not be able to address the conduct described above.

A. WHY THE FTC

At the moment, scholars across many fields have considered proposals ranging from robust privacy laws to bolstering antitrust protections. Privacy, however, has traditionally focused on the flows of data rather than how data itself is made.[109] Antitrust is promising, particularly with respect to the exclusionary tactics platforms use to edge out rivals.[110] However, whether antitrust actualizes this promise turns on the success of calls to shift antitrust goals from consumer welfare to market structure and power.[111]

Privacy and antitrust laws must continue to evolve. However, in the meantime, because the Commission has sought an expansive interpretation of its unfairness authority, such authority requires further legal analysis. Under Section 5, "unfair …acts or practices… are… unlawful."[112] A practice is "unfair" if it 1) "causes or is likely to cause substantial injury to consumers," 2) "which is not reasonably avoidable by consumers themselves," and 3) "not outweighed by countervailing benefits to consumers or to competition."[113]

The unfairness authority is a likely place to look to for several reasons. First, the Commission has often used this authority to respond to challenges brought by new technologies and harms.[114] In recent years, the Commission has pursued enforcement actions and suits related to technologies, such as facial recognition, dark patterns, and artificial intelligence.[115] Second, its authority has often been

---

[109] *See, e.g.*, Salomé Viljoen, *A Relational Theory of Data Governance*, 131 YALE L.J. 573 (2021).

[110] *See, e.g.*, Facebook Complaint, *supra* note 96.

[111] *See also* Lina M. Khan, Note, *Amazon's Antitrust Paradox*, 126 YALE L.J. 710 (2017).

[112] 15 U.S.C. § 45.

[113] *Id.* § 45(n).

[114] *See also* Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 2230, 2276–89 (2014).

[115] *See, e.g.*, Complaint, Fed. Trade Comm'n v. Rite Aid Corp., No. 2:23-cv-5023 (E.D. Pa. Dec. 19, 2023) (facial recognition); Complaint for Permanent Injunction, Civil Penalties, Monetary Relief, and Other Equitable Relief, Fed. Trade Comm'n v. Amazon.com, Inc., No. 2:23-cv-

lauded as flexible and nimble to cover a host of challenges, ranging from cybersecurity to data protection to discrimination.[116] Indeed, that "unfair" is meant to encompass a broad swathe of activity is evident from the House's Report that the Commission—not Congress—was better positioned to identify unfair practices.[117] And as Woodrow Hartzog and Daniel Solove noted, the common thread through the Commission's use of its unfairness authority has been to go after "those who would seek to unfairly manipulate parties by exploiting inherent biases and vulnerabilities."[118]

Further, in 2022, the Commission announced an Advanced Notice of Proposed Rulemaking (ANPR) on commercial surveillance and data security, indicating its interest in tackling questions peripheral to imposed vulnerability.[119] The notice specifically posed questions about consumer manipulation.[120] The rules approach has benefits over a common law approach: it creates more predictability and minimizes uncertainty for companies.[121] Still, even if the rule does not tackle the social processes embedded

---

0932 (W.D. Wa. June 21, 2023); Complaint, *In re* Rytr LLC, No. 232-3052 (Sept. 25, 2024) (artificial intelligence).

[116] *See, e.g.*, Fed. Trade Comm'n v. Wyndham, 799 Fed.3d 237 (3d Cir. 2015) (cybersecurity); Fed. Trade Comm'n v. Kochava Inc., 671 F. Supp. 3d 1161 (D. Idaho 2023) (data security); *see also* Andrew D. Selbst & Solon Barocas, *Unfair Artificial Intelligence: How FTC Intervention Can Overcome the Limitations of Discrimination Law*, 171 U. PA. L. REV. 1053 (2023) (offering a roadmap for the Commission to apply its unfairness authority to algorithmic discrimination) [hereinafter Selbst & Barocas, *Unfair Artificial Intelligence*].

[117] *See* Fed. Trade Comm'n v. R.F. Keppel & Bro. Inc., 291 U.S. 304, 310 n.1 (1934) (citing H.R. REP. NO. 63-1142, at 19 (1914) (Conf. Rep.)) ("It is impossible to frame definitions which embrace all unfair practices… If Congress were to adopt the method of definition, it would undertake an endless task."); *see also* Order Denying Respondent LabMD's Motion to Dismiss at 1–2, LabMD, Inc., FTC Docket No. 9357, 2014 WL 253518 (F.T.C. Jan. 16, 2014) ("Congress, in enacting Section 5(n), confirmed its intent to allow the Commission to continue to ascertain, on a case-by-case basis, which specific practices should be condemned as 'unfair.'").

[118] Hartzog & Solove, *supra* note 114, at 2250 (detailing the types of activities the Commission has deemed "unfair").

[119] Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51273 (proposed Aug. 22, 2022) (to be codified at 16 C.F.R. ch. 1).

[120] *See id.* at 51281-2, 51287. It focused these questions on children and teenagers, the prototypical archetype of vulnerable populations, but as Part I argued, framed as layers of ontological conditions and social arrangements, vulnerability affects *everyone*.

[121] *Id.* at 51276.

in datafication and interoperability as affirmatively unfair conduct, the Commission still has another route to enforcing its unfairness authority through the common law. The subsequent Sections discuss how direct enforcement of Section 5 both presents challenges and offers a pathway to address surplus vulnerability as caused by platforms.

B. SUBSTANTIAL INJURY

The first element looks to whether the conduct "causes or is likely to cause substantial injury to consumers." The conduct need not be the sole cause of injury; it is enough that firms facilitate injurious activity[122] or "create a significant risk of concrete harm."[123] To determine whether a harm is cognizable, Section 5(n) looks to consumer injury and public policy.[124]

1. *Consumer Injury*

Historically, consumer injury has been recognized as referring primarily to economic or health and safety harms.[125] Emotional and more intangible harms are comparatively rarely recognized and as the Unfairness Statement, which is treated as Section 5's legislative history, stated, they may form a basis for an unfairness finding only in extreme cases.[126] In this way, due to its intangible nature, an argument that imposed vulnerability on its own is a consumer injury cognizable under Section 5 is unlikely to get off the ground.

However, the direct argument of imposed vulnerability as consumer injury is not the only path to finding Section 5 liability, and it is worth exploring how more creative arguments may fare. One line of cases adds flesh to the definition of consumer injury, holding that consumer injury may include transaction costs arising from inefficient markets. In *FTC v. Zuccarini*, for example, the

---

[122] Fed. Trade Comm'n v. Neovi, Inc., 604 F.3d 1150, 1156 (9th Cir. 2010).

[123] Fed. Trade Comm'n v. Kochava Inc., 671 F. Supp. 3d 1161, 1172 (D. Idaho 2023).

[124] LabMD, Inc. v. Fed. Trade Comm'n, 894 F.3d 1221, 1229 n.24 (11th Cir. 2018).

[125] *In re* Int'l Harvester Co., 104 F.T.C. 949, 1984 WL 565290, at *1073 (FTC Dec. 21, 1984).

[126] FED. TRADE COMM'N, COMMISSION STATEMENT OF POLICY ON THE SCOPE OF THE CONSUMER UNFAIRNESS JURISDICTION 1075 (1980), *reprinted in In re* Int'l Harvester Co., 104 F.T.C. 949, 1073 n.16 (1984) [hereinafter UNFAIRNESS POLICY STATEMENT].

Commission sued Zuccarini for "mousetrapping."[127] Zuccarini would register misspellings of other domain names and redirect consumers to his website when they typed in the misspellings.[128] Once there, he would obstruct consumers' ability to exit the sites, while flooding them with ads for online gambling, instant credit, and pornography.[129] The Commission argued that the obstruction of consumers from exiting the ads, which resulted in transaction costs such as Internet connection fees, lost time, and lost data, was a substantial injury.[130]

The Commission's other actions have also shed light on other aspects of Section 5's text of "substantial injury to consumers." In particular, injuries may be aggregated across several individuals to determine whether the sum rises to a "substantial" injury.[131] In *Zuccarini*, the Commission noted that while each consumer suffered individual harm, the defendant's practices ultimately "prevent[ed] consumers [in the aggregate] from locating the Web sites they desire to visit."[132]

Further, the Commission has also signaled an interpretation of Section as including harms to consumers as a class rather than solely the aggregation of individual consumers. In *In re Napleton Automotive Group Commission*, in addition to noting the harms of travel costs and lost economic opportunities, the Commission also called discrimination based on protected status as a substantial injury.[133] Its recognition of discrimination as an injury is significant: it marks a shift from a focus on individualized harms to harms imposed on a class of people. Indeed, in support of its assertion, it cites to numerous studies documenting racial disparities in economic opportunities and health consequences.[134]

Putting these principles together, the argument would be that consumers as an entity and in the aggregate may be harmed because platforms' practices of constructing data contribute to market

---

[127] *See* Fed. Trade Comm'n v. Zuccarini, No. 01-4854 (E.D. Pa. 2001).

[128] *Id.* at 15, 17–20.

[129] *Id.* at 16.

[130] *Id.* at 24–31, 39–40.

[131] Dennis D. Hirsch, *From Individual Control to Social Protection: New Paradigms for Privacy Law in the Age of Predictive Analytics*, 79 MD. L. REV. 439, 483 (2020).

[132] *Zuccarini*, *supra* note 127, at 36.

[133] *In re* Napleton Auto. Grp., No. 2023195, 2022 WL 1039797, at *3 (F.T.C. Mar. 31, 2022)

[134] *Id.* at *3 n.9; *see also* Selbst & Barocas, *Unfair Artificial Intelligence*, *supra* note 116, at 1053–54 (arguing that reading "consumers" as a body rather than an aggregation of consumers allows us to distinguish between the social standing of a group and individualized, dignitary harms, and that the former constitutes "substantial injury").

manipulation.[135] Platforms may display products or information that do not match the genuine desires of the consumers.[136] Yet, by restricting the options available on the basis of our behaviors, APIs, and social plug-ins, which create conditions of imperfect information, consumers may overestimate the benefit of a given product or information. This phenomenon exacts transaction costs by artificially inflating demand and increasing the price.[137] Further, in cases where consumers are aware of such effects and seek to avoid them, they would have to expend more resources to find their desired products or information—again, levying transaction costs in the form of Internet connection fees, lost time, and lost data.[138]

The argument, however, is not without its challenges. One challenge cuts against the assumption that the choices made available do not match the genuine desires of consumers. In fact, the entire goal of targeted advertising is to target consumers with advertisements that would pique their interests and desires. As such, as at least one economist has argued, targeted ads actually reduce search costs and improve match quality, which in turn would lower transaction costs. However, that argument is premised on a fixed self, such that search costs and match quality lower transaction costs to the extent that they comport with a self that makes decisions and judgments independent of the advertising.

A second related and perhaps larger challenge is the difficulty of identifying the point at which platforms contribute to our baseline vulnerabilities, such that they cultivate our relational autonomies, and at which they impose vulnerability. As noted above, platforms have a place in addressing our baseline vulnerabilities, especially in connecting vulnerable communities such as LGBTQ+ teenagers with unsupportive parents.[139] At the same time, they may also lead to advertisers targeting members and allies of the LGBTQ+ community with transphobic content because platforms have tagged them as expressing an interest in "transgenderism."[140]

---

[135] *See* Calo, *supra* note 31.

[136] *See* Oren Bar-Gill, Cass R. Sunstein & Inbal Talgam-Choen, *Algorithmic Harm in Consumer Markets*, 15 J. LEGAL ANALYSIS 1, 20 (2023).

[137] *See id.* at 3, 17–18. There are also arguments that targeted advertising reduces search costs and improved match quality, which might lower transaction costs. Yan Lau, *A Brief Primer on the Economics of Targeted Advertising*, FED. TRADE COMM'N (2020), https://www.ftc.gov/system/files/documents/reports/brief-primer-economics-targeted-advertising/economic_issues_paper_-_economics_of_targeted_advertising.pdf [https://perma.cc/TS8P-GSKQ].

[138] *See* Calo, *supra* note 31, at 1027.

[139] *See* Miller, *supra* note 50, at 2.

[140] *See* Cotter, Medeiros, Pak & Thorson, *supra* note 78, at 8.

The hurdle for the Commission will then be to find the fine line between the two and define the market tightly and precisely. Substantial injury must entail the harms of imposed vulnerability but exclude the benefits reaped from platforms' contributions to our baseline vulnerabilities. As further detailed below, this goes hand in hand with a precise definition of the offending conduct.

2. *Public Policy*

Public policy also informs the harms cognizable under the Commission's authority, and examination of Section 5's legislative history sheds light on the precise role public policy can play. In 1964, the Commission defined a practice as "unfair" if it 1) "offend[ed] public policy as established by statutes, the common law, or otherwise," 2) was "immoral, unethical, oppressive, or unscrupulous," and 3) "cause[d] substantial injury to consumers."[141] The Supreme Court nodded to these factors approvingly in a footnote,[142] which incentivized the Commission to issue a "series of rulemakings relying upon… newly found theories of unfairness… based entirely upon the individual Commissioner's personal values."[143] This breadth of authority prompted outrage, and Congress went so far as to refuse to reauthorize the Commission for fourteen years.[144]

In 1980, the Commission adopted the Unfairness Policy Statement. The Statement articulated Section 5's three-prong test, reflecting the Commission's shift from the previous three considerations to focus on consumer sovereignty.[145] Although the Statement curbed the role of public policy, it also stated that public policy could "independently support a Commission action… when the policy is so clear that it will entirely determine the question of consumer injury… In these cases the legislature or court, in announcing the policy, has already determined that such injury does exist."[146]

---

[141] Unfair or Deceptive Advertising and Labeling of Cigarettes in Relation to the Health Hazards of Smoking, 29 Fed. Reg. 8324, 8355 (July 2, 1964).

[142] Fed. Trade Comm'n v. Sperry & Hutchinson Co., 405 U.S. 233, 245 n.5 (1972).

[143] J. Howard Beales, *The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection*, FED. TRADE COMM'N (May 30, 2003), https://www.ftc.gov/news-events/news/speeches/ftcs-use-unfairness-authority-its-rise-fall-resurrection [https://perma.cc/YH8V-GX98].

[144] *Id.*

[145] *Id.*

[146] UNFAIRNESS POLICY STATEMENT, *supra* note 126, at 1072–88.

Courts have taken two different approaches to interpreting the Statement, either of which support a finding that platform conduct, as mentioned above, is unfair. On the one hand, the unfairness must be articulated in "'clear and well-established' policies that are expressed in the Constitution, statutes, or the common law."[147] For example, the line of data security cases draws on common law negligence principles.[148]

The Commission may draw on at least two common law contract principles: 1) the extent of permissible conduct is that which is authorized by the contract[149] and 2) a contract must be consentable. The first principle has a long history with the Commission.[150] In *In re Sony BMG Music Entertainment*, Sony installed software on users' computers without their notice or consent and made the software difficult for users to locate and remove. Because installation was not sufficiently communicated to users as a condition of accessing a core service, the practice itself caused substantial injury.[151] Further, in an action against ReverseAuction.com, the Commission alleged that the company's use of user information obtained from eBay to send unsolicited commercial emails violated eBay's User Agreement and, thus, caused substantial injury.[152]

At this point, it is useful to return to Gillespie's discursive treatment of the term "platform."[153] Platforms present themselves as mediators of exchange, connecting independent entities to each other. Consider an excerpt from Facebook's terms of services:

> **Provide a personalized experience for you:**
> [. . .] For example, we use data about the connections *you make*, the choices and settings *you select*, and

[147] LabMD, Inc. v. Fed. Trade Comm'n, 894 F.3d 1221, 1231 (11th Cir. 2018); UNFAIRNESS POLICY STATEMENT, *supra* note 126, at 1076.

[148] LabMD, Inc., 894 F.3d at 1231.

[149] *See* RESTATEMENT (SECOND) OF CONTRACTS § 241 (Am. L. Inst. 1981) (listing factors that determine whether a failure of performance is a material breach).

[150] Apple Inc., FTC File No. 112-3109, 2014 WL 253519, at *7 (F.T.C. Jan. 15, 2014) ("The Commission commonly brings unfairness cases alleging failure to obtain express informed consent.").

[151] Complaint ¶¶ 7–9, 15–16, 20, *In re* Sony BMG Music Entm't, No. C-4195 (F.T.C. June 28, 2007).

[152] Complaint for Permanent Injunction and Other Equitable Relief ¶¶ 8, 10–13, 17, Fed. Trade Comm'n v. ReverseAuction.com, No. 00-00032 (D.D.C. Jan. 6, 2000).

[153] *See supra* Part II.B.

> *what you share and do on* and off our Products - to personalize your experience.[154]

The terms highlight that our experiences of the service are personalized according to *our* connections, *our* choices and settings, and what *we* share and do. What they fail to mention, however, is how Facebook structures the connections we *can* make, the choices and settings we *can* select, and what we *can* share and do. More precisely, they fail to mention how our connections and choices have been predetermined by factors such as how we are sorted into interest categories based on our behaviors and how different weights of different behaviors may alter which connections are recommended.[155] As such, Facebook exceeds the scope of authorized conduct through its terms of services and acts unilaterally to limit users' range of options. Such conduct thus arguably causes or is reasonably likely to cause substantial injury.

Yet, the overwhelming evidence about the futility of notice-and-choice regimes may actually favor platforms in this case.[156] As privacy scholars and commentators have long bemoaned, few consumers actually read companies' terms of service and, even if they do, they are far too often mired in overly vague and complex

---

[154] Terms of Service, FACEBOOK, https://m.facebook.com/legal/terms [https://perma.cc/XG5C-RHJX] (emphasis added). Other platforms are not immune. Instagram's privacy policy, which are incorporated into its terms of services, states:

> [W]e use *your* connections, preferences, interests and activities based on the data we collect and learn from you and others."

Data Policy, INSTAGRAM, https://help.instagram.com/155833707900388 [https://perma.cc/C3XU-5NZ7] (emphasis added). Amazon's terms of service read:

> We use your personal information to recommend features, products, and services that might be of interest to you, identify *your* preferences, and personalize your experience with Amazon Services.

Amazon.com Privacy Notice, AMAZON.COM, https://www.amazon.com/gp/help/customer/display.html?nodeId=GX7NJQ4ZB8MHFRNJ [https://perma.cc/2QTN-GS6S] (emphasis added).

[155] *See supra* Part II.B.

[156] *See, e.g.*, Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L.Q REV. 1461, 1463 (2019); Helen Nissenbaum, *A Contextual Approach to Privacy Online*, 140 DAEDALUS 32, 34 (2011).

language.[157] In other words, as the argument would go, the consumer does *not* consent to platforms' terms of service stating that they use *their* data to personalize their experience on the platform.

Further, empirical evidence illustrates that many users understand, however minimally, targeted ads and the impact on their user experience. In a 2019 Pew Research Center survey, 77% of Americans say they have at least basic knowledge of how companies use their online data to target ads.[158] In this regard, there is an argument to be made that the majority of consumers are aware that their feed is limited by their online activity.

The second contract principle sweeps broader: a contract must be consentable. A contract is not a license to engage in whatever conduct one pleases, and a contract is not valid if it renders a party excessively dependent on the other for their autonomy.[159] This is because consent "is the protector and implementor of autonomy."[160] Thus, even if the material terms were disclosed, users cannot consent to terms of service that, in effect, make them excessively dependent on platform affordances for their recognition and social participation.[161]

The other approach courts have taken rejects requiring a violation of a particular law.[162] As the court in *Federal Trade Commission v. Kochava Inc.* reasoned, this was, in part, because such a requirement did "not square with the text of the FTC Act."[163] It wrote that Kochava's sales of sensitive information subjected consumers to significant risk of harm, such as "embarrassment or

---

[157] Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J.L. & POL'Y FOR INFO. SOC'Y 543 (2008).

[158] Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar & Erica Turner, *3. Public Knowledge and Experiences with Data-Driven Ads*, PEW RSCH. CTR. (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/public-knowledge-and-experiences-with-data-driven-ads/ [https://perma.cc/5LXD-DA63].

[159] *See* NANCY KIM, CONSENTABILITY: CONSENT AND ITS LIMITS 92 (2019).

[160] *Id.* at 53. Importantly, Kim uses "autonomy" differently than I do, pointing to definitions that refer to an individualistic account rather than a relational one. *Id.* at 53–54.

[161] *See supra* Part II.B.

[162] *See, e.g.*, Fed. Trade Comm'n v. Kochava Inc., 671 F. Supp. 3d 1161, 1169–71, 1194 (D. Idaho 2023) (not requiring a predicate violation of law for an unfairness finding); Fed. Trade Comm'n v. Accusearch Inc., 570 F.3d 1187 (10th Cir. 2009) ("[T]he FTCA enables the FTC to take action against unfair practices that have not yet been contemplated by more specific laws."); *see also* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 640 (2014).

[163] *Kochava Inc.*, 671 F. Supp. 3d at 1170.

stigma," from third-parties, which is a cognizable theory of harm.[164] Even so, it concluded that the Commission's assertions of hypothetical scenarios where Kochava could create a risk of concrete harm did not rise to the level of "substantial injury" because the harms were mere hypotheses and so not "likely" to cause harm.

Following *Kochava*, the Commission may argue that platforms' restrictions of available options create an increased risk of secondary harm that is not just theoretical or likely,[165] but actual. This is clear in the many documented instances of erroneous or harmful advertisements, as well as the proliferation of misinformation. For example, Facebook allowed advertisers to target users interested in "informed consent"—a category likely to include users with varying perspectives—with anti-vaccination content.[166] Anti-abortion activists targeted those interested in "pregnancy" and "motherhood" with ads spreading misinformation about fetal development and urging users to reverse the abortion pill.[167] And, in an experiment, the Tech Transparency Project found that advertisers could easily target users with interests in "pharmacy," "pharmaceutical industry," "drugs.com," and "capsule (pharmacy)" with ads promoting pill parties and anorexia, regardless of how those users formed those interests.[168]

***

---

[164] *Id.* at 1171–73.

[165] Alex Hern, *Facebook Labels Russian Users as 'Interested in Treason,'* THE GUARDIAN (July 11, 2018, 12:39 PM), https://www.theguardian.com/technology/2018/jul/11/facebook-labels-russian-users-as-interested-in-treason [https://perma.cc/XWB7-YHER] (describing how advertisers could target Russians labeled as interested in "treason" and record their IP addresses).

[166] Julia Carrie Wong, *Revealed: Facebook Enables Ads to Target Users Interested in 'Vaccine Controversies,'* THE GUARDIAN (Feb. 15, 2019, 1:59 PM), https://www.theguardian.com/technology/2019/feb/15/facebook-anti-vaccination-advertising-targeting-controversy [https://perma.cc/D69R-9P22].

[167] Lauren Kirchner, Maddy Varner & Angie Waller, *As Demand for Medication Abortion Increases, Facebook Allows Ads for Potentially Dangerous 'Abortion Reversal' Procedure*, THE MARKUP (July 19, 2022, 6:00 AM), https://themarkup.org/citizen-browser/2022/07/19/facebook-allows-ads-for-potentially-dangerous-abortion-reversal-procedure [https://perma.cc/UJ4U-GUVP].

[168] *Pills, Cocktails, and Anorexia: Facebook Allows Harmful Ads to Target Teens*, TECH TRANSPARENCY PROJECT (May 4, 2021), https://www.techtransparencyproject.org/articles/pills-cocktails-and-anorexia-facebook-allows-harmful-ads-target-teens [https://perma.cc/6E5B-CZ6F].

The Unfairness Policy Statement instructs that the choice between the two approaches courts should take depends on the individualized circumstances of each action. In context, the Statement reads:

> *To the extent that the Commission relies heavily on public policy to support a finding of unfairness*, the policy should be clear and well-established. In other words, the policy should be declared or embodied in formal sources such as statutes, judicial decisions, or the Constitution as interpreted by the courts, rather than being ascertained from a general sense of the national values.[169]

The modifying clause (in italics) indicates that the degree to which public policy must be tethered to established law is contingent on whether the overall theory of harm rests heavily on public policy. This does not restrict uses of more abstract public policy in cases where the theory of harm weighs consumer injury more.[170] The more the Commission relies on consumer injuries, such as transaction costs, the more it can argue a public policy rationale, such as increased risk of secondary harm. Conversely, the less it relies on consumer injury, the more applicable public policy grounded in the law, such as contract principles, becomes.

To be sure, such a reading is consistent with the history of the Act itself. The outrage at the Commission's abuse of authority prior to the Unfairness Policy Statement was directed towards rules that relied heavily on public policy without regard to consumer injury.[171] In other words, it was outrage at the use of public policy at the expense of consumer injury considerations—not at the *type* of public policy that could be invoked.

Ultimately, to successfully address imposed vulnerability under its Section 5 unfairness authority, the Commission has groundwork available to it to build off of but also must tightly and precisely define the contour of the substantial injury done to consumers.

---

[169] UNFAIRNESS POLICY STATEMENT, *supra* note 126, at 1076.

[170] *See also* Luke Herrine, *The Folklore of Unfairness*, 96 N.Y.U. L. REV. 431, 509 (2021) ("Although the Unfairness Policy Statement is now commonly treated as a break from past statements on the meaning of unfair acts, its purpose was to emphasize continuity.").

[171] Beales, *supra* note 143.

C. NOT REASONABLY AVOIDABLE

The focal point of the second element of the Commission's statutory authority is consumer choice and sovereignty. As the Unfairness Policy Statement says, unfairness actions are not initiated "to second-guess the wisdom of particular consumer decisions," but are pursued in order to correct sales techniques that "may prevent consumers from effectively making their own decisions."[172]

This element is closely related to the discussion above related to exceeding authorized conduct in contract law. The Commission may argue that the logical premise of unauthorized conduct is that consumers are not equipped with sufficient notice or knowledge of the unauthorized conduct, and thus cannot avoid the injuries. That unauthorized conduct renders the injury not reasonably avoidable is supported by both the Unfairness Policy Statement and the Commission's cases. On the former, in its explanation of what constitutes "not reasonably avoidable," the Unfairness Policy Statement lists an example of when a seller "withhold[s] or fail[s] to generate critical price or performance data."[173]

On the latter, the Commission's enforcement actions for data security and privacy cases rely on failure to obtain authorization for material terms as a basis for satisfying the second prong. For example, in *Kochava*, the Commission alleged that Kochava's sale of data is "opaque to consumers" who "have never heard of and never interacted with" Kochava and "have no insight into how" Kochava uses their data.[174] The court found such allegations adequate to survive a motion to dismiss.[175] Similarly, in *Federal Trade Commission v. Ring*, the Commission argued that Ring's, a security camera vendor, practice of allowing thousands of employees and contractors to access video recordings without the customers' knowledge or consent was unfair.[176] Because its customers could not know about these failures, they could not have reasonably avoided the ensuing harms.[177]

---

[172] UNFAIRNESS POLICY STATEMENT, *supra* note 126, at 1074.

[173] *Id.*

[174] Complaint ¶ 31, Fed. Trade Comm'n v. Kochava Inc., 671 F. Supp. 3d 1161 (D. Idaho 2023).

[175] Fed. Trade Comm'n v. Kochava Inc., 671 F. Supp. 3d 1161, 1176 (D. Idaho 2023).

[176] Complaint for Permanent Injunction and Other Relief ¶¶ 25–29, 59–61, Fed. Trade Comm'n v. Ring LLC, No. 23-1549 (D.D.C. May 31, 2023).

[177] *Id.* ¶¶ 51, 59–61.

Consumers cannot reasonably avoid the harms that follow unauthorized conduct from platforms.[178] Without knowledge of how interest categories are formed or how different behaviors are weighed, they are not equipped with the necessary knowledge to alter their feeds in terms of the ads they are shown or the groups they are recommended to join. While it is true that, at least on Facebook, consumers can access and modify the interest categories they fall under,[179] that fails to address the default settings of how those categories are built in the first place or how the categories might come to inform the makeup of their feeds.[180] This is exacerbated by Facebook's statement that its feeds are personalized to users' preferences, such that users might come to believe that the feeds are a genuine reflection of their preferences.

In fact, not only can consumers not reasonably avoid the injuries, Facebook has also taken affirmative steps to block add-ons that allow users to take control of their feeds. In July 2020, developer Louis Barclay released a browser extension, Unfollow Everything, that allowed users to delete their News Feed.[181] The extension was intended to decrease the amount of time users spend on the platform and allow users to curate their feeds more intentionally.[182] Months later, Facebook sent a cease-and-desist letter, permanently disabled Barclay's account, and demanded that he never create a tool that

---

[178] There is of course a great of deal of scholarship about failures of notice and consent, which implicates whether the authorization is really the issue. *See* Solon Barocas & Helen Nissenbaum, *On Notice: The Trouble with Notice and Consent*, PROC. ENGAGING DATA FORUM: THE FIRST INT'L FORUM ON THE APP. AND MGMT. OF PERS. ELEC. INFO. (Oct. 2009). But many have also offered proposals on reforming how notice is communicated rather than how doing away with notice entirely. *See* Paul Ohm & Meg Leta Jones, *Voting for Consent*, 104 B.U. L. REV. 1107 (2024); Brett Frischmann & Moshe Y. Vardi, *Better Digital Contracts with Prosocial Friction-in-Design*, (forthcoming 2025) (on file with author).

[179] *Ad Topics*, FACEBOOK, https://www.facebook.com/help/247395082112892 [https://perma.cc/BJ9W-R27M].

[180] *See also* Cohen, *Infrastructuring*, *supra* note 10, at 22–25 (discussing platform control of advertising dashboards).

[181] Louis Barclay, *Facebook Banned Me for Life Because I Help People Use It Less*, SLATE (Oct. 7, 2021, 9:38 AM), https://slate.com/technology/2021/10/facebook-unfollow-everything-cease-desist.html [https://perma.cc/6WWQ-4GKX].

[182] *Id.*

interacts with Facebook.[183] Today, Unfollow Everything no longer exists.[184]

Second, consumers often do not have meaningful alternatives. The Unfairness Statement contemplates that "consumers will survey the available alternatives, choose those that are most desirable, and avoid those that are inadequate or unsatisfactory."[185] The central premise then is that consumers *have* available alternatives in the first place.

The landscape of competition in the platform market undercuts the premise. As many have commented, platforms have displayed monopolistic tendencies over their respective markets.[186] Merger and acquisition strategies, as well as management choices, have contributed to these tendencies.[187] Although it is contested whether such conduct rises to formal antitrust violations or whether they are symptoms of organic growth, the fact remains that consumers often have few comparable alternatives to meaningfully survey. As our social and economic activities are increasingly mediated through platforms, consumers then have little choice but to act according to platform logics.

D. COUNTERVAILING BENEFITS

The third prong considers whether the stipulated consumer harms are "outweighed by countervailing benefits."[188] Courts typically accept the posited claim without much dispute,[189] and have

---

[183] *Id.*

[184] *Id.* Professor Ethan Zuckerman recently created a browser extension, called Unfollow Everything 2.0, that would similarly allow users to delete their newsfeeds. Vittoria Elliott, *A Lawsuit Argues Meta Is Required by Law to Let You Control Your Own Feed*, WIRED (May 1, 2024, 12:09 PM), https://www.wired.com/story/meta-section-230-users-algorithm/ [https://perma.cc/46UK-FX35]. Zuckerman and the Knight First Amendment Institute at Columbia University filed a lawsuit, requesting the court to declare that the tool is immunized from legal liability or in the alternative, that the tool does not violate Meta's Terms of Service. Complaint at 2, Zuckerman v. Meta Platforms, Inc., No. 24-02596 (N.D. Cal. May 1, 2024).

[185] UNFAIRNESS POLICY STATEMENT, *supra* note 126, at 1074.

[186] *See generally* Lina M. Khan, *The Separation of Platforms and Commerce*, 119 COLUM. L. REV. 973 (2019).

[187] *See* Mason Marks, *Biosupremacy: Big Data, Antitrust, and Monopolistic Power over Human Behavior*, 55 U.C. DAVIS L. REV. 513, 552 (2021).

[188] 15 U.S.C. § 45(n).

[189] Selbst & Barocas, *Unfair Artificial Intelligence*, *supra* note 116, at 1062 ("In most of the cases that the FTC brings under its unfairness

offered different accounts of the precise methodology to be applied. For example, some courts exclusively consider the "potential costs that the proposed remedy would impose on the parties and society in general."[190]

Where courts have substantially engaged with the analysis, scholars and the Commission have suggested focusing the analysis on the offending conduct. In *In re International Harvester*, the Commission argued that relevant costs and benefits were those pertaining to the defendant's failure to disclose the risk of fuel geysering rather than those relevant to the broader design of the tractor.[191] Similarly, in *In re Apple*, the Commission alleged that Apple's payment system for in-app purchases failed to provide adequate notice that entering a password would permit users to incur unlimited purchases in a fifteen-minute window.[192] The costs and benefits to be weighed were not those related to the fifteen-minute window itself, but the offending practice or lack of notice.

Applied to platforms, the relevant costs and benefits are not those associated with the platforms as a whole, but those related to conduct and design choices that cause the above injuries. This might refer to the costs and benefits of disallowing add-ons, such as Unfollow Everything, or to unauthorized conduct, including forming interest categories, structuring advertising dashboards, and prioritizing certain behaviors, based on platforms' own interests. The costs, as mentioned, are transaction costs, contractual rights, and increased risk to secondary harm.[193] The benefit would be those conferred to Facebook for its prohibition of such add-ons or refusal to obtain authorization for its conduct. While it is true this would implicate Facebook's advertising revenue because it may lead to decreased user consumption of the service, the benefit arises *from* the cost. What benefit there might be must then be offset by the cost such that it represents the independent benefit of the conduct.

Another approach focuses the cost-benefit inquiry on the costs and benefits that are experienced by the harmed group.[194] The relevant benefits weighed against the costs are those received by the consumers—not the advertisers or Facebook. To the extent there are

---

authority, it alleges that the cost-benefit test is satisfied without any real argument, and such claims seem rarely to be challenged.").

[190] Am. Fin. Servs. Ass'n v. F.T.C., 767 F.2d 957, 975 (D.C. Cir. 1985); Fed. Trade Comm'n v. Kochava, Inc., 671 F. Supp. 3d 1161, 1176 (D. Idaho 2023).

[191] Int'l Harvester Co., 104 F.T.C. 949, 1050 (1984).

[192] Apple Inc., No. 112-3108, 2014 WL 253519, at *1, *26 (F.T.C. Jan. 15, 2014).

[193] *See supra* Part III.B.

[194] Selbst & Barocas, *Unfair Artificial Intelligence*, *supra* note 116, at 1066.

benefits to the consumer, these benefits might involve lower search costs or improved match quality.[195] Yet, to identify these as benefits is to presume a static self, such that the derived benefits attach to a self that makes judgments and decisions independent of advertising and of the range of available options. Thus, without any showing of any other additional benefit to the harmed consumers, the cost-benefit inquiry weighs in favor of liability.

CONCLUSION

Vulnerability demands legal protection. But before diving into the applicable legal doctrine, we need a robust understanding of the problem and the causal role of the relevant actors. As this Note argues, drawing from different disciplines requires us to reconceptualize vulnerability not as a status, but as iterative layers of ontological and social conditions. It also instructs us to interrogate the underlying sociotechnical processes of platforms. As the architects of the information economy, platforms determine the scope and form of the self through their involvement in datafication and interoperability. In doing so, they impose vulnerability.

The Federal Trade Commission may be called on to intervene. In light of its expanding authority, this Note detailed the arguments for and against characterizing the role of platforms in contributing to imposed vulnerability as an unfair practice. While traditional interpretations of the Commission's Section 5 authority are likely unable to do the job, the Commission's shifting interpretation of its authority demands at least an initial legal analysis for how it might reach that conclusion.

[195] *See supra* note 137.