A Minimally Just Framework for Digital Dignity: Unifying Contextual Integrity and the Capabilities Approach

Kat Roemmich
roemmich@umich.edu
University of Michigan
Ann Arbor, MI, USA

Florian Schaub
fschaub@umich.edu
University of Michigan
Ann Arbor, MI, USA

Kirsten Martin
kmarti33@nd.edu
University of Notre Dame
Notre Dame, IN, USA

ABSTRACT

Increasingly, powerful digital technologies impinge on human agency and dignity with intensifying risks. Although the European Union (EU) seeks to re-balance these power asymmetries with a human-centric, rights-based digital strategy, it remains challenging to transform formal entitlements into tangible opportunities to thrive. This paper integrates Contextual Integrity (CI), a context-relative *justificatory framework* for identifying "appropriate" data flows, with the Capabilities Approach's (CA) theory of *minimal justice*, establishing baseline conditions for the inviolability of human dignity. Reframing privacy as an essential human functioning, the integrated CI+CA framework provides a principled "line in the sand" with normative thresholds that appropriate data flows must meet—ensuring central human capacities remain protected even in technologically complex environments. We illustrate its theoretical and practical strength through a high-risk AI scenario under the EU's digital strategy, showing how this synergy extends standard rights-based governance to secure fundamental human values in the everyday realities of data-driven ecosystems.

CCS CONCEPTS

• **Security and privacy → Privacy protections**; • **Social and professional topics → Management of computing and information systems**; • **Applied computing → IT governance**.

KEYWORDS

Privacy, Ethics, Data Governance, AI Governance.

ACM Reference Format:
Kat Roemmich, Florian Schaub, and Kirsten Martin. 2025. A Minimally Just Framework for Digital Dignity: Unifying Contextual Integrity and the Capabilities Approach. In . ACM, New York, NY, USA, 5 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

> *"To be a good human being is to have a kind of openness to the world, an ability to trust uncertain things beyond your own control, that can lead you to be shattered in very extreme circumstances for which you were not to blame. That says something very important about the condition of the ethical life: that it is based on a trust in the uncertain and on a willingness to be exposed; it's based on being more like a plant than like a jewel, something rather fragile, but whose very particular beauty is inseparable from that fragility."* –Martha C. Nussbaum [28]

In our shared digital moment, nearly every facet of human life—from our capacity for autonomous choice to our deepest sense of dignity—has become vulnerable under the sway of increasingly sophisticated technologies. From technology giants to everyday digital platforms and services, our personal data is accumulated incessantly, shaping our daily rhythms and fueling algorithmic engines that promise consumer convenience and corporate efficiency. Yet behind this allure lies a capacity to harvest the most intimate contours of human life for profit or worse, hidden manipulative agendas. Regulators voice caution that structural power imbalances in data ecosystems concentrate asymmetrical control over personal information, undercutting the agency of individuals and communities worldwide [34].

Against this backdrop, the European Union (EU) stands as a champion of human-centric, rights-based digital transformation, enshrined in regulatory instruments like the General Data Protection Regulation (GDPR), the Digital Services Act (DSA), the Digital Markets Act (DMA), and the Artificial Intelligence (AI) Act. Guided by fundamental values for human rights and democracy, these regulatory frameworks aspire to empower all individuals in Europe's digital future—particularly those most vulnerable—with digital rights, securing entitlements like privacy and data protection into digital solutions rather than remaining abstract formalities. In extending the ethos of its Charter of Fundamental Rights [15] and the broader human-rights consensus [5] to jurisdictions far beyond its borders, the EU has produced a "Brussels Effect," raising global data protection and privacy standards and advancing a shared vision of human dignity [7].

Yet even amid these ambitious legal structures, a deep worry persists that the everyday digital experiences of privacy and agency are slipping beyond reach. Studies delegated by the European Commission suggest that over one-third of Europeans report feeling unprotected and unable to control personal data online—a decline from prior years [12]—while the only policy area in the EU's digital rights-based strategy showing negative growth for markets is that of "promoting fundamental rights and democratic values in digital spaces" [32]. The problem is not merely how to *affirm* digital rights in principle, but how to *transform* them into something genuinely meaningful—particularly for those bearing the brunt of structural

Conference'17, July 2017, Washington, DC, USA

ACM ISBN 978-1-4503-XXXX-X/2018/06
https://doi.org/10.1145/nnnnnnn.nnnnnnn

inequalities. If an individual has "rights" to privacy and data protection yet lacks any genuine capacity to exercise them—whether owing to manipulative platform architectures or socio-economic constraints—then their rights ring hollow. Thus, we face a central challenge: bridging the gap between privacy, data protection, and other fundamental entitlements and the lived realities of those exposed to ubiquitous data-driven technologies. In response, this paper proposes uniting Contextual Integrity with the Capabilities Approach.

Originally developed by economist Amartya Sen and philosopher Martha Nussbaum, the Capabilities Approach (CA) is a normative theory with broad applications across the humanities and social sciences. At its core, the CA asks what opportunities people have to *do and be what they value*, positing this as the appropriate measure of key human value abstractions— equality [4, 41], well-being [36, 39], justice [2, 30]—within our inherently interdependent societies [18]. In recent years, scholars have increasingly adopted CA lenses in socio-technical domains including Information and Communication Technologies for Development (ICT4D) [20], information rights [8], design [6], best interests standards [44], and cybersecurity [13]. Nussbaum's capabilitarian theory of justice, in particular, has deeply influenced both human rights [29, 40, 47] and technology ethics [10, 33], offering a methodology that reframes the normative criteria for justice with a set of "central capabilities" said to collectively constitute human dignity: life; bodily health; bodily integrity; senses, imagination, and thought; emotions; practical reason; affiliation; other species; play; and control over one's environment [30]. Where one lacks meaningful capacity to exercise agency within this "irreducible" constellation of capabilities up to the minimum thresholds Nussbaum's theory qualifies, the CA identifies a failure to meet the standard for "minimal justice," the globally agreed *inviolability of human dignity* [5], thereby obligating intervention [30]. Although Nussbaum's CA does not explicitly enumerate *privacy or data protection*, privacy scholars have articulated these values as essential for enabling and securing the conditions the central capabilities require for "self-fulfillment and more broadly for human flourishing" [11].

Contextual integrity (CI), for its part, similarly shifts attention from the abstraction of privacy as a human value with a descriptive account that locates privacy in the actual circulation of informational norms within and across myriad social domains. CI is not merely a descriptive theory but also a normative one, providing a "justificatory framework" that demarcates where data flows can be justifiably considered impermissible, *prima facie* where they contravene established norms within a particular context, constituting a privacy violation [26]. Although CI's normative heuristic ultimately directs us to assess informational norms against the moral and political values and contextual stakes relevant to secure the integrity of social life, it does not specify *which* human values ought to prevail. CI's value under-specification supports the generalizability of its framework, yet opens the possibility for it to justify data flows that fail to respect a fundamental value that ethical consensus considers non-negotiable *regardless of context*: human dignity [5].

We propose enriching CI's normative criteria with CA's minimal justice thresholds, recasting privacy as both a contextual phenomenon and a core human functioning. This merged framework would thus provide a principled line in the sand below which data practices violating human dignity can be identified and addressed to meet minimal justice standards, while still preserving CI's respect for the contextual nuances of privacy in everyday life.

We close by illustrating how our Capabilities Approach to Contextual Integrity (CA-CI) can strengthen the EU's digital strategy with examples of its application to obligations for high-risk AI scenarios, demonstrating its utility for ensuring that fundamental entitlements do not remain aspirational ideals, but become tangible conditions under which people and society may flourish.

2 CENTERING PRIVACY VULNERABILITIES

2.1 The Rising Tide of Digital Tracking

A contemporary landscape of pervasive data collection and exploitation has led to well-documented intrusions and harms [22], underscoring that privacy is neither an optional luxury nor an easily secured right. Since the GDPR took effect in 2018, regulatory actions have exposed widespread failures by major technology companies (e.g., Google, Uber, Meta), service providers (e.g., British Airways, Marriott) and employers (e.g., Amazon) to protect personal data; prevent breaches; and ensure lawful, fair, and transparent data processing [14]. These legal challenges illustrate systemic disregard for privacy safeguards, demonstrating that even well-established frameworks face significant enforcement gaps.

The problem extends far beyond compliance failures. As early as 2014, Facebook's large-scale emotional contagion experiment revealed how manipulations of social media feeds could influence users' emotional states [21], foreshadowing a business model that thrives on engagement-driven algorithmic amplification. Leaked internal documents in 2021 confirmed that Facebook's recommender algorithms deliberately prioritized negative content to sustain user attention [17]. Meanwhile, discriminatory outcomes in high-stakes domains such as housing, employment, and credit have resulted in landmark legal settlements and regulatory interventions, culminating in Meta's 2022 settlement with the U.S. Department of Justice over biased ad targeting [1, 45].

Yet, these headline cases represent only part of a broader pattern. Recent research shows that even child-focused sites embed invasive trackers and push targeted advertisements on sensitive topics ranging from mental health to sex toys [25]. In workplaces, employers increasingly push the boundaries of acceptable data practices, implementing algorithmic management and surveillance systems that undermine job security and erode institutional trust [19, 23].

Together, these examples highlight a digital reality in which vulnerabilities are not simply pre-existing individual traits, but the byproduct of *power asymmetries* that shape digital environments and the possibilities within them. When data subjects lack the meaningful capacity to exercise agency and maintain self-dignity in digital spaces, privacy vulnerabilities become the norm, not the exception [9, 16]. Yet, as Martha Nussbaum reminds us, human goodness itself depends on a willingness to trust in the other, outside the reach of our control [28]. Vulnerability in the digital sphere, then, is not merely a symptom of flawed digital infrastructures, but deeply entangled with fragile interdependence that characterizes ethical life.

2.2 Vulnerability and Trust

Far from a technical shortcoming, privacy shortfalls resonate with Nussbaum's conception of *vulnerability* as an inherent part of ethical life [28, 31]. To be human is to depend on others—not only for care and the development of our capacities, but also for the social trust that makes meaningful connection and cooperation possible. As Nussbaum observes, such vulnerability is both essential and precarious: our fragility is bound up with our capacity to trust, and with it, the risk of betrayal.

In digital contexts, this tension is intensified. The very structures that mediate our social connections demand trust while simultaneously eroding it [48], as systems optimized for data extraction reconfigure our dependencies to serve opaque and shallowly justified commercial [49] or political [42] goals rather than the common good. Where data architectures magnify these vulnerabilities, privacy emerges as a crucial line of defense—yet it remains insufficient if limited to a purely negative liberty (e.g., freedom from intrusion) without an *affirmative* dimension ensuring each person's capacity for autonomous choice and self-determination [11]. Hence, safeguarding digital vulnerability entails both privacy as a protective boundary and as a positive force that enables freedom to flourish—to choose, reflect, and grow without unbridled intrusion, interference, or manipulation.

3 ANCHORING CONTEXTUAL INTEGRITY IN HUMAN FLOURISHING

3.1 Why CI Alone Is Not Enough to Address Privacy Vulnerabilities

Privacy, under CI, is neither absolute nor singular; it emerges when data exchanges comfortably conform to established roles, attributes, and transmission principles that govern the acceptability of information flows in each social domain. CI's normative emphasis on preserving contextual norms pragmatically instrumentalizes privacy as a means to secure human values across complex social realms [27]. Yet it does not specify *which* human values must be upheld, relying on the assumption that fair social processes have shaped which norms are considered appropriate across competing interests within a context over time [26].

In modern digital environments, however, people are becoming habituated to ubiquitous privacy intrusions that erode their capacities for agency and dignity. Whether operating as employers with authoritarian degrees of control over workers' private lives [3] or providers of exploitative data-intensive consumer products [46], technology giants and the broader data ecosystems they enable wield disproportionate socio-technical power to scale autonomous systems that influence moods, beliefs, and behaviors *even pre-consciously* [43, 49]. Opportunities for meaningful participation in shaping norms continue to diminish [24], as commercial interests increasingly displace valued social norms [37, 38]. This power imbalance constrains the very domains where individuals should have real opportunities to negotiate what their fundamental entitlements look like.

These concerns echo John Rawls' *difference principle*: social arrangements must be structured to benefit the least well-off to be considered just [35]. When introducing the Capabilities Approach, Amartya Sen famously challenged Rawls to specify "equality of what?": Do we measure equality by income, resources, or something else [41]? CA's response is that the most telling measure of inequality—whether on account of individual differences or structural constraints that entrench vulnerabilities—lies in people's actual *capabilities*, their real opportunities to *be and do* what they value. In this light, privacy is a key facilitator that both protects and enables capabilities [11]—our abilities to develop thought, maintain intimacy, pursue autonomous life plans, and cultivate our own vision of the good [30]. By extension, Rawls' difference urges scrutiny into how power-imbalanced digital infrastructures systematically favor certain groups while exacerbating vulnerabilities for others—whether through biased algorithms or exploitative data business models—violating minimal justice standards by failing to protect or enhance the capabilities of the data subjects they render vulnerable.

3.2 A Unified Framework

To address this gap, we propose a unified framework that overlays CA's universal normative thresholds onto CI's theory of privacy. Specifically, we designate the "central capabilities" required for human dignity [30] as benchmark criteria that data flows must not compromise to be considered minimally just. In doing so, we retain CI's structure of informational norms—identifying the *context*, the *roles* of data subjects, senders, and recipients, the *types* of data involved, and the *transmission principles* that constrain the data flow—while injecting a more concrete normative stances about *which* human interests are non-negotiable.

We envision setting normative thresholds as transmission principles, based on an evaluation of the data flow's *impact* on each of the "central capabilities" (e.g., emotions, bodily integrity, practical reason, control over one's environment). If data flows, based on either reasonable anticipation or empirical knowledge, impede any capability below the minimum thresholds Nussbaum defines (e.g., for practical reason, "being able to form a conception of the good and to engage in critical reflection about the planning of one's life. (This entails protection for the liberty of conscience and religious observance.))" [30] they would be considered *inappropriate*.

By introducing central capabilities as universal normative anchors, the Capabilities Approach to Contextual Integrity (CA-CI, see Table 1) we propose not only identifies data flows that fail to respect human dignity, but opportunities for socio-technical interventions that can adjust the data flow such that it meets the bar for minimal justice. At a moment when societal relationships to technology threaten human values perhaps more than ever before, CA-CI draws a line that identifies the *core* human values that ought never be compromised, no matter how local norms evolve under the sway of disproportionately powerful actors. Through this alignment, CA-CI offers a more robust ethical framework for evaluating digital vulnerabilities and ensuring that privacy and data protection remain vehicles of empowerment—values that enable *all* people to exercise genuine agency and maintain dignity in the face of ever-shifting data practices.

3.3 Alignment with the EU's Digital Strategy

Under Contextual Integrity (CI), legitimate privacy claims are not grounded in personal preference, but in the moral and political

Dimension	Contextual Integrity (CI)	Capabilities Approach (CA)
Key Theoretical Focus	Appropriate data flows governed by context-specific norms; norm-driven and context-relative.	Substantive freedoms for human flourishing; emphasizes real capacity to convert rights/ resources into capabilities.
Aim or Purpose	Preserve context-specific informational norms that implicitly protect societal values.	Ensure individuals can actually exercise agency and realize well-being (bodily integrity, practical reason, etc.).
Limitations and Gaps	Does not specify which core values or ends must be safeguarded; assumes fair norm-setting.	Historically not focused on data privacy *per se*; needs bridging to info-governance contexts.
Relevance to Digital Vulnerabilities	Identifies *in*appropriate data flows but may not address structural inequalities in capacity to push back.	Unequal abilities to convert privacy rights into meaningful control; emphasizes overlooked vulnerabilities.

Table 1: Comparative Overview of Contextual Integrity and Capabilities Approach.

values at stake and whether a given information flow serves or disrupts the context's ends or purposes (and the broader social values it supports). CI posits that contextual norms and their underlying moral, political, and contextual values form the justificatory basis for a data practice's *context-specific* acceptability [27]. However, it does not specify *which* human values must be upheld, presuming instead that fair social processes have historically shaped the norms balancing competing interests within each particular context [26].

In the European Union, the right to privacy and data protection is founded on the principle of human dignity [15], itself deemed inviolable in both EU and international law [5]. Therefore, when applying CI within the EU framework, contextual norms (including any relevant moral and political values) must align with dignity-based justifications as part of the Union's foundational rights structure. Put differently, while CI does not inherently require a commitment to human dignity on its own, any use of CI within the EU must be interpreted through this dignity lens if it is to remain compatible with the Charter's bedrock principle.

If we adopt Nussbaum's account, which defines human dignity in terms of "central capabilities," then ensuring no data flow undermines those capabilities below a minimal threshold functions as an additional "transmission principle." Within this *Capabilities Approach to Contextual Integrity* (CA-CI), any application of CI in EU governance would be bound to respect and promote human dignity, because privacy and data protection themselves exist to secure that dignity.

Beyond this clear justificatory alignment with the EU's digital strategy, CA-CI offers two crucial contributions:

(1) *Strengthening Anticipatory Governance:* By identifying novel AI risks that should be either prohibited or tightly regulated;
(2) *Clarifying Regulatory Ambiguities on Harm:* Addressing gaps that persist even after the release of the Commission's draft guidelines (not yet formally adopted).

3.3.1 Anticipatory Risk Management. Recital 28 of the EU AI Act prohibits AI systems that enable manipulative, exploitative, or socially controlling practices, precisely because they conflict with the Union's commitment to *human dignity*. By using dignity as the basis for AI prohibitions and heightened obligations, CA-CI furnishes a methodology that enables **anticipatory governance** by flagging the risk of eroding human dignity *before* they are explicitly enumerated as Prohibited or High-Risk. Under CA-CI, one could map how an AI system's data flows and design features (as per CI) align with or erode the central capabilities needed for human dignity (as per CA). If dignity is materially threatened—even in a new or unanticipated use case—there is a compatible basis to classify the practice as prohibited or warranting strict regulation. Moreover, CA-CI offers a structured means to conduct formal rights impact assessments required for certain high-risk AI processing by examining the precise data flows (CI's domain) against each capability threshold (CA's domain), thereby uncovering manipulative or exploitative uses *prior* to any explicit ban.

3.3.2 Significant Harm. The Commission's draft guidelines clarify that prohibited or tightly controlled AI uses—such as those distorting behavior through subliminal, deceptive, or manipulative techniques—must undergo a risk assessment to gauge both the magnitude and likelihood of harm. This includes potential physical, psychological, financial, or economic harm, with particular emphasis on compounding effects that may accumulate over time, exacerbate vulnerabilities, and produce severe long-term consequences.

Under Article 5(1)(a) of the AI Act, a significant harm threshold triggers prohibitions against subliminal, manipulative, and deceptive AI. The guidelines note that determining significant harm requires a fact-specific, case-by-case assessment of whether an AI system appreciably impairs individuals' ability to make informed decisions and undermines their free choices. Crucially, harm may not manifest immediately—addiction-like behaviors or erosions of autonomy over time still count if they are "reasonably likely to occur."

CA-CI addresses this under-specification of harm thresholds—akin to CI's under-specification of which human values prevail—by anchoring significant harm in the impairment of central capabilities. Once an AI system's design or data flow (mapped via CI) is shown to degrade any capability below Nussbaum's minimum threshold for human dignity, that use case signals a *significant harm* that warrants prohibition or strict oversight. This approach grounds evaluations in a consistent, dignity-based benchmark, helping regulators pin down (1) the types of harms involved, (2) their threshold of significance, and (3) the causal link to AI-driven manipulation.

Thus, CA-CI unifies Contextual Integrity's robust methodology for mapping data flows with a capabilities-based account of dignity, furnishing a clear and adaptable standard for identifying "significant harm" in AI systems. This not only strengthens existing EU digital

governance but also provides a principled approach to upcoming and unanticipated risks.

REFERENCES

[1] Muhammad Ali, Piotr Sapiezynski, Miranda Bogen, Aleksandra Korolova, Alan Mislove, and Aaron Rieke. 2019. Discrimination through Optimization: How Facebook's Ad Delivery Can Lead to Biased Outcomes. *Proc. ACM Hum.-Comput. Interact.* 3, CSCW, Article 199 (Nov. 2019), 30 pages. https://doi.org/10.1145/3359301

[2] Elizabeth Anderson. 2010. Justifying the capabilities approach to justice. *Measuring justice: Primary goods and capabilities* 81 (2010), 100.

[3] Elizabeth Anderson. 2017. Private Government: How Employers Rule Our Lives (and Why We Don't Talk about It).

[4] Elizabeth S Anderson. 1999. What is the Point of Equality? *Ethics* 109, 2 (1999), 287–337.

[5] UN General Assembly et al. 1948. Universal declaration of human rights. *UN General Assembly* 302, 2 (1948), 14–25.

[6] Scott Boylston. 2019. *Designing with society: A capabilities approach to design, systems thinking and social innovation.* Routledge.

[7] Anu Bradford. 2020. *The Brussels Effect: How the European Union Rules the World.* Oxford University Press.

[8] Johannes Britz, Anthony Hoffmann, Shana Ponelis, Michael Zimmer, and Peter Lor. 2013. On considering the application of Amartya Sen's capability approach to an information-based rights framework. *Information Development* 29, 2 (2013), 106–113.

[9] Ryan Calo. 2013. Digital market manipulation. *Geo. Wash. L. Rev.* 82 (2013), 995.

[10] Alessandra Cenci and Dylan Cawthorne. 2020. Refining value sensitive design: A (capability-based) procedural ethics approach to technological design for well-being. *Science and Engineering Ethics* 26, 5 (2020), 2629–2662.

[11] Julie E Cohen. 2012. What privacy is for. *Harv. L. Rev.* 126 (2012), 1904.

[12] European Commission. 2024. Monitoring of Digital Rights and Principles – Support study 2024 | Shaping Europe's digital future. https://digital-strategy.ec.europa.eu/en/library/monitoring-digital-rights-and-principles-support-study-2024

[13] Partha Das Chowdhury and Karen Renaud. 2023. 'Ought'should not assume 'Can'? Basic Capabilities in Cybersecurity to Ground Sen's Capability Approach. In *Proceedings of the 2023 New Security Paradigms Workshop*. 76–91.

[14] DPM. 2024. 20 biggest GDPR fines so far [2025]. https://dataprivacymanager.net/5-biggest-gdpr-fines-so-far-2020/

[15] European Union. 2000. Charter of Fundamental Rights of the European Union. Official Journal of the European Communities. Notice No. 2000/C 364/01, Page 1.

[16] Federico Galli. 2022. Digital vulnerability. In *Algorithmic marketing and EU law on unfair commercial practices*. Springer, 181–207.

[17] Keach Hagey and Jeff Horwitz. 2021. Facebook tried to make its platform a healthier place. It got angrier instead. *The Wall Street Journal* 16 (2021).

[18] Nimi Hoffmann and Thaddeus Metz. 2017. What can the capabilities approach learn from an Ubuntu ethic? A relational approach to development theory. *World Development* 97 (2017), 153–164.

[19] Mohammad Hossein Jarrahi, Gemma Newlands, Min Kyung Lee, Christine T Wolf, Eliscia Kinder, and Will Sutherland. 2021. Algorithmic management in a work context. *Big Data & Society* 8, 2 (2021), 20539517211020332.

[20] Dorothea Kleine. 2013. *Technologies of choice?: ICTs, development, and the capabilities approach.* MIT press.

[21] Adam DI Kramer, Jamie E Guillory, and Jeffrey T Hancock. 2014. Experimental evidence of massive-scale emotional contagion through social networks. *Proceedings of the National Academy of Sciences* 111, 24 (2014), 8788–8790.

[22] Jacob Leon Kröger, Milagros Miceli, and Florian Müller. 2021. How data can be used against people: A classification of personal data misuses. *Available at SSRN 3887097* (2021).

[23] Lan Li, Tina Lassiter, Joohee Oh, and Min Kyung Lee. 2021. Algorithmic hiring in practice: Recruiter and HR Professional's perspectives on AI use in hiring. In *Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society*. 166–176.

[24] Nora McDonald and Andrea Forte. 2020. The politics of privacy theories: Moving from norms to vulnerabilities. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. 1–14.

[25] Zahra Moti, Asuman Senol, Hamid Bostani, Frederik Zuiderveen Borgesius, Veelasha Moonsamy, Arunesh Mathur, and Gunes Acar. 2024. Targeted and troublesome: Tracking and advertising on children's websites. In *2024 IEEE Symposium on Security and Privacy (SP)*. IEEE, 1517–1535.

[26] Helen Nissenbaum. 201-0. *Privacy in context: Technology, policy, and the integrity of social life.* Stanford University Press.

[27] Helen Nissenbaum. 2018. Respecting context to protect privacy: Why meaning matters. *Science and engineering ethics* 24, 3 (2018), 831–852.

[28] Martha Nussbaum. 1988. Interview with Bill Moyers on *A World of Ideas*. Public Broadcasting Service (PBS). https://billmoyers.com/content/martha-nussbaum/ Transcript accessed 2025-02-03.

[29] Martha C Nussbaum. 1997. Capabilities and human rights. *Fordham L. Rev.* 66 (1997), 273.

[30] Martha C Nussbaum. 2000. *Women and human development: The capabilities approach.* Cambridge University Press.

[31] Martha C Nussbaum. 2003. *Upheavals of thought: The intelligence of emotions.* Cambridge University Press.

[32] German Presidency of the Council of the European Union. 2020. Berlin Declaration on Digital Society and Value-Based Digital Government. https://ec.europa.eu/isa2/sites/isa/files/cdr_20201207_eu2020_berlin_declaration_on_digital_society_and_value-based_digital_government_.pdf

[33] Ilse Oosterlaken. 2012. The capability approach, technology and design: Taking stock and looking ahead. In *The capability approach, technology and design*. Springer, 3–26.

[34] Wojciech Rafał Wiewiórowski. 2025. Shaping a Safer Digital Future: a New Strategy for a New Decade | European Data Protection Supervisor. https://www.edps.europa.eu/press-publications/publications/strategy/shaping-safer-digital-future

[35] John Rawls. 2017. A theory of justice. In *Applied ethics*. Routledge, 21–29.

[36] Ingrid Robeyns. 2020. Wellbeing, place and technology. *Wellbeing, Space and Society* 1 (2020), 100013.

[37] Michael J Sandel. 1998. *What money can't buy: the moral limits of markets.* Brasenose College, Oxford.

[38] Michael J Sandel. 2013. Market reasoning as moral reasoning: why economists should re-engage with political philosophy. *Journal of economic Perspectives* 27, 4 (2013), 121–140.

[39] Amartya Sen. 1993. Capability and well-being73. *The quality of life* 30 (1993), 270–293.

[40] Amartya Sen. 2005. Human rights and capabilities. *Journal of human development* 6, 2 (2005), 151–166.

[41] Amartya Sen et al. 1979. *Equality of what?* Vol. 1. na.

[42] Daniel J Solove. 2011. *Nothing to hide: The false tradeoff between privacy and security.* Yale University Press.

[43] Daniel Susser, Beate Roessler, and Helen Nissenbaum. 2019. Online manipulation: Hidden influences in a digital world. *Geo. L. Tech. Rev.* 4 (2019), 1.

[44] Michael Thomson. 2021. A capabilities approach to best interests assessments. *Legal Studies* 41, 2 (2021), 276–293.

[45] Aditya Srinivas Timmaraju, Mehdi Mashayekhi, Mingliang Chen, Qi Zeng, Quintin Fettes, Wesley Cheung, Yihan Xiao, Manojkumar Rangasamy Kannadasan, Pushkar Tripathi, Sean Gahagan, Miranda Bogen, and Rob Roudani. 2023. Towards Fairness in Personalized Ads Using Impression Variance Aware Reinforcement Learning. In *Proceedings of the 29th ACM SIGKDD Conference on Knowledge Discovery and Data Mining* (Long Beach, CA, USA) *(KDD '23)*. Association for Computing Machinery, New York, NY, USA, 4937–4947. https://doi.org/10.1145/3580305.3599916

[46] Joseph Turow, Nora Draper, Mara Einstein, James F Hamilton, and Edward Timke. 2021. The voice catchers: How marketers listen in to exploit your feelings, your privacy, and your wallet. *Advertising & Society Quarterly* 22, 4 (2021).

[47] Mahbub Ul Haq. 2003. The birth of the human development index. *Readings in human development* 2 (2003), 127–137.

[48] Ari Ezra Waldman. 2018. *Privacy as Trust: Information Privacy for an Information Age.* Cambridge University Press.

[49] Shoshana Zuboff. 2019. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power, edn. *PublicAffairs, New York* (2019).