Routledge
Taylor & Francis Group

Globalizations

ISSN: 1474-7731 (Print) 1474-774X (Online) Journal homepage: www.tandfonline.com/journals/rglo20

Consent, coercion, colonialism: a manifesto for digital rights from the left

Phoebe V. Moore, Peter Bloom & Rodrigo Nunes

To cite this article: Phoebe V. Moore, Peter Bloom & Rodrigo Nunes (10 Feb 2026): Consent, coercion, colonialism: a manifesto for digital rights from the left, Globalizations, DOI: 10.1080/14747731.2025.2591534

To link to this article: https://doi.org/10.1080/14747731.2025.2591534

Published online: 10 Feb 2026.

GLOBALIZATIONS
https://doi.org/10.1080/14747731.2025.2591534

Routledge
Taylor & Francis Group

Consent, coercion, colonialism: a manifesto for digital rights from the left

Phoebe V. Moore [a], Peter Bloom[b] and Rodrigo Nunes[b]

[a]Management and the Futures of Work, Essex Business School, University of Essex, Essex, UK; [b]Political Theory and Organization, Essex Business School, University of Essex, Essex, UK

ABSTRACT

Digital transitions, involving the widespread adoption of biometric, algorithmic, and AI systems across public and private sectors, are often framed as inevitable and necessary for progress. However, these transitions are not neutral. They are shaped by coercive data extraction practices of digitalization, which consolidate corporate power, and reproduce colonial social relations. At the center of this process is the erosion of meaningful consent, alongside the expansion of surveillance infrastructures that restructure subjectivity without recognition or accountability. Dominant rights frameworks, including liberal notions of personhood and existing legal protections, fail to confront these harms. Regulatory frameworks overlook relational dynamics, systemic misrecognition, and the asymmetries of digital colonialism. Coercion is overtaking consent in the digital realm. A new political struggle is needed to reclaim subjectivity and argue for a manifesto of digital rights from the left.

ARTICLE HISTORY
Received 3 February 2025
Accepted 13 November 2025

KEYWORDS
Digital transition; digitalization; data extraction; coercion plus consent; colonialism; subjectivity

I. Introduction

When the internet became widely accessible in the 1990s, from Silicon Valley to Seoul, its inclusive and revolutionary potential created global excitement. East Asian teenagers clustered in game rooms playing World of Warcraft across oceans. Singles, closeted homosexuals, fetish enthusiasts, and counterculture fans joined chat rooms seeking love, political communities, and shared interests in seemingly safe, inclusive environments. Platforms like Second Life offered identity exploration impossible 'in real life' (IRL). Early spaces emerged: Usenet newsgroups like alt.queer, AOL chatrooms, forums like PlanetOut (founded in 1995), The WELL (Whole Earth 'Lectronic Link, founded in 1985) bringing together hackers, writers, and countercultural thinkers like Howard Rheingold for essays and debates, and VNS Matrix, Australian cyberfeminist artists exploring gender, technology, and digital identity subversively.

These experiments were fuelled by optimism extending beyond screens. Permaculture movements flourished, recycling and green politics gained traction, maker culture thrived. Though surveillance technologies existed, their public reach remained limited. The internet appeared

CONTACT Phoebe V. Moore p.moore@essex.ac.uk

liberating, opening new sociality and self-expression forms. Data extraction risks, from digitalized interactions or urban movement, seemed unimportant and a distant concept. Yet this liberation was already underpinned by emerging control regimes. Infrastructures enabling early digital freedoms were rapidly consolidated by actors operating within extractive, profit-driven logics. Monopoly tech firms expanded, states deepened surveillance capacities, and users became entangled in opaque profiling and prediction systems. Initial 'worldwide web' excitement soon gave way to cynicism, caution, and a sense of lost autonomy.

Perhaps the clearest indicator of this shift, is the erosion of meaningful *consent*. Today's online agreements are manufactured through manipulative interface design and hidden coercion. 'Dark patterns' nudge users toward accepting data tracking. 'Accept all' buttons dominate visual hierarchies while 'manage settings' options are buried or complicated. Consent banners are intentionally confusing, and continued platform use is interpreted as implied consent. Bundled consent collapses multiple data practices into single checkboxes, leaving users unaware of scope or implications. Apps request unnecessary permissions such as flashlight apps asking for geolocation data. Refusing consent often means losing service access entirely. These practices simulate rather than facilitate consent under structural coercion conditions that have already been documented in workplace regimes of control (Petrosino, 2024; Tourish & Willmott, 2023). During recent UK leisure facility facial recognition rollout, users refusing biometric enrollment were denied entry altogether (ICO, 2024).

This article places responsibility on Big Tech companies, complicit states, and inadequate rights regimes, interrogating frameworks that failed to prevent or sufficiently acknowledge social harms. From a Marxist perspective, we look at digitalized extraction's social relations, where identities are commodified and subjectivities shaped and reshaped. While online self-expression rights were always entangled with changing norms, few frameworks address how personhood and recognition are at stake when platforms determine not only visibility but legibility. Current data protection laws and human rights frameworks' assumed sufficiency has masked these harms' structural nature.

We address issues in digitalized, rather than digital transitions; looking at 'digitalization' rather than focussing only on 'datafication'. 'Digitalized' colonialism introduces a better framing, because colonial aggression is occuring in more areas than data extraction, where other digitalized advancements cause fissures and power imbalances. The term 'data' on its own, does not problematize sufficiently; does not involve accountability questions; does not refer to an active process. At stake are the intensifying vulnerabilities for people which are insufficiently addressed by data protection law (Malgieri, 2023), which are underrepresented in critical data studies, and do not directly address the problems of identify, self-formation, and overall, in social relations. Building on the themes of this Special Issue, this article examines how colonial logics of extraction shape digitalized transitions, focusing on the power structures and social relations in digitalized transitions. Other articles in this special issue focus on 'green transitions'.[1]

Current legal frameworks for data protection and human rights are ill – equipped to address the lived realities of digitalized life. We advocate, therefore, for a digital rights from the left, not simply adding protections to existing liberal frameworks, but rather, rethinking what rights are for, who they serve, and how they are enacted. A leftist approach must be grounded in collective recognition, resistance to domination, and redistribution of informational and infrastructural power. It must confront coercion not as an exception within liberal systems, but as a fundamental part of their structural condition. This article offers a manifesto for such an approach, an invitation to reclaim consent, recognition, and subjectivity on new terms, claiming digital rights for the left.

II. Digitalized colonialism and the restructuring of social relations

The transition from the early internet's participatory promise to its present enclosure represents not only a governance shift but a deeper transformation in the political economy of digitalized interaction. This transformation can be understood as part of a longer history of colonial appropriation in which new technologies are mobilized to extract value from previously uncommodified, non-digitalized, life-worlds. 'Data colonialism' describes this reorganization of social life as raw material for accumulation, extending colonial dispossession logic into the digital domain (Couldry & Mejias, 2019b; Thatcher et al., 2016). A convergence of digitalized extraction underpins what Berardi (2024) identifies as hyper-colonial trends, intersecting these transitions governed by shared accumulation logics.

Within this landscape, a quantified work typology (Moore, 2019), and social quantification sector has emerged (Couldry & Mejias, 2019b), signalling regimes where social and productive life have become digitalized, and therefore, become extractable material. Digitalized practices of mining, scraping, systematic review automation, and data retrieval, operate across spreadsheets, platforms, web, and databases (Kumar et al., 2024). Algorithms track productivity, sentiment, consumer behavior, and emotional states during travel or at border checkpoints (Karathanasis, 2023; Opiah, 2024). These systems represent more than technical innovations but mark normative consent conditions' collapse, and replacement by coercion, depletion, and non-reciprocity structures (Chagnon et al., 2022). Users are, in fact, directly used.

So, rather than 'data colonialism' or 'datafication', what we call *digitalized colonialism* and, digitalization, reflect the constellation of relationality that goes beyond data extraction alone, and the precise practices that require action from specific sources. A process of turning the concrete and material of living subjects to abstraction, via digitalization, is underway. This is how oppression operates. The forms of dispossession at stake do not *only* involve land seizure or forced natural resource extraction, but continuous capture of social relations (Couldry & Mejias, 2019a), sociality and subjectivity itself by specific actors e.g. Big Tech and governments. Everyday activities like searching, messaging, posting, paying, even walking through public spaces, are reconfigured as data-generating events (Powell, 2021), appropriated, stored, and processed within centralized infrastructures controlled by corporate and state actors, ensuring we are data *subjects* colonized sense, forced into new knowledge and power asymmetries.

This process differs from traditional commodification insofar as the seized material is not preformed 'property' but generated through social interaction and human experience. The capacity to render social relations as data is itself a product of historically specific socio-technical systems, dependent on abilities to quantify, categorize, and correlate human activities across time and space. This seizure echoes older colonial logics in which territorial expansion accompanied epistemic domination – imposing classificatory systems that redefined people and places according to imperial governance needs (Milan & Treré, 2019). In its contemporary form, this epistemic capture is mediated through platforms and algorithmic systems that continuously translate life into structured, computable, and tradeable forms. Cloud data centers, mobile communication networks, and algorithmic recommendation engines act as the new ports, shipping lanes, and colonial administrations of the digital order (Couldry & Mejias, 2019a).

The reconfiguration of social life as data requires not merely technological capacity but reorganization of legal, economic, and cultural systems to enable its extraction (Thatcher et al., 2016). Just as earlier colonial regimes imposed legal frameworks redefining land as property alienable from its occupants, the current digital order embeds appropriation relations within everyday digital

participation conditions. Formal consent regimes, expressed in privacy policies or 'terms of service', mask structural absence of real choice (Couldry & Mejias, 2019b). Burawoy (1970) discussed workers' 'production of consent' that is tied to their 'pragmatic role acceptance' (Mann, 1970), which is not authentic consent because there is no corresponding choice. Jaser and Tourish build on these arguments to discuss workers' 'performance of consen' (2024). Access to essential social, economic, and political infrastructures increasingly presupposes acquiescence to data capture, much as colonial economies once required participation in imposed trade systems. The right to refuse, whether to land alienation in the past or data capture in the present, foreclosed because participation in the dominant order is necessary for survival.

Digitalized colonialism thus operates as dual appropriation: capturing data as a resource and subordinating social relations through which that data is generated (Couldry & Mejias, 2019b). This duality explains why existing data protection frameworks are structurally inadequate. Such frameworks presume a pre-existing liberal subject with stable rights and capacity to exercise them through informed choice. In the colonial context here, subjectivity itself is reshaped by capture systems and acceptance require adopting the system's classificatory schemas and prescribed identities (Milan & Treré, 2019). The analogy to historical colonialism these authors make is *not* merely rhetorical. Just as imperial expansion required imposing extractive infrastructures onto subjugated territories, digitalized colonialism installs digital supply chains integrating cognitive labour, computational processing, and planetary-scale resource extraction (Couldry & Mejias, 2019b; Thatcher et al., 2016).

The global South provides much hidden labour for this system, e.g. data labeling in Philippine call centers, content moderation in Kenya, clickwork in Venezuela (Ricaurte, 2019). These activities, often low-paid and precarious, feed machine learning systems that refine the digital order's extractive capacities (Muldoon et al., 2024). Simultaneously, digital infrastructure environmental costs, these being vast energy consumption, rare-earth mineral extraction, and water usage for cooling, parallel earlier colonial resource economies' ecological devastation (Thatcher et al., 2016). Understanding digitalized colonialism also requires recognizing how it restructures knowledge production by privileging computational correlations over situated, embodied ways of knowing, particularly Indigenous, feminist, and subaltern traditions that resist quantification, making it as much about suppressing epistemic diversity as economic appropriation (Milan & Treré, 2019).

The implications for consent are profound. In the digital colonial paradigm, consenting or refusing are no longer discrete decisions, but an ongoing condition of forced relationality with extractive infrastructures. A person walking through a city with pervasive facial recognition cannot meaningfully opt out of biometric data capture, just as someone living under colonial rule could not meaningfully opt out of the imposed economic system. Individuals' control over their own data is the promise of privacy and data protection law, and perhaps should be its central premise. The promise is revealed as fiction, when everyday life infrastructures presuppose data capture for capital as its participation condition. Some argue that capitalism is over (Varoufakis, 2024; Durand, 2024), and that monopoly forms of data extraction reflect feudal forms to build capital, where domination extends beyond the material aspects of property and subsume all areas of life, including people'minds.

This structural absence of real consent means digitalized colonialism must be analysed not simply as a privacy issue but as a political-economic regime. Like earlier colonial orders, it redefines the possible's boundaries, or terms on which individuals can participate in social life, ways people can be recognized by one another, and futures we can imagine. Within this regime, subjectivity erosion is not an accidental by-product, but extraction's necessary condition The failures of human

rights support in the digital sphere must be understood within a longer trajectory in which such frameworks have repeatedly functioned to legitimise, rather than dismantle, systems of domination. Far from being a neutral vocabulary for universal dignity, human rights have historically been mobilized by institutions to stabilize the very political-economic orders they claim to regulate. As scholars of decolonial thought have noted, the post – World War II rights architecture emerged in tandem with the consolidation of U.S.-led liberal capitalism, embedding within it a particular conception of the human: individual, autonomous, and legible to bureaucratic and juridical authority.

This framing reproduced a colonial division ensuring 'universal' rights could only operate within governance modes that maintained extractive access to resources, labour, and subjectivity, making data protection legal limitations not anomalies, but inheritances of institutional histories, where recognition is only granted on the most powerful's terms. Fanon's critique of colonial humanism remains prescient here, where a colonial order could not be reformed from within, because its epistemology, the very grammar through which it named and recognized the 'human', was inseparable from the logics of domination it upheld (Fanon, 1967; 2004; Gordon, 2015). Applying this to the present, we can see that oscillation between state regulation and capitalist privatization is less a tension than a choreography: both modes rely on enclosing subjectivity within classificatory, surveillant, and extractive infrastructures. Whether through the bureaucratic rationality of public-sector governance or the market rationality of Big Tech, the condition for recognition remains the same, submission to being rendered knowable and exploitable within a system that claims universality while foreclosing alternative ways of being. Troubling this oscillation means not merely demanding better consent mechanisms or more ethical oversight, but unsettling the institutional imaginaries that make consent intelligible only as a function of capture.

Gargarella called for a manifesto for rights for the left (2023). While Gargarella is not writing about data extraction, his arguments are based in constitutional theory offering a distinctive framework for thinking about digital and data-driven society governance. Central to his idea is that law should operate as a 'conversation among equals', based on a normative commitment requiring political and legal institutions designed to guarantee effective participation of all affected persons in decision-making processes. Applied to the problems of digitalization, this perspective foregrounds the contemporary digital order's deeply asymmetrical nature, reflecting existing hierarchies of race, gender, class, and geopolitical location reproducing the 'coloniality of power' (Quijano, 2000). A Gargarella-inspired model of rights 'from' instead of just 'for' the left, would require redesigning institutional and regulatory architectures. The most affected by digitalization must have constitutive roles in shaping governing norms, reframing the struggle over digital rights as a struggle over who gets to define recognition, consent, and legitimacy terms in the digitalized order. Gargarella argues that contemporary rights frameworks are fully anchored in property rights above all else. Data, in colonial extractions, is a commodity. Protections and defence of the property objective, as though this is the most important right, are increasingly becoming institutionally and individually coercive, online and offline. Colonialism, strictly speaking, is racialized domination (Benjamin, 2016; Browne, 2015; Mbembe 2003, 2017; Mignolo, 2007; Mignolo and Walsh, 2018; Noble, 2018; Noble & Tynes, 2016) and rights to personhood are extracted and disappeared. Decolonial critiques look at data justice (Singh, 2020; Singh and Gurumurthy, 2021). Just because the internet has saturated social life does not mean we all have equal access to equality. Our arguments are epistemological but are rooted in the ontological, racialized sociotechnical regime of classification and extraction. The expanding ratio of coercive techniques for online and what is becoming offline sociality in expanding demographics mean fascism is increasingly plausible.

III. Choice, consent, coercion

Big Tech has realized the immense economic value of collecting, analysing, and monetizing traces of our digitalized lives. What were once discrete acts of online self-expression – posting a comment, browsing a product, choosing a name – have become raw material for data extraction at scale. This shift has happened largely without users' knowledge, nor understanding. The idea that digitalized life involves choice has been steadily eroded. Today, users are routinely asked to 'consent' to data collection, but under conditions that render such consent meaningless. What we are witnessing is a systemic transition: from meaningful choice, to superficial consent, to pervasive coercion embedded in digitalized participation infrastructures.

Three major forces have contributed to this erosion. First, sheer power concentration within Big Tech platforms allows them to dictate digitalized engagement terms. Second, states and regulatory bodies have largely failed to meaningfully challenge these platforms' dominance, often opting for minimal compliance or regulatory capture. Third, civil society, while increasingly aware of privacy harms, has yet to develop adequate frameworks to contest the deeper social domination dynamics that data relations involve (Mahnkopf, 1986; Sajed, 2024) Consent in this context must be understood, thus, as a social relation, not simply a procedural checkbox. While feminist theorists have problematized consent in contexts such as sexual violence, where the line between agreement and coercion is blurred (Cefai, 2023; MacKinnon, 1989; Pateman, 1980), and bioethics has established frameworks for consent in life-and-death scenarios (Beauchamp & Childress, 2019; Benjamin, 2016; Faden & Beauchamp, 1986; Miller & Wertheimer, 2010), few critical frameworks have addressed consent as a routine, everyday political relation embedded in technological infrastructures. Pateman (1980) argues, in this respect, that consent theory often suppresses its own most radical implications – namely, that 'consent' is frequently invoked to stabilize illegitimate power relations under the guise of voluntarism (Tyler and Jackson, 2014).

In digitalized contexts coercion begins long before a user even sees a consent option. Tracking technologies begin collecting data before any agreement is sought. Even when users are asked, they rarely have necessary information to make informed choices: they are not told what data will be collected, how long it will be stored, to whom it will be sold, or what inferences will be made from it. This opacity undermines any meaningful autonomy. Even when users want to withhold consent, they often cannot: refusal can lead to app malfunctions, restricted services, or total exclusion. 'Bundled consent' reduces complex terms to a single checkbox. Apps request irrelevant data access – such as geolocation for a flashlight – and make that data a precondition for use. Today, entering a website or signing up to social media is less an invitation than a demand: users are presented with large, brightly coloured 'Accept All' buttons that bundle together tracking, profiling, and data sharing permissions, while 'Manage Settings' or 'Reject' options are buried under multiple clicks or rendered in faint grey text. Consent interfaces are designed to wear down resistance – each 'no' is met with reduced functionality, constant reprompting, or inability to use the service altogether. Participation is effectively conditional on accepting surveillance, making refusal either impractical or impossible.

Equally important, the ability to revisit or reverse a consent decision is virtually nonexistent. While frameworks may include rights to ex post revision (Hansen, 2023), data extraction's permanence, especially with facial recognition, health records, or financial profiles, makes such revision ineffectual. These profiles continue to shape subjects' futures long after the original data point was captured, with no real recourse to intervene. This temporal rigidity renders the very idea of revocable consent a legal fiction.[2] These dynamics manifest in everyday situations: cookie banners that

obscure privacy settings; public announcements in train stations declaring real-time biometric surveillance (ICO, 2024); workplace practices requiring screenshots, camera monitoring, or constant audio recording. Digital infrastructures have become engines of manufactured consent, extending beyond media and communications to every life dimension (De Grazia, 1981; Herman & Chomsky, 1994). One of the clearest examples of this coerced recognition in platform governance is Facebook's enforcement of its 'real-name' policy, which requires users to register under their legal names. In 2014, the company suspended accounts of dozens of drag performers, transgender users, and others whose chosen or community-recognized names differed from their government-issued identity documents (see Holpuch, 2014). Drag artist Heklina described the experience starkly: 'I have been Heklina for 20 years … Facebook is saying Heklina no longer exists' (Tyler, 2014).

The wrongful arrest of Robert Williams in Detroit in 2020, likewise, starkly illustrates facial recognition systems' dangers and their capacity to erase personhood through machine misidentification. Arrested in front of his family and detained for thirty hours despite clear evidence of his innocence, Williams was the first publicly documented case in the United States of wrongful arrest based solely on facial recognition match. His case is not an aberration but a predictable outcome of systems that disproportionately misidentify racialized individuals: U.S. National Institute of Standards and Technology (NIST) studies show such technologies misidentify Black and Asian faces at rates up to one hundred times higher than white faces (NIST, 2019). Consent is further eroded in workplace monitoring, where digitalized tools increasingly capture and interpret workers' physical and affective states without meaningful choice or transparency. Workers report that refusal to submit to such monitoring often results in reduced functionality of essential tools or even loss of work access altogether (Fairwork, 2023). These practices progressively collapse any distinction between voluntary participation and coerced compliance.

The entanglement of coercion and consent, thus, sustains digitalized capitalism's ideological dominance. Gramsci (1971) theorized that power functions not only through force but through voluntary acceptance of domination. In the digitalized age, this hegemony is achieved through seamless blending of interface design, behavioral nudging, and infrastructural conditioning. Viljoen (2021) argues that datafication's core harm is not only that it erodes capacity for subject formation but that it reinforces and materializes unjust social relations. Neo-Gramscian scholars such as Cox (1983), Morton (2007), and Bieler and Morton (2004) show how material and ideological structures align to reproduce inequality and rule systems. Yet the accelerating collapse of even formal consent, paired with global rise of authoritarian populism, suggests a shift from consent-based hegemony toward more overt and insidious modes of control.

What is wrong with human 'rights'?

The preceding discussion has shown how conditions for meaningful consent in the digitalized sphere are rapidly collapsing, replaced by structural coercion embedded in data extraction infrastructures. If consent, recognition, and subjectivity are being eroded, what frameworks can protect individuals from harms? Human rights are often assumed to provide such protection, yet these rights were conceived to safeguard individuals from overt state abuse rather than confronting global digital capitalism's diffuse, colonial power (Madianou, 2024). D'Souza (2018) argues that there is no consistent empirical evidence that human rights enshrined in law reliably protect human beings in practice (see also Alegre, 2024). Existing frameworks are largely abstract, functioning as idealized statements, but their capacity to confront entrenched corporate and technological

power is minimal. Social movement studies should reconsider their reliance on rights discourse as the primary means of achieving justice, instead interrogating how rights might be re-imagined to serve transformative, left-oriented political projects that prioritize structural change over symbolic recognition. Current legal regimes offer little protection for data subjects' relationality – for conditions under which individuals can control how they are recognized and represented in digitalized systems. When consent is hollowed out, the capacity to sustain subjectivity and refuse imposed recognition forms, is also eroded.

Human rights protections for personhood, likeness, and will-formation

Grounded in liberal assumptions of static legal subjectivity, individual autonomy, and procedural fairness, the dominant rights frameworks we now address come from an anglo-centric purview do not account for collective dispossession, structural misrecognition, and extractive architectures underpinning today's data infrastructures. Rather than protecting users, dominant Western frameworks legitimize the surveillance (Zuboff 2019a, 2019b), profiling, and coercive systems they regulate. The digitalized sphere no longer offers space for experimentation or self-invention but instead enforces legibility and conformity. As this coercive dynamic intensifies, subjectivity itself becomes a site of extraction and control (Moore, 2024), demanding a political response that reclaims conditions for recognition, refusal, and collective autonomy (Chun, 2021; Clemons et al., 2024).

Legal protections for 'personhood' and 'likeness' often collapse into narrow, technical forms of individualization. In the context of digital rights, such frameworks rarely deliver meaningful remedies. Two central problems stand out. First, mainstream rights approaches tend to focus on the suffering of the victim rather than on the structural abuse of power – diverting attention away from Big Tech as the systemic perpetrator. Second, they depict the data subject as already possessing the legal status and rights needed to claim protection. This assumption ignores the social and political work required to make such rights materially accessible, particularly in the domain of data extractivism. Our critique focuses on European law and its associated rights protections, as colonial power structures are rooted in European legal traditions.

Current frameworks do not recognize the agency of data subjects in any sense; nor do they establish the fundamental relational right to consent; nor the right to self-formation, at least not outside of capitalist norms of ownership, that make individuals responsible for managing their own exposure and vulnerability (Rose, 1992). This overriding emphasis on individual responsibility obscures the structural conditions that make meaningful choice impossible, perpetuating cycles of harm while absolving powerful actors of accountability.

Existing human rights regimes tend to preserve the institutional status quo and invisibilize harms, rather than transform, or even disrupt. D'Souza (2018) questions the validity of the term 'human' in 'human rights', noting that it presupposes the human as an abstract, pre-social entity divorced from material conditions and power relations. In the legal treatment of data extractivist social relations, agency is often displaced onto machinic actors – algorithms, systems, automated decision makers – while the human role in designing, deploying, and profiting from these technologies is systematically obscured. This displacement allows harm to be reframed as the neutral consequence of 'calculation' or 'automation', even within Western technology law's rhetorical commitment to 'human centredness' (Colclough, 2024; Holistic AI, 2024). Hildebrandt (2015), in particular, warns that such smart technologies can 'undermine, reconfigure and overrule' constitutional democracy itself, challenging the foundational assumptions upon which liberal rights frameworks depend.

The category of the 'human' in these contexts is rarely interrogated with the rigor it demands. Technology law often invokes the need for a 'human in the loop' as a safeguard against algorithmic harm, but without clarifying who this human is, how they are positioned within power structures, what resources they possess, or what meaningful role they can actually play in rights protection. Adams-Prassl et al. (2023) note significant conceptual slippage between the human in the loop, before the loop, after the loop, and above the loop – distinctions that fundamentally alter the nature and effectiveness of oversight.[3] These epistemological gaps undermine the credibility of 'human in the loop' safeguards as meaningful protections and reveal them as largely performative gestures.

Keeping a human 'in the loop' in data governance is ostensibly intended to protect rights, yet this formulation is fundamentally tautological: it assumes a human subject whose identity is already fixed by law and whose legitimacy as a rights bearer depends entirely on that prescribed identity. This logic forecloses the possibility of choosing among a constellation of possible selves, thereby limiting the agency necessary for genuine self-determination – a particularly urgent concern as new profiling technologies and intensifying data extraction make subjectivity itself the primary site of contestation, 'shifting the site of identification into a digital sphere' (Zehner, 2019).

Other areas of law do not require such constant reaffirmation of humanity or anxious delimitation of the human subject. Labour law does not need to assert repeatedly that workers, managers, or interns are people, rather than machines. Contract law does not need to clarify obsessively that a solicitor is a person or that a legal document possesses documentary rather than human status. Nor does commercial law need to remind anyone that a banana is not an orange, or that goods possess different properties than services. Yet in the realm of digital rights, where identity and recognition are continually mediated, reconstructed, and contested by algorithmic systems, this struggle over defining and protecting the 'human' becomes unavoidable, and exposes the fundamental limits and internal contradictions of existing legal frameworks. Visibility of a human in the loop does not automatically produce solutions. But if the oppressor is unnamed, remedies remain illusory, and victims risk being held responsible for their own oppression.

Rights assume other rights, despite non-consented 'recognition'

Western liberal rights are part of a long-standing colonial project. The rights that citizens of the European Union are formally entitled to claim are explicitly articulated in the Treaty on European Union, Article 2: respect for human dignity; freedom; democracy; equality; the rule of law; and respect for human rights, including the rights of persons belonging to minorities. In theory, these rights function as foundational principles of the Union's constitutional order, guiding both legislation and governance. In principle, they are invoked in political rhetoric as evidence of the EU's moral and democratic legitimacy, and in legal contexts as a benchmark for assessing compliance with European norms. However in practice, they become increasingly difficult to defend, because of the erosion of consent for how one is recognized by power holders, which is, ultimately, a moral question.

It is worth revisiting these moral questions to ask 'In order to be involved as morally responsible persons, individuals need not only legal protection from interference in their sphere of liberty, but also the legally assured opportunity for participation in the public process of will-formation, an opportunity that they can only actually take advantage of, however, if they also have *a* certain social standard of living' (Honneth, 1995, p. 117; also see Fraser & Honneth, 2003). This fundamental tension in liberal democratic theory becomes acute in the context of digital rights and digital recognition. First, the notion of 'morally responsible persons' presupposes autonomous decision-

making capacity to e.g. consent to data collection about the self, but this itself must be socially cultivated. Nevertheless, algorithmic systems recognize, categorize, and make decisions about individuals without meaningful participation in recognition processes. Legally assured opportunity for participation in the public process of will-formation encompasses the broader capacity to shape one's social identity and influence how one appears in public discourse, particularly relevant to digital rights because algorithmic profiling and biometric recognition systems essentially participate in and have an impact on digitalized representations which become socially and economically consequential, without the subject's input or consent. Legitimacy of law is recursively reliant on assumed public consent (Tyler and Jackson, 2014).

Third, participation in rights frameworks requires a certain social standard of living concerning not merely material resources, but also social, cultural, and technological literacy necessary to engage meaningfully with complex systems of recognition and representation. This creates a recognition gap, where those lacking sufficient social standing or resources are most vulnerable to having their identities constructed by algorithmic systems whilst also being least equipped to challenge these processes, with implications extending beyond individual privacy to democratic participation itself. Digitalized, data-driven recognition systems increasingly mediate access to employment, credit, social services, and other opportunities. Honneth was not writing about digital rights, but his focus on the dangers of a reduction of access to will-formation for humans, sourcing foundational philosophers (Hegel), matters.

The right to will-formation is not the same as the right to claim you own your face, and it is your individual property. Ownership, however, is really as far as debates have come for legal protections, such as Denmark's Copyright Act reform, planning to give citizens the 'right to their own facial features, voice and body' (Global Legal Group, 2025). The Global Legal Group report cited here, however, seems to leave out a word between the words [right to], and the word [their own]. Should this state: the right to [own]? If so, does this mean no Danish person owned their face until now? Does this only mean right to [defend] and to defend what? The face, or corrupted images of the face? Right to [change]? Right to [consent to what happens with the image data] and at what stage? Is it in the first data capture moment, or is is [after deep fake is posted]? Image data 'ownership' is not identical to a right to will or liberty to decide what your face looks like (such as in the case of plastic surgery or botox acquisition) nor the right to decide who one is, whether to do with gender, political views, and religion, but whether practices such as loitering or walking slowly are signs of your personality type or criminal activity. Questions of identity and recognition are increasingly linked to biometric data extraction, whether one has consented to data extraction, or not.

The right to own your own image is not the same as the right to the surrounding social relations of recognition, and it certainly does not overturn structural inequalities. Rather than the right to your face, the right to will-formation as linked to identity itself, and access to formation of the same, should be fundamental in rights frameworks internationally. Malgieri (2023) addresses this question, arguing that 'data subject' as a human identification category is insufficient, because there is no truly average data subject. An added anomaly emerges with biometric digital rights. The paradox is that biometric data only exists based on human identity, yet definitively contains within its procedural apparatus as being data in itself, an objectifying role. Biometric data automatically attributes the identifier with labelling power, and the power to identify another human, and therefore to prescribe an identity. There is a specific relationality question which must be asked to prevent rights violations in biometric profiling and deepfakes (see Ajana, 2020) which cannot be resolved by property ownership strategies typically seen in rights frameworks, as Gargarella argues.

The GDPR provides criteria for Lawfulness of Processing, indicating that data collection, processing and usage can be defended as lawful 'only if and to the extent that at least one of the following applies' (GDPR Art. 6): consent; contract necessity; legal obligation compliance; vital interests protection; public interest tasks; or legitimate interests. The first criterion, consent, may be the most complicated and difficult to achieve for reasons seen above, while the sixth, legitimate interest, is the most general and requires further justification based on the type of interest being reflected (usually business-focussed interests).

Balboni et al. (2013) wrote even before the GDPR rollout, an excellent analysis of the difficulties in selecting criteria for lawfulness for data extraction, because this requires 'an appropriate balance between the protection of personal data and data subjects' rights, the smooth flow of information across the EU (and beyond), and economic opportunity and privacy compatible growth in line with the expectations of society (the 'appropriate balance')'. The GDPR explicitly states that personal data relates to 'an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person' (GDPR, Art 4), and many technologies record items that allow for identifying such aspects of a natural person.

Biometric data is quietly extracted and analysed, infiltrating the emotional texture of working life and undermining the very possibility of meaningful consent – especially for those already in vulnerable social positions. The EU AI Act bans systems designed to infer emotions in workplaces or education, except for medical or safety reasons, and prohibits biometric profiling for social scoring that could lead to disproportionate or harmful treatment. Affective computing and facial recognition (FR) are among the most troubling frontiers of data hyper – colonialism, in this regard, where machines not only identify people but also attempt to read their emotions Yet in the UK, ow beyond EU jurisdiction, biometric tracking is expanding rapidly. Emotion recognition and algorithmic affect management (Moore et al., 2024), are spreading in workplaces. Pasquale warns that such systems foster 'misrecognition, privacy invasion, modulation, and alienation' (Pasquale, 2024). Police use of FR is rising, with shoplifter databases (Skelton, 2024) helping to normalize technologies banned in much of Europe. Racial profiling is emerging even as black faces are systematically misrecognised and minority groups oppressed (see Burton-Harris and Mayor, 2020; Eubanks, 2018).

The spread of technologically trained biometric systems raises crucial questions about privacy, discrimination, and the right to a non-exposed emotional life. These rights are deeply relational and subjective (Noble, 2018), yet existing EU protections do little to guard against the psychosocial harm caused by misrecognition (Raposo, 2024). One person wrongly flagged as a shoplifter, for example, endured significant distress before the error was revealed (Clayton, 2024). Such harms are hard to prevent because FR often operates invisibly, justified by a long list of seemingly practical uses: unlocking phones, finding missing persons, preventing shoplifting, banking security, healthcare, gambling monitoring, law enforcement, and attendance tracking (Einorytė, 2024). Discrimination by proxy remains a serious and under – acknowledged threat to mental and social well – being (Hajian & Domingo-Ferrer, 2013; Veale & Binns, 2017).

The removal of the right to recognition (Honneth, 1995; Taylor, 1985, 1989, 1996) is linked to the politics and struggle for identity, and misidentification and its impact on data subjects is insufficiently addressed in leftist debates. The right to 'likeness' appears in some research (Goffman, 1959; Hogan, 2023), but there is insufficient research on the converse to recognition, where misrecognition is also generated from or by machines (Waelen, 2022). This can be seen either less intentionally in FR mistakes or intentionally, where personae hacking leads to online slander and cancel culture. Ideally, our data doubles and digital twins are only made possible via

our own involvement in crafting them (Boddington, 2024; Ruckenstein, 2014), but access to consent must first be secured.

IV. A manifesto for 'digital rights from the left': reclaiming dignity and recognition

A manifesto for 'digital rights from the left' is urgently needed to correct the fundamental harms outlined throughout this analysis. This approach involves forming a theory of rights and recognition from the left that moves beyond the traditional rights-based framework, which has proven complicit in prolonging oppression and digitalized colonialism. Rather than merely reforming existing structures, this manifesto acknowledges their inherent limitations and proposes radical transformations of how we conceive of human dignity, autonomy, and recognition in the digitalized age.

The current liberal rights framework, while appearing protective on its surface, operates within a system that fundamentally prioritizes capital accumulation and technological efficiency over human flourishing and democratic participation. This creates what we might call a 'rights paradox' – where formal protections exist alongside systematic exploitation, where consent mechanisms coexist with coercive data extraction practices, and where privacy rights are undermined by the very economic structures they purport to regulate. A leftist approach to rights must therefore be fundamentally redistributive, recognizing that true protection requires not just legal frameworks but material conditions that enable meaningful choice and resistance.

As Cheney-Lippold (2017) reminds us in *We Are Data*, *Algorithms and the making of our digital selves* digitalized subjectivity is not simply a matter of legally recognized personhood, but is continuously produced through algorithmic classification systems that operate outside the reach of formal law. These systems assign us shifting, probabilistic identities that shape access, visibility, and life chances, regardless of whether such identities align with our self understanding. In this sense, digitalized subjection exposes the insufficiency of rights frameworks grounded solely in the juridical subject. If power operates through extra – legal infrastructures that classify, sort, and govern us before we enter any legal or social relation, then a manifesto for 'digital rights from the left' must directly confront these formations. It must articulate protections and refusals that address not only how subjects are recognized in law, but also how they are *made* in code, in markets, and in the opaque architectures of algorithmic governance.

At present, the experience of entering a social media platform or visiting a website is structured to maximize extraction rather than facilitate informed choice. A new user is typically met with a wall of prompts: 'accept all cookies' buttons in large, brightly coloured fonts; privacy settings hidden behind multiple clicks; and consent forms bundled with unrelated permissions, such as agreeing to share geolocation data to post a photo. Opting out often means degraded functionality, loss of access, or unusable interface. In a rights-driven model, this entry point would be inverted. Cookie and consent prompts would default to no tracking, with clear, plain language explanations of what each type of data collection does, who uses it, and for what purpose. Consent would be granular: location sharing, behavioral tracking, and personalization would each require separate, affirmative choice, with 'no' causing no loss of basic functionality. On social media platforms, users would have the option to engage in 'tracking-free mode' by default, algorithms could be turned on only with explicit consent, and content could be viewed in purely chronological order.

For this purpose, we propose a manifesto for rights from, and for, the left, because of the limitations in existing rights frameworks, moving toward a more comprehensive framework for digital liberation:

Purpose Limitation and Analogue Alternatives: The right to privacy must be protected through absolute purpose limitation, where any time there is a way to carry out any transaction in the public or private sector, an analogue method – one that does not involve collecting, processing, and storing personal data – becomes the required default method. This principle challenges technological determinism that assumes digitalized solutions are inherently superior, instead prioritizing human agency and choice.

Meaningful Consent and Meaningful Refusal: The right to consent to data being gathered and used for decision-making must be meaningfully matched with an equally robust right to refuse, backed by material protections that ensure refusal does not result in social or economic exclusion. This means creating parallel systems, public options, and legal protections that guarantee access to essential services regardless of one's willingness to submit to data extraction.

Immediate Data Access and Withdrawal Rights: Data subjects must have automatic, immediate access to all data collected about them, along with the unconditional right to withdraw it from public or private domains before processing occurs and therefore before it can be used for profiling purposes. This proactive approach is essential for preventing inference-based discrimination and algorithmic profiling that creates digitalized redlining and social sorting.

Recognition, Redistribution, and Rights Integration: Digital rights from the left must be intrinsically connected to recognition rights and redistribution rights, forming an integrated framework that addresses the material, social, and cultural dimensions of digitalized oppression. This means that data protection cannot be separated from broader struggles for economic justice, racial equity, gender liberation, and democratic participation.

Subjectivity and Recognition Protection: There is currently no automatic right to protection of personality and subjectivity within existing rights frameworks (see Brüggemeier 2009 for examples in European law). A leftist approach demands the right to personally construed subjectivity and therefore to be correctly recognized, as well as the fundamental right not to be misrecognized by algorithmic systems. This extends beyond accuracy to encompass the right to complexity, contradiction, and change – recognizing that human identity cannot be reduced to data points or algorithmic predictions.

Self-Identification and Anonymity Balance: A comprehensive 'digital rights from the left' framework must include the enforceable right not to be misrecognized, incorporating data subjects' rights to choice in self-identification, the right to sociality and integrity, and the right to be recognized on one's own terms. Simultaneously, any rights for recognition must be balanced with equally strong rights to anonymity, allowing individuals to move through digital and physical spaces without constant identification and tracking.

Corporate Power and Antitrust Enforcement: Enforceable rights require more than frameworks of normative ideals, they demand concrete mechanisms to restrict data extraction by Big Tech companies through robust competition and antitrust law. This means treating data accumulation as a form of monopolization, breaking up tech giants, and creating public alternatives to essential digitalized infrastructure.

Accountability over Victimization: The right to recognition must shift focus from victimhood to accountability, placing responsibility squarely on the abuse of power that occurs through data use by public and private entities. This means protecting victims' identities and maintaining anonymity where data subjects desire it, while simultaneously ensuring that those who cause harm through algorithmic discrimination, surveillance, and digitalized exploitation face meaningful consequences.

These digital rights demand legislative interventions that both prohibit the most coercive technologies, including real-time facial recognition in public spaces, emotion recognition in workplaces

and schools, and biometric categorization based on race or gender, and mandate data minimization as a binding default with independent oversight empowered to audit and sanction violations. Beyond prohibitions, rights-based reform must resource non-extractive alternatives through public funding for cooperative, community-owned digitalized infrastructures operating on principles of data sovereignty, while requiring platforms and employers to offer full functionality without forcing users into profiling regimes, thereby protecting the right to refuse without loss of access or essential services. Transparency requirements must extend to source code, training data, and algorithmic decision-making logic, with enforceable rights to contest automated decisions, creating a comprehensive framework that moves beyond proceduralism toward substantive protection of digital autonomy.

Legislative boundaries against coercive data practices will only hold if anchored in a broader culture of resistance that confronts the opacity and silent violence of digitalized extraction and what Ajunwa calls 'data laundering' (2020), through promoting shared political literacy – requiring public education campaigns, citizen assemblies on technology governance, and data justice curricula that demystify infrastructures currently operating beyond public scrutiny. This resistance must be organized through worker-led campaigns against biometric workplace tracking, tenant associations opposing facial recognition systems, grassroots coalitions mobilizing against algorithmic police surveillance, and cross-movement alliances linking digital rights advocates with climate, racial, and labour justice organizations to reframe data hyper-colonialism as part of a larger struggle against extractive power.

This manifesto represents more than a wish list, it constitutes a call for fundamental transformation of the relationship between technology, power, and human dignity. These suggestions for reclaiming 'rights' from allegedly protective data and privacy policies are increasingly urgent because hyper-extraction, based on systematic coercion, is beginning to invade humanity's very subjectivities and our collective right to consent to our shared future. The choice before us is not between privacy and convenience, but between digital liberation and technological authoritarianism.

V. Conclusion: toward digital rights from the left

In contemporary regimes of data hyper-extraction, humans occupy a position of inherent vulnerability because they lack the substantive right to determine how any aspect of their humanity is depicted, interpreted, or operationalized in digitalized systems. The capacity to meaningfully consent to the collection of personal data is already tenuous; the ability to consent to the interpretation of that data to the inferences, profiles, and acts of recognition generated from it is almost entirely absent. People now experience minimal access to any form of consented, much less self-chosen, relationality in their data relations. This erosion occurs in parallel with the broader deterioration of the material and ecological conditions in which rights are exercised, conditions shaped by the accelerating 'green transition' that is itself entangled with ecological crisis. These logics extract agency, constraining both individual and collective capacities to shape one's own digital and social existence.

Our position is not simply to advocate for wholesale abandonment of digitalization processes but to reject the extractivist, profit-driven model that currently govern these processes. Digitalization is entangled with massive ecological costs, deepening authoritarian governance, and consolidating data dominance over populations. Without a revolution of its political economy, one that prioritizes ecological sustainability, collective data sovereignty, and democratic oversight, further

expansion risks entrenching these harms rather than addressing them. Indeed, the question is not whether digitalization should continue, but under what terms, and for whose benefit. Current dominant corporate-controlled, extractive political and economic logics are incompatible with democratic, ecological, and relational rights and will exacerbate rather than alleviate current crises, unless radically re-oriented toward public interest goals under enforceable limits. Without intervention, we face the entrenchment of a data hypercolonial order where biometric surveillance, algorithmic profiling, and consent manipulation become pervasive structural features of everyday life, demanding strong legal prohibitions, enforceable rights to refuse profiling without loss of access, mandatory data minimization by default, and treatment of algorithmic management as a labour rights issue. Yet legislation alone is insufficient. Social resistance through workers' unions, civil society organizations, and community movements must press for abolition of coercive biometric systems while advocating for publicly funded, non-extractive digitalized infrastructures that serve collective rather than corporate interests.

These conditions gesture toward data domination in the Gramscian sense: a situation in which the rights to sociality, dignity, self-formation, and subjectivity – and, more fundamentally, the right to consent – are all subordinated to the imperatives of extraction. Human rights frameworks neither meaningfully recognize nor adequately protect the relational and collective dimensions of the human condition. Even within Europe, the allegedly strongest and most socially democratic, existing frameworks are insufficient because they leave intact the capitalist epistemologies that sustain them. Legal and policy discourses continue to prioritize values and ethics in the abstract, even embedding them within data protection regulations (Veale & Binns, 2017), yet these rhetorical commitments have not translated into material protections.

When a person's worth is quantified through opaque, metrics-driven evaluative scores that circulate as truth claims, the twin logics of digital and ecological extraction converge into hyper-destruction. The human subject is progressively stripped of the right to define one's own subjectivity, to exercise agency in digital environments, and ultimately, to participate as a fully recognized actor in social and political life. On the platforms that mediate much of our existence, coercion now consistently exceeds consent. This signals the collapse of the liberal promise of a consensual social contract in the digital realm, and the emergence of a new hegemonic order in which domination is normalized via digitalization. Future research must grapple with what Donoghue (2024) terms the 'bio-psycho-socio-economic implications' of algorithmic management and AI integration into everyday life, where the overcoding of desire is molding fascist subjects (Faramelli and Piper, 2022).

Our call for digital rights from the left is not a peripheral addition to existing frameworks, but a demand for their fundamental reorientation where people, as Brett Zehner said to the current author Moore in August 2025: 'sieze the means of consent'. Such rights must transcend the liberal fixation on individual autonomy toward a collective, relational, and anti-colonial politics of recognition and refusal. A politics of digital rights from the left should be abolitionist in its horizon, refusing the inevitability of data domination and insisting on the right to be untracked, unprofiled, and uncoerced. Anything less will concede the digitalized transitions to the same extractive forces that have historically dispossessed communities of land, labour, identities, and futures.

Notes

1. Data extraction involves data collection from a source, where preparation for processing and storage involves categorization, consolidation and potentially, integration. Also called mining, scraping, systematic review automation, and retrieval, this is where data is extracted from spreadsheets, platforms,

the web, databases and other sources. To be used for profiling, data is organized consolidated and placed into centralized locations, where data sets are stored within data lakes, and organized into data hubs, which cultivate and generate forms of AI. In this sense, this is first step in the extract, transform, load (ETL) or extract, load, transform (ELT) processes (Bartley, 2024; Schmidt et al., 2021).

2. See Gilbert (2024) for an account of where even non-personal data is creating tensions for workers.
3. Adams-Prassl et al. (2023) argue that to restore human agency in data and algorithmic management systems, a series of redlines must be established, where the concept of humans being in the loop to justify or oversee data extraction should be expanded so that this would refer to 'in the loop' being linked to banning fully automated terminations; 'after the loop' referring to the right to meaningful review; 'before the loop' having to do with information and consultation rights being granted; and 'above the loop' meaning there are impact assessments when data extraction is intended.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Notes on contributors

Phoebe V. Moore is a Professor of Management and the Futures of Work at Essex Business School, University of Essex.

Peter Bloom is a Professor of Management at Essex Business School, University of Essex.

Rodrigo Nunes is an Associate Professor of Political Theory and Organization, at Essex Business School, University of Essex.

Acknowledgments

Authors would like to thank three anonymous reviewers for extremely helpful comments. Authors thank Essex Business School for providing funding for Open Access. Moore would like to thank the Copenhagen Business School JURASOC Research Group for excellent comments during the research seminar where she presented earlier versions of the paper, including Andrej Savin, Negar Mansouri, Benjamin Ask Popp-Madsen, and Marianne Jade Buffat.

ORCID

Phoebe V. Moore http://orcid.org/0000-0002-8254-070X

References

Adams-Prassl, J., Abraha, H., Kelly-Lyth, A., Silberman, M. S., & Rakshita, S. (2023). Regulating algorithmic management: A blueprint. *European Labour Law Journal*, *14*(2), 124–151. https://doi.org/10.1177/20319525231167299

Ajana, B. (2020). Biometric datafication in governmental and personal spheres. In N. Lushetich (Ed.), *Big data: A new medium?* Routledge.

Ajunwa, I. (2020). The 'black box' at work. *Big Data & Society*, *7*(2). https://doi.org/10.1177/2053951720938093

Alegre, S. (2024). *Human rights, robot wrongs: Being human in the age of AI*. Atlantic Books.

Balboni, P., Cooper, D., Imperiali, R., & Macenaite, M. (2013). Legitimate interest of the data controller new data protection paradigm: Legitimacy grounded on appropriate protection. *International Data Privacy Law*, *3*(4), 244–261. https://doi.org/10.1093/idpl/ipt019

Bartley, K. (2024). *ELT vs ELT: What's the difference?* https://rivery.io/blog/etl-vs-elt/.

Beauchamp, T. L., & Childress, J. F. (2019). *Principle of biomedical ethics*. Oxford University Press.

Benjamin, R. (2016). Informed Refusal: Toward a justice-based bioethics. *Science, Technology, & Human Values*, *41*(6), 967–990. https://doi.org/10.1177/0162243916656059
Berardi, F. B. (2024, October 9). Hyper-colonialism and semio-capitalism. *e-flux*.
Bieler, A., & Morton, A. D. (2004). A critical theory route to hegemony, world order and historical change: Neo-Gramscian perspectives in International Relations. *Capital and Class*, *28*(1), 85–113. https://doi.org/10.1177/030981680408200106
Boddington, G. (2023). *The extended self: Our future digital twins (Fast Forward S2), podcast*. https://fastforward.podbean.com/e/digital-healthcare-technology/
Browne, S. (2015). *Dark matters: On the surveillance of Blackness*. Duke University Press.
Brüggemeier, G. (2009). Protection of personality interests in continental Europe: The examples of France, Germany and Italy, and a European Perspective. In N. R. Whitty, & R. Zimmermann (Eds.), *Rights of personality in Scots law*. Dundee University Press.
Burawoy, M. (1970). *Manufacturing Consent: Changes in the Labor Process Under Monopoly Capitalism*. University of Chicago Press.
Burton-Harris, V., & Mayor, P. (2020, June 24). *Wrongfully arrested because face recognition can't tell Black people apart* [Press release]. American Civil Liberties Union.
Cefai, S. (2023). Consent-deception: A feminist cultural media theory of commonsense consent. *Feminist Theory*, *25*(3), 471–492. https://doi.org/10.1177/14647001231206026
Chagnon, C. W., Durante, F., Gills, B. K., Hagolani-Albov, S. E., Hokkanen, S., Kangasluoma, S. M. J., & Vuola, M. P. S. (2022). From extractivism to global extractivism: The evolution of an organising concept. *The Journal of Peasant Studies*, *49*(4), 760–792. https://doi.org/10.1080/03066150.2022.2069015
Cheney-Lippold, J. (2017). *We are data: Algorithms and the making of our digital selves*. New York University Press.
Chun, W. H. K. (2021). *Discriminating data: Correlation, neighborhoods, and the new politics of recognition*. MIT Press.
Clayton, J. (2024). I was misidentified as shoplifter by facial recognition tech. *BBC Newsnight*. https://www.bbc.co.uk/news/technology-69055945
Clemons, E. K., Savin, A., Schreieck, M., Teilmann-Lock, S., Trsazkowski, J., & Waran, R. (2024). A face of one's own: The role of an online personae in a digital age and the right to control one's own online personae in the presence of digital hacking. *Electron Markets*, *34*(1), 31. https://doi.org/10.1007/s12525-024-00713-3
Colclough, C. (2024). Christina Colclough's commentary, chapter 18. In C. Régis, J. Denis, M. L. Axente, & A. Kishimoto (Eds.), *Human-centered AI: A multidisciplinary perspective for policy-makers, auditors, and users*. CRC Press.
Couldry, N., & Mejias, U. A. (2019a). *The costs of connection: How data is colonising human life and appropriating it for capitalism*. Stanford University Press.
Couldry, N., & Mejias, U. A. (2019b). Data colonialism: Rethinking big data's relation to the Contemporary Subject. *Television & New Media*, *20*(4), 336–349. https://doi.org/10.1177/1527476418796632
Cox, R. W. (1983). Gramsci, hegemony and International Relations: An Essay in Method. *Millennium*, *12*(2), 162–175. https://doi.org/10.1177/03058298830120020701
De Grazia, V. (1981). *The culture of consent: Mass organization of leisure in fascist Italy*. Cambridge University Press.
Donoghue, R. (2024). Algorithmic management: A threat to the freedom of workers as choosing subjects. Unpublished.
D'Souza, R. (2018). *What's wrong with rights? Social Movements, Law and Liberal Imaginations*. Pluto Press.
Durand, C. (2024). *How Silicon Valley unleashed techno-feudalism: The making of the digital economy*. Verso.
Einorytė, A. (2024, July 17). Facial recognition: Everything you need to know. *NordVPN*.
Eubanks, V. (2018). *Automating inequality: How high-tech tools profile, police, and punish the poor*. St. Martin's Press.
Faden, R. R., & Beauchamp, T. L. (1986). *The history and theory of informed consent*. Oxford University Press.
Fairwork. (2023). *Fairwork annual report 2023: State of the global platform economy*. Oxford Internet Institute, University of Oxford, & WZB Berlin Social Science Center.
Fanon, F. (1967). *Black Skin, White Masks* (C. L. Markmann, Trans.). Grove Press.
Fanon, F. (2004). *The Wretched of the Earth* (R. Philcox, Trans.). Grove Press.

Faramelli, A., & Piper, I. (2022). Everybody wants to be a fascist online: Psychoanalysis and the digital architecture of fascism. *CLCWeb: Comparative Literature and Culture*, *24*(4).
Fraser, N., & Honneth, A. (2003). *Redistribution or recognition? A political-philosophical exchange*. Verso.
Gargarella, R. (2023). *Manifiesto por un derecho de izquierda* (1st ed.). Siglo XXI Editores.
Gilbert, A. (2024). How important is non-personal data? And how might worker, firm and national interests align around its governance? Institute for the Future of Work blog 23/09/24
Global Legal Group. (2025, July 1). *Denmark takes action to tackle deepfake harms*. https://iclg.com/news/22776-denmark-takes-action-to-tackle-deepfake-harms
Goffman, E. (1959). *The presentation of self in everyday life*. Doubleday.
Gordon, L. R. (2015). *What Fanon Said: A Philosophical Introduction to His Life and Thought*. Fordham University Press.
Gramsci, A. (1971). *Selections from the Prison Notebooks*. Translated from Italian by Hoare, Q. and Nowell Smith, G. Lawrence and Wishart.
Hajian, S., & Domingo-Ferrer, J. (2013). A methodology for direct and indirect discrimination prevention in data mining. *IEEE Transactions on Knowledge and Data Engineering*, *25*(7), 1445–1459. https://doi.org/10.1109/TKDE.2012.72
Hansen, H. K. (2023). Governing through metrics in the digital age. *Globalizations*, *20*(1), 137–152. https://doi.org/10.1080/14747731.2022.2156700
Herman, E. S., & Chomsky, N. (1994). *Manufacturing consent: The political economy of the mass media*. Vintage.
Hildebrandt, M. (2015). *Smart technologies and the end(s) of law*. Edward Elgar.
Hogan, B. (2023). *The Proper Likeness and the models that matter*. Presentation for Channels of Digital Scholarship workshop, 02/02/23, Maison Française d'Oxford.
Holistic AI. (2024). *Key issues: Human oversight*. EU AI Act. https://www.euaiact.com/key-issue/4.
Holpuch, A. (2014, October 1). Victory for drag queens as Facebook apologises for 'real – name' policy. *The Guardian*.
Honneth, A. (1995). *The struggle for recognition: The moral grammar of social conflicts*. Polity Press.
Information Commissioner's Office. (2024, March 23). *ICO orders Serco Leisure to stop using facial recognition technology to monitor attendance of leisure centre employees*.
Jaser, Z., & Tourish, D. (2024). Hegemonic surveillance at work: Fabricating the cyberised, totalised and thespianised employee. *Organization Theory*, *5*(1). https://doi.org/10.1177/26317877241235940
Karathanasis, T. (2023, October 20). EU iBorderCtrl: When Commercial Interests outweigh the Public Interest. *Team AI Regulation*.
Kumar, V., Ashraf, A. R., & Nadeem, W. (2024). AI-powered marketing: What, where, and how? *International Journal of Information Management*, *77*, 102783. https://doi.org/10.1016/j.ijinfomgt.2024.102783
MacKinnon, C. A. (1989). *Rape: On coercion and consent. From Toward a feminist theory of the state*. Harvard University Press.
Madianou, M. (2024). *Technocolonialism: When technology for good is harmful*. Polity.
Mahnkopf, B. (1986). Hegemony and consent: Patterns of regulation in internal company social relations and their legitimation effect. *Berkeley Journal of Sociology*, *31*, 35–52.
Malgieri, G. (2023). Vulnerability and data protection law. In *Oxford data protection & privacy law* (Online ed.). Oxford Academic.
Mann, M. (1970). The social cohesion of liberal democracy. *American Sociological Review*, *35*(3), 423–439. https://doi.org/10.2307/2092986
Mbembe, A. (2003). Necropolitics. *Public Culture*, *15*(1), 11–40.
Mbembe, A. (2017). *Critique of Black reason*. Duke University Press.
Mignolo, W. D. (2007). Delinking: The rhetoric of modernity, the logic of coloniality and the grammar of decoloniality. *Cultural Studies*, *21*(2–3), 449–514.
Mignolo, W. D., & Walsh, C. E. (2018). *On decoloniality: Concepts, analytics, praxis*. Duke University Press.
Milan, S., & Treré, E. (2019). Big data from the South(s): Beyond data universalism. *Television & New Media*, *20*(4), 319–335. https://doi.org/10.1177/1527476419837739
Miller, F. G., & Wertheimer, A. (2010). *The ethics of consent: Theory and practice*. Oxford University Press.
Moore, P. (2019). *The quantified self in precarity: Work, technology and what counts*. Routledge.

Moore, P. (2024). Workers' right to the subject: The social relations of data production. *Convergence*, *30*(3), 1076–1098.
Moore, P., Barnard, G., & Thomas, A. (2024). *Data on our minds: Affective computing at work*. Institute for the Future of Work.
Morton, A. D. (2007). *Unravelling Gramsci: Hegemony and passive revolution in the global political economy*. Verso.
Muldoon, J., Graham, M., & Cant, C. (2024). *Feeding the machine: The hidden human labour powering AI*. Canongate Books.
National Institute of Standards and Technology. (2019, December). *Face recognition vendor test (FRVT), Part 3: Demographic effects (NIST Interagency/Internal Report No. 8280)*. U.S. Department of Commerce.
Noble, S. (2018). *Algorithms of oppression: How search engines reinforce racism*. NYU Press.
Noble, S. U. (2018). *Algorithms of oppression: How search engines reinforce racism*. NYU Press.
Noble, S. U., & Tynes, B. M. (2016). *The intersectional internet: Race, sex, class, and culture online*. Peter Lang.
Opiah, A. (2024, June 18). UK train stations trial Amazon emotion recognition on passengers. *Biometric Update*.
Pasquale, F. (2024). Affective computing at work: Rationales for regulating emotion attribution and manipulation. In A. Ponce Del Castillo (Ed.), *Artificial intelligence, labour and society* (pp. 175–179). The European Trade Union Institute.
Pateman, C. (1980). Women and consent. *Political Theory*, *8*(2), 149–168. https://doi.org/10.1177/009059178000800202
Petrosino, A. (2024). Coercion and Consent in Automated Management. *Digital Society*, *61*(3), 1–17.
Powell, A. (2021). *Undoing optimization civic action in smart cities*. Yale University Press.
Quijano, A. (2000). Coloniality of Power and Eurocentrism in Latin America. *International Sociology*, *15*(2), 215–232.
Raposo, V. L. (2024). When facial recognition does not 'recognise': Erroneous identifications and resulting liabilities. *AI & SOCIETY*, *39*(4), 1857–1869. https://doi.org/10.1007/s00146-023-01634-z
Ricaurte, P. (2019). Data epistemologies, the coloniality of power, and resistance. *Television & New Media*, *20*(4), 350–365. https://doi.org/10.1177/1527476419831640
Rose, N. (1992). Governing the enterprising self. In P. Hellas & P. Morris (Eds.), *The values of the enterprise culture* (pp. 141–164). Routledge.
Ruckenstein, M. (2014). Visualised and interacted life: Personal analytics and engagements with data doubles. *Societies*, *4*(1), 68–84. https://doi.org/10.3390/soc4010068
Sajed, A. (2024). Epistemologies of domination: Colonial encounters, heterology, and postcolonial pedagogy. *International Studies Review*, *26*(3), 1–19. https://doi.org/10.1093/isr/viae035
Schmidt, L., Finnerty, M. A. N., Elmore, R., Olorisade, B. K., Thomas, J., & Higgins, J. P. T. (2021). Data extraction methods for systematic review (semi)automation: Update of a living systematic review. *F1000Research*, *10*, 401. https://doi.org/10.12688/f1000research.51117.1
Singh, R. (2020). Data colonialism and its discontents. *Communication, Culture and Critique*, *13*(4), 524–532.
Singh, R., & Gurumurthy, A. (2021). Data justice: A decolonial perspective. *Internet Policy Review*, *10*(2).
Skelton, S. K. (2024, April 11). Facial recognition to play key role in UK shoplifting crackdown. *Computer Weekly*.
Taylor, C. (1985). Atomism. In *Philosophical Papers* (pp. 187–210). Cambridge University Press.
Taylor, C. (1989). *Sources of the self. The making of modern identity*. Cambridge University Press.
Taylor, C. (1996). *Conditions of an unforced consensus on human rights*. Unpublished paper.
Thatcher, J., O'Sullivan, D., & Mahmoudi, D. (2016). Data colonialism through accumulation by dispossession: New metaphors for daily data. *Environment and Planning D: Society and Space*, *34*(6), 990–1006. https://doi.org/10.1177/0263775816633195
Tourish, D., & Willmott, H. (2023). Despotic leadership and ideological manipulation at Theranos: Towards a theory of hegemonic totalism in the workplace. *Organization Studies*, *44*(11), 1801–1824. https://doi.org/10.1177/01708406231171801
Tyler, C. (2014, September 18). Facebook refuses about – face on drag queen names. *ABC7 News*.
Tyler, T. R., & Jackson, J. (2014). Popular legitimacy and the exercise of legal authority: Motivating compliance, cooperation, and engagement. *Psychology, Public Policy, and Law*, *20*(1), 78–95. https://doi.org/10.1037/a0034514

Varoufakis, Y. (2024). *Technofeualism: What killed capitalism*. Penguin Books.
Veale, M., & Binns, R. (2017). Fairer machine learning in the real world: Mitigating discrimination without collecting sensitive data. *Big Data & Society*, *4*(2), 205395171774353. https://doi.org/10.1177/2053951717743530
Viljoen, S. (2021). A relational theory of data governance. *The Yale Law Journal*, *131*(2), 370–781.
Waelen, R. A. (2022). *The struggle for recognition in the age of facial recognition technology*. AI Ethics, 3, 215–222. https://doi.org/10.1007/s43681-022-00146-8
Zehner, B. (2019). Machines of subjection: Notes on a tactical approach to artificial intelligence. *Machine Feeling*, *8*(1). https://aprja.net/article/view/115414
Zuboff, S. (2019a). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. Public Affairs.
Zuboff, S. (2019b). Surveillance capitalism is an assault on human autonomy. *The Guardian*. https://www.theguardian.com/books/2019/oct/04/shoshana-zuboff-surveillance-capitalism-assault-human-automomy-digital-privacy