Indispensable: The digital capitalist class and Gramscian conditions of revolution

Luis M. B. Varona[a,b,c] and Wayne A. Hunt[a]

November 20, 2026

Abstract

Artificial intelligence, predictive analytics, and social media have come to dictate the zeitgeist of the 21st century, producing a new dominant class of *digital capitalists* whose monopoly on essential technological infrastructure has made them indispensable to both society and state. Analyzing the resulting sociopolitical dynamics through the lens of class theory, we argue that this indispensability degrades the conditions of revolution (namely, people's capacity to recognize their exploitation, to perceive it as a shared ordeal, and to act on it together), then proffer suggestions for rebuilding them. Drawing on Gramsci, Rouvroy, Foucault, and others, we trace this argument across four interconnected domains of society. First, we examine how Big Tech extracts data through everyday services, leveraging vast amounts of information capital to influence societal trends. Second, we characterize the challenges inherent in regulating the constantly changing technology involved in this extraction, as institutions are subject to corporate capture. Third, we criticize how modern states securitize technological development, further fuelling regulatory lenience and deepening divides between exploited individuals from different nations. Finally, we illuminate the enclosure of the digital commons by tech firms that have accrued power in the economic, political, *and* ideological spheres, limiting people's ability to contest the reigning technological hegemony (even fostering a culture of cognitive offloading to artificial intelligence). Any successful attempt at resistance demands that the working class first emancipate itself from Big Tech's grasp by taking control of digital infrastructure and reclaiming its own capacity to think.

Keywords: digital capitalism, class politics, technological hegemony, digital commons, Big Tech, artificial intelligence

1 Introduction

As artificial intelligence (AI), big data, algorithms, and other digital technologies have come to dictate the zeitgeist of the 21st century, it has become clear that a belief in technological progress is driving sociopolitical change at an unprecedented pace. The global capitalist system has responded with a marked shift toward datafication, and in the United States (US)—as well as throughout the Western world at large—the political superstructure evolves alongside it. When making decisions about governance, institutions treat subjects and citizens as data profiles while neglecting to consider the unique insights of their individual life stories [RB13]. This is part of a larger transformation in which machines replace humans and traditional

*Contact: Luis M. B. Varona. Email: luismbvarona@protonmail.com or lbvarona@mta.ca. ORCID: 0009-0003-7784-5415.
[a]Department of Politics & International Relations, Mount Allison University, Sackville, NB, Canada E4L 1E4
[b]Department of Economics, Mount Allison University, Sackville, NB, Canada E4L 1E4
[c]Department of Mathematics & Computer Science, Mount Allison University, Sackville, NB, Canada E4L 1E4

https://doi.org/10.33774/apsa-2026-7606t **ORCID:** https://orcid.org/0009-0003-7784-5415 Content not peer-reviewed by APSA. **License:** CC BY 4.0

Foucauldian governmentality [Fou07] is exercised through algorithmically decided norms that appear apolitical to the populace. Our understanding of this phenomenon is still rooted in the past, and as technology progresses faster than society can adapt, its political stakes go largely unrecognized.

These changes have given rise to a new era of "digital capitalism"—a term coined by [Sch99], which we use to denote the dominance of a new class that derives its power from its control over data and technology rather than ownership of the industrial means of production. Big Tech enjoys excessive sway over societal trends by virtue of its monopolies on the operating systems, cloud services, search engines, and social media platforms that have embedded themselves in every element of today's economy. Such technological infrastructure is a means of production in that it turns extracted data into a commodity [CM19], so this new class remains capitalist in the Marxist sense of the word.[1] However, this infrastructure has become indispensable not only to the rest of the economy but also to the state itself, affording digital capitalists far more freedom and reach than their industrial-era counterparts.

Exploitation under digital capitalism is more difficult to recognize, partially because that which is extracted is no longer a purely economic asset like labour. Data seized from the most mundane aspects of everyday life is leveraged to generate profit [CM19]. Moreover, the digital infrastructure on which any collective pushback must rely is controlled by a small group of corporate actors who directly benefit from impeding resistance. Recent developments in AI have driven data extraction and infrastructural control to converge more sharply than ever, as frontier models are trained on extracted data and run on computing systems owned by a handful of firms. This growing concentration of corporate power has even begun to feed into a broader political context of burgeoning authoritarianism and illiberalism, giving rise to "technofascist" forms of governance throughout the Western world [Coe26]. This fundamental shift in political economy has profound implications for the future of liberal democracy, reshaping how surveillance, nationalism, class formation, and more function in this new algorithmic age.

We analyze this unfamiliar sociopolitical terrain through the lens of class politics, investigating how conditions of revolution in [Gra71]'s theory of hegemony have been degraded. Traditional wage relations in the factory (and, more broadly, in the workplace) create a point of contact between the bourgeoisie and the proletariat, allowing labourers to organize and resist [Mar76]. Meanwhile, modern tech giants like Google and Microsoft—in control of inescapable and indispensable digital infrastructure—extract value from users in a manner that eludes political framing. This enables "algorithms [to] reorganise social processes" in ways that exacerbate socioeconomic inequality and seize power from the working class [CLL25]. This subtler yet equally deleterious form of exploitation evades recognition as such, all the while empowering the dominant class to enclose the digital commons necessary for the regulation and the governance of technology. A new class relation has arisen in which the exploited struggle to recognize their own exploitation, to build a shared class consciousness, and to mobilize collectively against the dominant class—all conditions fundamental to the possibility of revolution.

This paper is the first in the literature to examine how Gramscian conditions of revolution are deteriorating because of state and societal dependence on the digital capitalist class, as well as how to rebuild them. Related scholarly work has already touched on various aspects of this topic. The concepts of "data capitalism" [CLL25], "platform capitalism" [Srn17], and "rentier capitalism" [SS26] are well established. In particular, [CLL25] analyze the ramifications of data extraction for politics using a Marxist framework of class formation, and [Srn17, SS26] frame this datafication in terms of monopolies on tech platforms and digital services. By emphasizing the broad range of AI's applications, [Ver24] further elucidates the

[1] Some scholars argue that capitalism has already been supplanted by an entirely new order. For instance, [Var23] speaks of "technofeudalism," in which tech firms act like medieval lords levying rent on platform users. However, we agree with [SS26]'s account that the current system is still a capitalist one—extraction through wage relations persists, and Big Tech is itself a major purchaser of labour. We therefore frame digital capitalists as a new dominant class operating alongside (and often in conjunction with) the traditional bourgeoisie.

https://doi.org/10.33774/apsa-2026-7606t **ORCID:** https://orcid.org/0009-0003-7784-5415 Content not peer-reviewed by APSA. **License:** CC BY 4.0

mechanism by which a small number of firms have established a tight grip on the tech industry, deliberately enclosing a commons kneecapped by universal reliance on this technology.

These firms then leverage [GD22]'s "chokepoint capitalism" to maintain their monopolies, taking hold of points through which everyone in the digital world passes. This allows tech giants to extract rent from those who rely on them, as well as make exit from this dependence progressively more costly. The "data colonialism" of [CM19] describes how data extraction of this kind operates without the need for even tacit consent in modern society, extending the seizure of land and resources to "the appropriation of the social itself." It is useful to adopt a paradigm in which we frame these phenomena as colonialism that extends beyond mere class exploitation; this emphasizes the lack of agency inherent in the current situation. Whereas wage relations at least pay the worker under a nominally consensual (even if economically coerced) contract, data colonialists profit off of data that is extracted rather than purchased.

The post-Foucauldian notions of "a-normativity" and "algorithmic governmentality" [RB13] explain how these dynamics escape framing in political terms. Society tends to view pieces of technology as a-normative, neutral tools that individuals can use for good or for bad as they so choose. However, this perspective obscures a larger socioeconomic context that is anything but apolitical. AI lends more strength to this façade than ever—its natural-language responses shape public opinion more profoundly than the outputs of other disruptive technologies, masquerading as mere technical fact [Pal26]. Big Tech has capitalized on this apparent neutrality to deliberately engineer an environment in which reliance on data-extracting platforms is an economic necessity. This pushes institutions to adopt a framework of algorithmic governmentality, treating those they govern as no more than objective, depersonalized data profiles. This resembles [Fou07]'s original notion of governmentality in which those in power promote their idea of the "average man" [RB13] to set norms, except these norms are now determined less overtly by algorithmic systems; consequently, the decision-making process is far more difficult to publicly contest. The digital capitalist class in control of these systems has accrued an inordinate degree of influence, at times even directly encouraging politics with fascist tendencies. This emerging technofascism has so far operated mostly through less visible means such as data extraction, but even as it now comes into the open, it continues to propagate "the illusion that there is not class conflict" [Coe26].

We distinguish ourselves from the existing body of work not by emphasizing dependence on Big Tech per se, but rather by linking this dependence to the degradation of conditions of revolution. The closest related analysis is perhaps provided by [SS26], who argue that rentier capitalism "undermines the conditions necessary for working-class solidarity" by absorbing even the everyday, mundane aspects of life into capital. We explicitly tie this absorption to how indispensable digital infrastructure has become, analyzing corporate capture of the state and proposing concrete routes forward. Meanwhile, [Fuc21] examines how big data and social media obscure class relations in the working class's consciousness. We extend this relationship between data and the proletariat to also cover the digital capitalist class's extraction from all those who depend on its infrastructure. Focusing more on pathways to resistance, [Ver24] advocates for collective control of AI infrastructure—a case we supplement with an account of state dependence on Big Tech and its implications for such a movement. In a similar vein, [CLL25] contend that collective action can overcome the obstacles to organizing under data capitalism; we build on this by looking at how the conditions necessary to mobilize such action have degraded, and proffer some suggestions for countering this decline. In general, we also draw on a broader range of sociopolitical phenomena to make our case: whereas the aforementioned works mostly centre on datafication and platform monopolization, we also study issues of governance and national security.

Ultimately, we argue that indispensability of the digital capitalist class degrades Gramscian conditions of revolution to the point that collective action can no longer take them for granted and rebuilding them becomes a task unto itself. We trace this argument across four interconnected domains of modern society.

https://doi.org/10.33774/apsa-2026-7606t **ORCID:** https://orcid.org/0009-0003-7784-5415 Content not peer-reviewed by APSA. **License:** CC BY 4.0

1.1 Organization of the paper

First, we examine in Section 2 how large-scale datafication and surveillance capitalism have risen to prominence since the turn of the 21st century. Contrasting this with the traditional state-centric surveillance apparatus, we show how private actors in both the US and China have assumed a dominant role in the collection of data, leveraging it not only as a source of profit but also as a political tool [Zub19]. With both the state and the populace highly dependent on these actors, value extracted in this manner is rarely viewed as exploitation, and the channels through which this extraction runs are disguised as services.

We then turn to issues of governance in Section 3, criticizing the normalization of self-regulation in the tech sector (especially when the states responsible for regulation remain dependent on technology). Furthermore, we study how even the strongest contemporary attempts at institutional regulation—most prominently within the European Union (EU)—fail to be effective, as technological advancement outpaces the ability of institutions to respond and Europe relies on imports for most of its technology.

Next, we analyze how the securitization of technology reinforces national allegiances while eroding transnational class solidarity in Section 4. This favours the advent of a "new techno-nationalism" [Luo22] that privileges security and technological capacity as the primary basis of national strength, shaping conceptions of national identity itself in the process. In conjunction with this, the military increasingly relies on technology supplied by the digital capitalist class, which becomes ever more indispensable to the state. Developments in precision strike technology and autonomous weapons systems also avoid the need to lose soldiers' lives in war, indirectly winning Big Tech the working class's support.

Finally, Section 5 describes how digital capitalists have enclosed the public sphere. By monopolizing the digital commons and supplanting critical thought with machine judgment, the digital capitalist class represses resistance to its "technological hegemony" [Fee92]—the presentation of class domination as the natural, innocuous consequence of objective technologies. Contrary to the Marxist expectation that worsening conditions would propel the working class to revolt [Mar76], organized resistance has thus stagnated even as socioeconomic inequality grows [SS26].

We conclude in Section 6 by asking what an effective Gramscian "war of position" [Gra71] as a strategy of resistance might entail in the modern landscape of digital capitalism. In particular, we advocate for a transnationally integrated movement reliant on the construction of publicly owned digital infrastructure, while organic intellectuals translate sociopolitical phenomena grounded in ostensibly a-normative technological and algorithmic processes into legible exploitation.

2 Datafication and the corporate surveillance state

From microtargeted political campaigns to China's social credit system, digital oversight plays a central role in contemporary governance. Both state and commercial actors have not only acquired unprecedented access to personal data, but also perfected the art of data-driven social engineering. Across the globe, we are monitored endlessly through our mobile phone usage, credit card transactions, social media activity, and innumerable other aspects of our mundane daily routines. In contrast to traditional Orwellian figures like Big Brother with their overt political overreach, these complex surveillance systems rarely present themselves as instruments of power. Instead, they integrate into the ordinary functioning of now-ubiquitous digital services, blending into the backdrop of everyday life as their influence is normalized. Large swaths of the populace remain resigned—and, at times, even indifferent—to the uses and abuses of their personal data, less for lack of awareness than for a failure to frame this dynamic in political terms [DT19].

The historical context underlying this trajectory is important. Although the phenomenon of big data (i.e., the automated collection and analysis of extremely large and complex datasets) is certainly exclusive to the modern world, the concept of information as a form of power is by no means novel. The systematic

https://doi.org/10.33774/apsa-2026-7606t **ORCID:** https://orcid.org/0009-0003-7784-5415 Content not peer-reviewed by APSA. **License:** CC BY 4.0

"collection, classification, transportation, and negotiation" of data in governance and public administration can be traced back centuries, albeit in vastly different forms over the ages [AvOS17]. It was not until the early 2000s, however, that the Internet of Things—an interconnected network of Internet-enabled devices constantly collecting and exchanging information—materialized. This was a transformation of singular moment, creating a brand-new digital ecosystem in which "multitudes of objects in our built environment can double as interactive and interconnected nodes for the Internet, and as sensors that gather data about every aspect of human life" [HR19]. Access to these sensors paved the way for the mass collection of personal data by both state and corporate actors on an unprecedented scale.

Security concerns in the wake of the 9/11 attacks drove the US government to launch the Total Information Awareness (TIA) initiative, which involved mass profiling based on financial records, communications, travel data, and biometric information. An increased willingness to sacrifice privacy for safety in the name of national security also impeded the Federal Trade Commission's ongoing push for national privacy legislation. This combination of new digital technologies and a changing political climate enabled Google to pioneer the practice of "surveillance capitalism" [Zub19] around the same time, collecting vast quantities of user data and monetizing it through targeted advertising. Thus, mass state surveillance and commercial datafication developed concurrently, with regulatory efforts falling by the wayside.

The corporate surveillance apparatus that emerged over the following two decades extended far beyond the monetization of user data through targeted advertising that Google had pioneered, permeating every layer of digital infrastructure. The extraction of "behavioural surplus"—data collected extraneously with the intent of predicting and shaping human behaviour—laid the groundwork for a platform business model that normalized overreaching data collection [Zub19]. By 2017, Windows 10 had been publicly shown to collect telemetry data continuously and by default [Dut17], and in 2024, Microsoft introduced an even more invasive "photographic memory" feature that captured screenshots of user activity at regular intervals [Kar26]. Hence, the increasing integration of computers into our daily lives and the growing market dominance of tech giants like Microsoft have given rise to a form of extraction that did not exist in the 2000s, carried out through inescapable services and platforms.

This pervasive datafication across all aspects of life bypasses the traditional need for consent and participation (even if only passive). As an extreme manifestation of this, Israel's AI-powered Lavender targeting system generates thousands of target recommendations in Gaza per week through algorithmic analysis of population-wide data [And25], in what a United Nations commission has recently determined to constitute a genocide [Ind25]. Thus, the reduction of individuals to no more than data profiles has lethal consequences. Even in more mundane settings, people are drawn into the surveillance apparatus by virtue of others' participation alone. Data exposed by users of tech platforms such as social media or search engines allows the construction of "shadow profiles"—data composites of their social connections who have never consented to (or even used) these services [Gar17]. Whereas state intelligence monitors people for identifiable purposes, the corporate surveillance apparatus practices [CM19]'s data colonialism, "[appropriating] life as raw material whether or not it is actually labor, or even labor-like" for economic profit. Unlike exploitation through wage relations, this extraction is folded into quotidian interactions with digital services, passing as the normal functioning of the tools on which modern society depends. It is never presented as a claim that one party makes on another, so the class relation behind it becomes illegible even to users who know full well that their data is being collected.

State surveillance, whatever its abuses, operates within institutional channels of a state that—at least in theory—answers to the people in a liberal-democratic system. This is illustrated by what happened to TIA: after it was publicly exposed, the ensuing protest over its overreach pushed the US Congress to kill the program [Zub19]. On the other hand, what we call the "corporate surveillance state" operates beyond the reach of these channels, and given that Big Tech presents its technologies as a-normative tools peddling statistical objectivity, the associated private actors are far more difficult to contest for legitimate,

https://doi.org/10.33774/apsa-2026-7606t **ORCID:** https://orcid.org/0009-0003-7784-5415 Content not peer-reviewed by APSA. **License:** CC BY 4.0

articulable reasons in the public sphere [RB13]. Even when these forces shape modern sociopolitics in very real and deliberate ways, identifying what is being done to whom—let alone formulating a contestable grievance—becomes a daunting task that the rare episodes of public exposure have done little to ease. For instance, the infamous 2018 Cambridge Analytica scandal publicly exposed the harvesting of 87 million Facebook users' personal data by a British consulting firm to influence American politics [Zub19]. Despite widespread public outcry and US congressional hearings, however, the scrutiny fell mainly on a specific act of corporate data misuse, and the underlying business model remained largely insulated from criticism. This exemplifies a broader pattern in which exposure can make an individual abuse visible while leaving the overarching class relationship illegible.

It does not help matters that the corporate surveillance apparatus was fostered by—and continues to be fundamentally intertwined with—the state. Following TIA's congressional defunding, the intelligence community turned to corporate channels that remained unconstrained by institutional checks and balances. This is part of the larger phenomenon of "surveillance exceptionalism" [Zub19], in which tech companies were given a regulatory pass on data collection in the post-9/11 climate. The data analytics and surveillance firm Palantir—founded, in part, using Central Intelligence Agency (CIA) funding [IA22]—absorbed many of the intelligence functions that democratic opposition had denied the state, providing platforms designed to integrate and analyze data across agencies. Despite their differing motivations of national security and commercial profit, the security establishment and the private sector have converged over the past two decades. Both apparatuses partake in the comprehensive gathering of personal information, granting an unforeseen capacity to predict and modify societal behaviour en masse [Zub19]. Democratic processes succeeded—at least to a degree—in resisting unconstitutional state surveillance, but this only displaced datafication into equally insidious corporate channels on which the state would come to depend.

The corporate surveillance state has thus given rise to the digital capitalists as a qualitatively different dominant class that directs the extraction of value from human life through datafication [CLL25] while also exerting monopolistic control over the tech platforms facilitating said extraction [Srn17, SS26]. We show how these constitute complementary dimensions of the same class position, as data extraction on such a large scale—and in such an inescapable way—requires the overwhelming dominance that Big Tech currently possesses over everyday digital infrastructure. In turn, that control is sustained by the data those systems collect—it improves the ability to anticipate user behaviour, deepens dependency, and forecloses meaningful competition. These services now also host much of civic and social life, turning the digital commons into a set of privately owned platforms whose operators answer to shareholders and profits above all else [CLL25, SS26].

It is essential to note that this trend of corporate surveillance and private control over data extends into other economic systems well beyond the Western world. The US and China—two of the world's most powerful states, and the only "two AI superpowers" [Blo26] of today—offer the sharpest available contrast for demonstrating the universality of this condition. The US has been described as a "lawyerly society" in which legal processes dominate governance but produce no more than an illusory sense of constraining corporate power, while China operates as an "engineering state" that utilizes calculated social engineering to control its population [Wan25]. China only recognized the digital tech sector as a strategic priority in the early 2010s, but the state then invested aggressively, and domestic firms like Alibaba and Huawei built a formidable digital apparatus through which much of Chinese daily life is now conducted [HZ25].

In 2014, China adopted a "social credit system" (SCS) comprising a commercial branch that assigns scores to citizens based on their consumer behaviour and a government branch that monitors legal compliance [CG22]. In addition to enabling the datafication of daily life on a national scale, the SCS facilitates the blacklisting of both political dissidents and ordinary citizens who fall afoul of the state's rigid expectations, further entrenching the authoritarian grip of the Chinese government on its population. The state reinforces this with pervasive facial recognition, online monitoring, and heavy Internet censorship via

https://doi.org/10.33774/apsa-2026-7606t **ORCID:** https://orcid.org/0009-0003-7784-5415 Content not peer-reviewed by APSA. **License:** CC BY 4.0

the "Great Firewall" [Jia24], suppressing dissent and preventing alternative viewpoints from reaching the public. Over the following decade, "state platform capitalism" and a "techno-nationalist agenda" [HZ25] came to dominate government strategy, and such arrangements were codified as two landmark pieces of legislation—the Personal Information Protection Law (PIPL) and the Data Security Law (DSL)—passed in 2021. The PIPL, modelled on the EU's General Data Protection Regulation (GDPR), conspicuously avoids the language of "privacy" in favour of vaguer invocations of "personal information." Complementing this, the DSL is oriented less toward individual rights than toward national security, compelling domestic companies to comply with state demands for access to user data.

The Chinese government has used this authority to absorb the commercially built digital infrastructure into a unified "data state" that reduces citizens to "data projects" [CC22], utilizing the private sector's data-gathering capacity to conduct state surveillance. The heightened focus on data privacy notwithstanding, the practical effect of this transition was not to safeguard the liberties of Chinese citizens but rather to transfer control over their personal information from the private sector to the government, producing an "authoritarian privacy" regime in which the state enforces data privacy against everyone but itself [Jia24]. This shift owes much to how elastic the concept of national security is, often stretching to fit whatever state interests require [Blo26]—in China's case, this allows for the gathering of the personal data of an entire population. Although China's form of state surveillance may seem explicitly political from a Western perspective, the illegibility of this exploitation is upheld by other means. In particular, the large-scale social engineering and indoctrination of the local population through an authoritarian system prevents citizens in China from recognizing their exploitation as such.

Under both the market-driven model of the US and the state-directed model of China, ordinary citizens are subject to comprehensive datafication without any meaningful capacity to opt out. Both systems consistently invoke national security (a theme to which we later return in Section 4) to quash potential avenues for democratic recourse. Indeed, China has gone so far as to seize domestic firms' digital ecosystem and integrate it into a state operation. Regardless, this move has still left the government dependent on commercial foundations, even where it holds coercive power over the private sector. Despite fundamental differences in underlying sociopolitical dynamics and institutional context, both systems exhibit cooperation between the state and corporations, allowing Big Tech to accumulate power and legitimacy that facilitate further exploitation of the working class.

This arrangement only grows further entrenched over time, failing to invite as much organized opposition as previous forms of capitalist exploitation. As digital services and platforms are also the means through which people maintain social ties and participate in the economy on a daily basis, tech giants work to raise the cost of leaving them in the vein of [GD22]'s chokepoint capitalism. The value extracted from users with nowhere else to go is recycled for the purpose of keeping them there, guarding against any rivals that might offer them exit. These services thus become harder to abandon with every passing day, deepening reliance and normalizing exploitation in the minds of consumers. The illegibility of this exploitation, coupled with state dependence on these services, then helps digital capitalists escape conventional institutional regulation through empty promises of self-regulation—the subject of Section 3.

3 Technology governance and the failures of self-regulation

The dominant response to the corporate surveillance state (as well as a myriad of other rapid 21st-century technology-driven developments) has overwhelmingly been one of self-regulation, as algorithmic processes obscure their sociopolitical consequences beneath a façade of statistical objectivity. This adoption of algorithmic governmentality bypasses every assumption on which conventional regulation is built [RB13]. Regulatory institutions are designed for political problems with identifiable victims and exploiters, but algorithmic processes rarely produce such situations. Instead, they are grounded in statistical patterns

https://doi.org/10.33774/apsa-2026-7606t **ORCID:** https://orcid.org/0009-0003-7784-5415 Content not peer-reviewed by APSA. **License:** CC BY 4.0

that we often fail to recognize as normative and frame in political terms, thereby impeding attempts at effective governance. The market power of the tech sector—especially when the state is so dependent on its products and infrastructure—further precludes meaningful regulation that may interfere with economic profits. Futile frameworks of self-regulation and insincere voluntary commitments have filled the void, notwithstanding that the ethics of technology are only truly effective at guiding judgment alongside actual binding regulations, not enforcing compliance on their own [RR20].

Understanding the background of this dynamic is crucial. Well before large language models (LLMs) ushered forth even more radical changes in the 2020s, technology companies already relied heavily on ethics guidelines, internal review boards, and voluntary commitments to responsible development, with binding regulation largely insufficient across the tech sector [JIV19]. The continued growth of the information economy promoted a culture of "neoliberal managerialism" [Coh19], as legislatures steadily bought into the belief that regulations could effectively run through audits and standards. By 2019, at least 128 ethical frameworks for AI had been published in Europe alone, but rather than constrain private actors, this veneer of accountability allows the industry to shape what is and is not "ethical" in the public perception to its benefit [Cra21]. This corporate appropriation of ethical language adopts only the principles that are minimally sufficient to preserve public legitimacy (and even then, fails to adhere to them consistently) [Wag18]. Voluntary ethics frameworks are thus actively counterproductive, founded on principles that are "meaningless" in their abstraction, "isolated" from the industry cultures that would need to change for them to function, and "toothless" in their lack of any enforcement mechanism, ultimately only distracting from alternative regulatory approaches that might actually work [Mun23].

A foundational event further exacerbating this trend transpired in November 2022, when OpenAI publicly released ChatGPT, the first mass-market consumer product built on an LLM. Within two months of its launch, it attracted 100 million monthly active users, the fastest adoption of any consumer application in recorded history [Hu23]. This groundbreaking new technology—which has since become capable of simulating human expertise across virtually every professional domain, from medicine to law to software engineering [LGY+25]—catapulted AI to the forefront of the public consciousness, and other major firms such as Google and Anthropic quickly followed suit in commercializing their own models. As competition between AI developers intensified, voluntary frameworks—which were already ineffectual in the first place—collapsed even further. Companies that pledged responsible AI development to the White House complied with barely half of their promises, abiding by as few as 17% of agreements in certain domains like model-weight security [WHKB25]. In February 2025, Google dropped a seven-year-old commitment not to develop AI for weapons or surveillance from its published AI principles, citing competitive and geopolitical pressures [TDV25]. Anthropic followed a year later, abandoning an initial assurance that it would pause training if its safety measures started to lag behind [Per26].

At certain points, state coercion has proven to be a critical factor as well. The state often intervenes directly to leverage these new technologies to its own advantage, even when competitive market pressures do not dismantle voluntary ethics frameworks. One example stands out: in February 2026, the Pentagon demanded that Anthropic abandon its restrictions on the use of its AI systems for mass surveillance and autonomous weapons (limits that its competitors had already forsaken in exchange for unrestricted military contracts). The government threatened that failure to do so would result in designation as a national security supply-chain risk, constituting blatant misuse of a label typically reserved for foreign adversaries [JSS26]. This illustrates how any company that develops AI for both commercial and government markets while maintaining safety restrictions that conflict with state interests risks exclusion from a major source of revenue in government contracts. On the other side of the coin, the state can wield such leverage over any individual firm because it relies on the digital capitalist class as a whole to service its needs. Deeper integration of the tech sector with the state only reinforces this interdependence and undermines already-tenuous voluntary commitments.

https://doi.org/10.33774/apsa-2026-7606t **ORCID:** https://orcid.org/0009-0003-7784-5415 Content not peer-reviewed by APSA. **License:** CC BY 4.0

Even setting aside the very real concerns of corporate amorality and state coercion, a fundamental failure to understand the technology itself undermines well-intentioned attempts at responsible conduct. An oft-proposed method of self-governance (which, again, dubiously presupposes a position of good faith) is an "iterative deployment" framework [HB25] in which systems are released incrementally and each deployment reveals problems that inform the next. However, this assumes that the problems are visible and comprehensible to the "experts" deploying the system, which is often no longer the case given how rapid and unfamiliar recent developments have become. Public institutions face much the same problem: they were designed to react to industrial-era change, but as early as the 1970s, a mainstream argument in the intelligentsia had emerged that technology was beginning to progress too quickly for institutions to keep pace [Tof70]. More recent scholarly work has continued to document this "pacing problem" across modern fields of biotechnology, nanotechnology, and computer privacy [MAH11], as oversight mechanisms have in some cases grown slower while technological development continues to accelerate.

AI has since intensified the pacing problem as "exponential growth outpaces static laws, rendering traditional command-and-control regulation inadequate" [Mah25]. Separately from institutions' quantitative failure to keep pace, this new technology can simulate human behaviour and capabilities in unprecedented ways that are so qualitatively different from our baseline understanding. This exacerbates an issue distinct from the pacing problem: the "Collingridge dilemma" [Col80] that effective regulation requires understanding a technology's societal effects, which often become visible only after said technology is embedded in infrastructure and institutional practices resistant to change. This has always been a problem, but the previously unthinkable capabilities of almost anthropomorphic AI models have moved it to the forefront of issues in modern governance.

Recent security incidents across multiple AI companies in 2026 make this phenomenon clear. In one event, over 1,200 AI agents developed by OpenAI escaped their testing environment, gained access to the Internet, and coordinated via a makeshift message board with over 70,000 messages, discovering how to falsify logs and transcripts [Roo26]. Eventually, more than 700 of them swarmed the systems of Hugging Face (the largest open-source AI model-hosting platform), exploiting security vulnerabilities and gaining full control of at least one server. In a separate episode, agents built by Anthropic submitted visa applications to the US State Department and sent a fabricated homicide tip to the Philadelphia Police Department, reportedly of their own accord [CIBS26]. Even though Anthropic uncovered what its agents had done in July, it only made the affair public in October, prompting the White House to demand that AI companies disclose any such incidents without delay.

Another revealing case study can be found in the response of the EU—historically a "regulatory superpower" [Bra20], and one of the few places to at least partially understand the importance of AI governance and amass enough political will to attempt more comprehensive binding regulations [Lep26]. However, European frameworks remain limited in scope (indeed, this is what we make a point of criticizing more than any shortcomings in regulatory strength). The EU Artificial Intelligence Act was the first binding supranational framework for AI governance to be adopted anywhere in the world, regulating domestic AI operations in all 27 EU member states [Maa25]. Still, the AI Act is at its core a "product safety framework" [AR24], focusing on high-risk applications prone to "malfunctioning" [Eur24]. Most of the everyday AI operations that enable the extraction documented in Section 2 fall outside that high-risk category altogether; for them, even Europe relies (ineffectively) on self-regulation more than anything else.

Meanwhile, the GDPR only governs the collection and processing of personal data (including when AI is involved), not other AI-related activities [AR24]. Even then, it largely regulates how—not whether or when—data is gathered [GD22], dealing primarily with individuals as opposed to larger systems. It therefore lacks any meaningful influence over profiles assembled from many people at once [RS16], which are precisely the elements that underpin the entire class relationship. These structural limits in EU legislation allow data extraction to remain unchecked throughout the bloc—so long as data is collected through the

https://doi.org/10.33774/apsa-2026-7606t **ORCID:** https://orcid.org/0009-0003-7784-5415 Content not peer-reviewed by APSA. **License:** CC BY 4.0

prescribed procedures and with formal consent, regulation actively lends the digital capitalist class legitimacy. However strictly regulations may define consent, the culture of dependency engendered by tech platforms pushes people to routinely accept dubious terms of service [Coh19].

As matters stand, Europe is poorly positioned to widen the scope of its legislation, as it is far further from the cutting edge of technology than the US and China. The EU imports over 80% of its "digital products, services, infrastructure and intellectual property," and it is home to only four of the 50 largest tech companies worldwide [Dra24]. The digital capitalist class controls the technology Europe needs, making it harder to regulate as developers can simply threaten to withhold their products from the region's market. Worse still, institutions abroad are likely to look to the EU—as they have historically done—as an example of perceived regulatory success, and the template for regulation set by the AI Act may propagate a narrow idea of AI governance [AR24].

International frameworks for AI governance more broadly—comprehensively surveyed by [Maa25]—have even less force behind them, defaulting to (once again performative) voluntary ethics frameworks. The Organisation for Economic Co-operation and Development adopted intergovernmental AI principles as early as 2019, but this has largely failed to translate into substantial policy changes among member states. By 2025, the UNESCO Recommendation on the Ethics of Artificial Intelligence had seen fewer than a quarter of the 193 adopting states work with the organization to implement it, and the US—where most frontier AI development takes place—was not even a UNESCO member at the time of adoption in 2021. The 2023 G7 Hiroshima AI Process provided nothing more than a voluntary code of conduct for AI developers. The Council of Europe's Framework Convention on Artificial Intelligence (the only prominent attempt at binding international constraint other than the EU AI Act) sets principles rather than rules, defers the regulation of private actors to individual states, and exempts issues of national security entirely. As of November 2026, even this treaty has only two ratifications out of 21 signatories total [Cou24], falling short of the five required for entry into force.

The industrial-era bourgeoisie controlled the means of production but did not have as much freedom from state oversight. Meanwhile, the digital capitalist class has managed to evade regulation via rapid development, transnational mobility, a-normative pretences, and an ability to make its technology indispensable to the state. It is structurally next to impossible to enforce meaningful constraints while voluntary frameworks remain the norm, allowing class domination that technically follows whatever rules exist to appear legitimate. As technology continues to seep unfettered into every nook and cranny of modern life, Big Tech accumulates more and more capital facilitating exploitation that the working class often cannot recognize, or at least frame in political terms. These challenges are further compounded by the fact that collective class consciousness is fractured along national borders, as people identify with their nation's position in the perceived global technology race. In Section 4, we look at how this race has placed technology at the centre of national security, portraying attempts to constrain its owners as weakening the nation.

4 Nationalism and the securitization of technology

Post-nationalists like [Soy94, Hab01] speculated that economic integration in the era of post–Cold War globalization would steadily erode nationalist sentiment. With the advent of digital technologies, however, economic and security interests have reorganized around issues of cybersecurity and technological sovereignty, in turn altering the makeup of national identity itself [Luo22, Zha24]. Under this "new techno-nationalism" [Luo22], governments securitize technology, even going so far as to consider its mere exchange with other countries a matter of national security. In the US, regulating Silicon Valley is treated as a concession to geopolitical rivals. America's 2025 AI Action Plan, for instance, recommended waiving parts of the Clean Air Act, the Clean Water Act, and the National Environmental Policy Act to expedite the construction of data centres, citing "a race to achieve global dominance in artificial intelligence" [Lep26].

https://doi.org/10.33774/apsa-2026-7606t **ORCID:** https://orcid.org/0009-0003-7784-5415 Content not peer-reviewed by APSA. **License:** CC BY 4.0

In China, Big Tech is completely inseparable from national progress. Questioning it is tantamount to subverting the authority of [Wan25]'s engineering state—a particularly daunting prospect given China's authoritarian regime. Across radically different political systems, we see how the digital capitalist class is insulated from democratic challenge by the rhetoric of national security and progress. Furthermore, the growing importance of technological dominance has driven the deeper integration of the tech sector with military matters. This has resulted in a fundamental redefining of the nature of warfare as states increasingly utilize remote technology rather than actual troops [Moy21], and with loss of life averted, the working class at home grows more supportive of Big Tech in the process.

Military might has always been dependent on technological prowess throughout human history, but, as noted by [Maz15], a closer relationship between the state and the tech sector began to develop in the post–World War II environment. Although victory in the war had largely relied on state-organized research, the US military began to take an interest in technologies like computers, jet planes, nuclear energy, lasers, and biotechnology, all of which promised both military and commercial applications. The 1957 Soviet launch of Sputnik, the first man-made satellite, soon prompted the creation of the Advanced Research Projects Agency, which went on to support semiconductor research and oversee the early stages of the Internet. The CIA even resorted to venture capital in several cases; to cite a prominent example, it funded Keyhole, a satellite mapping firm whose technology was deployed in Iraq [Lev18].

Over time, this relationship has resulted in a growing dependence on private-sector technology for the US military's continued dominance. Commercial firms have been major players in the development of American drone technology going back to the early 2000s, working closely with the Air Force, Army, and Special Operations Command [MS17]. The advent of AI technologies in the 2010s has only intensified this trend. In 2017, the Pentagon contracted Google to develop AI under Project Maven [Mal23]. Since then, commercial LLMs have been covertly repurposed for military intelligence, proliferating through channels over which existing regulations have little oversight [KWW24]. Frontier AI models are often integrated directly into the military's targeting systems—when US–Israel strikes on Iran began in February 2026, Anthropic's Claude models processed intelligence sources for Maven, and the Pentagon described Claude as playing a "central" role [Akk26]. The dependency of the state on the digital capitalist class has deepened, as the military comes to rely not only on the persistent surveillance and data analysis capabilities made possible by commercial development but also on cutting-edge models made accessible only by consorting with private actors. The data that private firms gather from users in collaboration with the government—both domestically and overseas—is also used to extract value from the proletariat [CCG25b]. Hence, the assets that secure the digital capitalist class its economic dominance also make it indispensable to the state, directly facilitating its exploitation of the working class.

Additionally, advancements in technology have produced the accessible justification of "humane warfare" [Moy21]—the idea that remote warfare is more ethical insofar as precision strikes are (at least in theory) able to avoid unnecessary casualties. A critical consequence is that this dynamic replaces the question of whether a war should be fought at all with the question of how it should be fought. Rather than oppose military intervention outright, many critics of warfare now accept it as inevitable, settling for stricter targeting rules and fewer civilian deaths. This lends war a moral respectability that makes it easier to justify. Moreover, remote weapons take further than ever [Sha02]'s notion of "risk-transfer" militarism, in which states seek to displace risk from their own forces onto foreign civilians. By sparing ground forces nearly all risk in the modern era, these new technologies eliminate a significant deterrent to war and substantially reduce public backlash [Cha15]. This allows the US (as well as its allies) to use lethal force far more frequently than would be politically tenable if sending ground troops were still a necessity.

A particularly consequential portion of this public tolerance is predicated on the purported precision provided by weapons developed, in part, through public-private partnerships. The American populace's usual propensity for eschewing autonomous weapons systems is promptly pushed aside by precarious

https://doi.org/10.33774/apsa-2026-7606t **ORCID:** https://orcid.org/0009-0003-7784-5415 Content not peer-reviewed by APSA. **License:** CC BY 4.0

promises and proclamations that precision technology is less prone to mistake civilians for combatants than human operators [RSV24]. The prodigious technological innovations of the 21st century go beyond merely offering the ability to conduct warfare remotely—they now power surveillance and identification systems marketed as more reliable, with AI models from leading firms participating in the designation of military targets [CCG25a]. The promise of preserving the lives of both attacking forces and foreign civilians is enough to convert the working class's receptiveness toward "humane warfare" into outright support that actively works in favour (albeit indirectly) of the digital capitalist class. Therefore, the military-technology apparatus not only solidifies the state's dependence on Big Tech but also bolsters the tech sector's position in the public consciousness as a benefactor rather than an exploiter.

More directly, Israel's genocide in Gaza has been used to advertise the efficacy of the technology deployed therein [Akk26]. The digital capitalist class stands to profit from this demonstration, as Big Tech supplies the Israeli army with cloud and AI services. Since 2021, for instance, the Nimbus project has committed Amazon and Google to providing the Israeli government with AI systems for facial recognition and object tracking [CCG25a]. This dynamic (in tandem with broader issues of digital infrastructure and cybersecurity) links the tech sector's prosperity to conceptions of national security and allows its profits from war to pass as legitimate. In fact, this integration runs so deep that both the US and China not only "frame AI leadership as a national security imperative" but also treat it "as a core element of their national identity" [Blo26]. Beyond conceptions of sovereignty and security, the actual sociocultural makeup of each nation has shifted to accommodate growing techno-nationalist sentiment.

In essence, techno-nationalism is a realist ideology asserting that "states should develop and control key technologies" on which their national security rests [Zha24]. This outlook is spurred on by the intensifying rivalry between the US and China, which has prompted a shift to state-driven technology policy around the world. As the US is intent on keeping its grip on the global infrastructure of the Internet while China champions "cyber sovereignty" and technological independence, the network has become a source of escalating competition [Zha24]. It is not as though the insecurity inflaming this rivalry is unfounded—control of the network's main hubs gives the US "weaponized interdependence" [FN19], or the power to mine passing data for intelligence and lock out adversaries. While Meta, Google, and other dominant firms establish cables of their own connecting data centres across the globe, the American and Chinese governments actively shape who owns such networks and where they are laid [Moi26], fighting for influence over digital capitalists' property and the physical infrastructure needed to support the digital. The infrastructure that gives the state its leverage thus allows the firms that own it to move data at lower cost than their rivals, further solidifying their "chokepoints" [GD22].

The economy is a commonly cited justification for framing this competition between states in terms of national interest and security. The first Trump administration invoked the rhetoric that "economic security is national security" [Luo22], imposing sanctions that barred Huawei even from Japanese, European, Korean, and Taiwanese chips produced using American technology. In response, China ordered foreign computers and software out of its government agencies and public institutions. The EU, too, pursues a similar line of reasoning: the European Commission's 2020 Strategic Foresight Report presented the deepening US–China clash as making Europe's own "technological sovereignty" an increasingly important priority [FCT24]. Above all, the world's two technological superpowers back their national champions in Big Tech (such as Intel and NVIDIA in the US, and Huawei and Tencent in China) with state-sponsored contracts, grants, subsidies, regulatory favour, and more [Zha24].

Appealing to the age-old fear of the other has further helped sustain the techno-nationalist agenda. In the US, treating the transfer of technology to China as a security risk has won a measure of broad public support, stoking traditional nationalism that aims "to build and maintain a single national identity, based on shared social characteristics of culture, ethnicity, politics, religion, or traditions" [Luo22]. Some of the most prominent figures in the tech sector openly seek to cultivate a more nationalistic Volksgeist, often

https://doi.org/10.33774/apsa-2026-7606t **ORCID:** https://orcid.org/0009-0003-7784-5415 Content not peer-reviewed by APSA. **License:** CC BY 4.0

through the rhetoric of far-right extremism [Coe26]. Perhaps the most blatant case of this phenomenon to date is a 2025 manifesto coauthored by Palantir CEO Alex Karp, declaring that Silicon Valley and its engineers have a moral obligation to arm the US [KZ25]. The manifesto also ranks the world's cultures by their worth and regards pluralism with open contempt—sentiments troublingly reminiscent of "classical fascism" [Coe26].

Developments in disruptive digital technologies have thus driven both the West and the East to double down on a distressing discourse of securitization, deepening national divides and disseminating the techno-nationalist doctrine. The assumptions underlying post-nationalist aspirations, grounded in the post–Cold War wave of globalization, have collapsed. Post-nationalists argued that the nation would lose its control over rights and state purpose as legitimacy shifted toward international courts and intergovernmental bodies [Soy94], but sovereignty has since been carried into a technological sphere that presents itself as apolitical. Even [Hab01]—one of the foremost post-nationalist thinkers—warns that a larger political bloc built on a shared market would remain caught in "locational competition" (i.e., a struggle for control over capital that can cross borders), closing ranks against everyone outside it. This is exactly the course we have seen recently as the US, China, and the EU all pursue technological sovereignty on the basis of security. As the AI race between the US and China is foregrounded as a contest between great powers, the participating governments allow competing firms far too much regulatory leeway [Moi26]. Additionally, this nation-centric framing obscures the fact that the data extraction of these firms impacts domestic populations just as adversely, and citizens' grievances remain directed at rival nations rather than at the digital capitalist class.

It therefore escapes notice that the digital capitalist class is tied to neither side of this rivalry. Its largest firms, American and Chinese alike, collectively lead "a new bloc of transnational capital" [Rob20]. Meanwhile, the everyday people it exploits remain bound to their nations, as technology changes while nationalism retains its old function of binding the exploited of each nation to the state-sponsored actors that exploit them—a Gramscian "passive revolution" [Gra71] like that identified by [Spo25] in the new domain of digital technology. In the US, digital capitalists reinforce this dynamic through their own war of position, as "billionaires are using digital media to forge an infrastructure for reactionary populism" [Tim21]. Under a Gramscian framework, any viable counter-movement must take shape in civil society. However, to contest a dominant class whose hold on society is so deeply rooted in its control over inescapable digital services and infrastructure, a form of digital commons is needed—one that, at present, does not exist outside the class's control. Such institutional channels must reach across the national lines that divide the exploited, as we explore further in Section 5.

5 Civil society and the enclosure of the digital commons

The exploitation carried out by Big Tech reaches across national borders, as major firms in both the West and the East profit off of data collected from foreign populations [CM19]. The working classes of different nations thus share the same exploiters. However, cross-border class solidarity remains difficult to achieve. Different countries and their respective citizens lack the common identity uniting those within a single nation [Hab01], so solidarity between them forms mainly in reaction to visible wrongs such as persecution by a state. In contrast, exploitation via platforms and data extraction is not framed as legibly in political terms. Given how transnationally mobile the digital capitalist class and its technology have become, a similarly transnational counter-hegemonic war of position is paramount in resisting this domination [Muh24]. Any such war of position also requires a robust digital commons, since the working class has to win leadership in the institutions where consent forms before it can take power [Gra71], and these institutions depend more and more on modern technological infrastructure. Unfortunately, the capitalist markets and reigning cultural hegemony of today are unconducive to such a commons.

https://doi.org/10.33774/apsa-2026-7606t **ORCID:** https://orcid.org/0009-0003-7784-5415 Content not peer-reviewed by APSA. **License:** CC BY 4.0

The digital capitalist class controls most of the infrastructure on which the press, political parties, unions, and the rest of civil society depend in an increasingly technology-centric 21st century, granting it an inordinate degree of influence over public opinion. Digital capitalists have perfected the practice of [Fee92]'s technological hegemony, as they propagate their beliefs and ideals without most people even conscious of the fact that this is happening. To cite one specific instance of many, tech platforms are now able to decide which posts people see in their feeds in a world where social media is ever more ubiquitous. This allows these platforms to personalize political advertising, news, and all manner of miscellaneous content that affects political trends. Despite many users' objections to such personalization in theory, they often fail to concretely notice—let alone change—the AI and algorithms that decide what they receive [KLSH+21]. Most of the values and priorities woven into Big Tech's infrastructure are thus never written down, all the while shaping the opinions and even options of users. As the growing adoption of [RB13]'s algorithmic governmentality by institutions promotes these unwritten priorities in lieu of explicit rules that the working class can dispute, "we lose the possibility to contest the norm" [RS16].

Class domination has long rested on a Foucauldian "regime of truth" [Fou80]—the control that a select few institutions (such as universities and the press) exert over what society at large accepts as true. The digital capitalist class now enjoys a significant share of this control, as users believe the curated outputs of search engines and AI models. The dominant class's worldview thus becomes part of people's "common sense" [Gra71]—that which they take as given—and the underlying domination goes unrecognized. This differs from the old regime of truth in that digital services reach vast numbers of people at once, far beyond the audience of any one scholarly body or newspaper [Pal26]. Moreover, the ruling institutions of old were held to standards open to public scrutiny, whereas Big Tech sets the rules for its systems behind closed doors, maintaining an a-normative pretence all the while. For instance, the summaries in Google AI Overviews are mostly taken at face value; US users, specifically, open sources only 1% of the time when viewing summaries with citations [CL25]. Platforms further consolidate this control by allegedly "fact-checking" their content, but primarily with their own biased tools [Pal26]. Oftentimes, these services actively make it harder for outsiders to inspect their internal logic. Shortly after purchasing Twitter (now X) in 2022, Elon Musk cut off researchers' bulk access to its data as part of a larger campaign "to silence the free speech of public-interest researchers" [Bla24].

Big Tech's power over what people see (and thus believe) endures because its products are so entrenched in modern society that more ethical options fail to present themselves as viable in the public consciousness. Consider how Apple and Google have come to control such a large share of the market that virtually all widely used mobile devices now run on their software, and most applications are accessed via their digital marketplaces. They are then able to leverage their hold on this "chokepoint" to charge and deprioritize competitors that wish to be listed on the App Store or Google Play, thereby locking users into using their messaging, browsing, navigation, and cloud storage services as well [GD22]. This inertia afflicts not only everyday citizens but governing bodies too—despite scattered (and oftentimes impermanent) attempts by individual cities to switch to open-source alternatives like Linux [Sar26], approximately three-quarters of public administrations' productivity software in the EU still comes from Microsoft [Tri25].

Beyond these practical barriers, the reigning technological hegemony limits what we can even imagine as alternatives [Fee92]. When asked to describe a search engine, people cite Google; when forming a mental image of social media, they think of Instagram or Facebook. Big Tech's products have become what digital services are taken to be by default, as if their underlying design were fundamentally dictated by technical necessity and nothing too drastically deviant could have ever been built. Accordingly, alternatives are judged by how closely they match the perceived norm rather than by what they do differently. Even free software, long seen as the alternative to corporate products [Alc26], is evaluated as a stand-in: Linux is weighed against Windows, and LibreOffice is pitted against Microsoft Office.

https://doi.org/10.33774/apsa-2026-7606t **ORCID:** https://orcid.org/0009-0003-7784-5415 Content not peer-reviewed by APSA. **License:** CC BY 4.0

The openness that defines free software—whose code anyone can see and use, and to which it is easy to contribute—can even help firms win control of platforms. In 2007, Google "heavily invested in" and open-sourced its operating system Android; the ensuing inflow of contributors, combined with phone makers' freedom to adapt Android devices in a myriad of ways, secured Google's place in the mobile device duopoly alongside Apple [WWW24]. In the AI industry, too, open-weight models do little to truly emancipate users from the hold of Big Tech, which ultimately remains in control of the computing infrastructure required to run them—another "chokepoint" [GD22] granting the tech sector the ability to draw rent from customers. Alternatives, however open, escape this hold only if they are owned outside of the dominant class. A few "digital commons projects" [Fuc21], such as Wikipedia, already belong to the communities that build them. More could follow in the form of platform co-operatives owned by their workers—much like [Mar76]'s "freely associated" producers—or online platforms run as a public service (consider, for instance, the broadcasting corporations in Canada, the United Kingdom, and numerous other countries). However, until such alternatives enter the mainstream, society remains as dependent on the digital capitalist class as the state is.

Under [CLL25]'s system of data capitalism, users clash with tech firms over who owns data and who decides how it is used. A worrying trend of platform monopolization tilts this conflict in Big Tech's favour, as dominant firms accrue more and more control over this new form of capital. Once a firm holds a platform market, each new user adds virtually nothing to expenses while contributing to rent, which the firm can afford to raise as demand for its services increases [SS26]. Monopolization extends to the development and sale of AI models as well—owning the integrated system of chips and cloud computing (an advantage enjoyed almost exclusively by Big Tech) is paramount to success in such a market [WWW24]. The largest cloud providers capitalize on this edge by bundling access to models with processing capacity, attracting customers with demand for both goods. Every additional user then generates data used to train and improve these models, whose increased capabilities in turn grow the user bases of the leading firms [Ver24].

More fundamentally, Big Tech's hold extends to the minds of those who depend on its technology. During the Industrial Revolution, burgeoning capitalism proletarianized workers by imbuing machinery with their skills. In a parallel yet more extreme manner, digital capitalism has brought about "the proletarianization of the mind" [Non24] as it leads people to offload their cognitive labour to new technologies capable of these tasks. AI in particular decides what users see and read—from the posts that fill their feeds to the results of their web searches, all too often accepted without question—thereby gradually cementing the worldview it promotes in their minds. People increasingly turn to LLMs like ChatGPT to research topics, to fact-check claims, and even to make crucial decisions on their behalf, ceding human judgment to machines [Pal26, Non24].

In addition to this worrisome surrender of human decision-making capacity, professionals in cornerstone fields such as journalism, healthcare, governance, and law hand much of their actual work to AI. In the legal industry, AI increasingly takes over research and writing tasks that traditionally trained junior lawyers to exercise judgment, eroding a body of expertise integral to the contemporary justice system [Run26]. The temptation to delegate to AI along these lines discourages people from fostering the skills needed to critically engage with modern society, diluting the public discourse underpinning our democratic institutions. Studies like [BBS+25, FTL+25], for instance, show a significant degradation in analytical ability among both secondary and post-secondary students overreliant on LLMs. This atrophy of critical faculties—running from childhood education up to adults' careers, and compounding at every step—bodes poorly for any counter-hegemonic resistance as it leaves people's common sense malleable under the digital capitalist class's technological hegemony. Revolution relies on nurturing the working class's "good sense" [Gra71]—that is, the subset of common sense that is already at odds with the hegemonic Weltanschauung. Regrettably, developing this good sense first requires the same cognitive capabilities that are being steadily worn down by the proletarianization of the mind.

https://doi.org/10.33774/apsa-2026-7606t **ORCID:** https://orcid.org/0009-0003-7784-5415 Content not peer-reviewed by APSA. **License:** CC BY 4.0

Nonetheless, some sites of resistance exist. On occasion, Big Tech's workers have organized against it and won: in 2018, a petition from employees pressured Google into letting its Project Maven contract expire [Tim21], and in 2022, Amazon warehouse workers on Staten Island successfully voted to unionize [AJ23]. Such efforts benefit from the fact that, as in industrial-era capitalism, the workers involved share an employer and often a workplace. However, most of the people exploited under digital capitalism interact with Big Tech as part of a dispersed network of users, and organized resistance on the whole has stalled despite class domination only growing worse [SS26]. Section 6 now turns to what it might take to revitalize such resistance, drawing on everything that we have discussed thus far.

6 Conclusion

Across the interconnected domains of corporate surveillance, institutional governance, national security, and civil society, we have shown that both state and societal dependence on the digital capitalist class degrades the conditions necessary for shared class consciousness and counter-hegemonic resistance. Exploitation becomes less legible (and, in certain forms such as data colonialism, no longer requires even tacit consent); institutions lose authority over the private sector; divides between nations deepen; and the digital commons is enclosed by the dominant class. The civil society necessary to wage a war of position against the digital capitalist class now runs on its technological infrastructure, and the enclosure reaches even further by corroding people's critical faculties—crucial factors in any potential resistance. Such a war must therefore begin by rebuilding the conditions of revolution, by securing the ground that the dominant class does not (yet) own, and by making this modern form of exploitation legible.[2]

Placing digital infrastructure in public hands is key to this crusade, and several public bodies in Europe are already attempting such a transition. France is moving its civil servants to Linux [DIN26], the German state of Schleswig-Holstein is adopting open-source programs [Sta25], and Denmark's Ministry of Digitalization is replacing its Microsoft software with LibreOffice [Bos25]. Likewise, the International Criminal Court is abandoning Microsoft to protect its institutional independence from the US [Tri25]. Still, much of this direction is motivated by the pursuit of technological sovereignty—governments are building toward a more competitive European economy, not necessarily counter-hegemonic resistance [TPSS26]. These governments increasingly justify their switches through the same rhetoric of security seen in Section 4, and the alternatives they seek may lie in private (albeit domestic) hands. Indeed, Big Tech explicitly markets its products to Europe as offering this type of sovereignty [Sar26]; this holds the potential to undermine the start of the shift we have observed thus far. Even open-source software offers no easy escape, with much of its development paid for and directed by the likes of Google and Microsoft [Alc26]. Control over digital infrastructure should rest with the people who depend on it, rather than with governments prone to switching for the sake of sovereignty and competitiveness (or, even worse, with the large corporate firms behind this technology). As the dominant class operates across national borders, a transnational movement of citizens is needed to win this control and cultivate the digital commons [Hab01].

Still, this constitutes only one half of the war of position we need to resist the digital capitalist class—the proletariat also requires organic intellectuals to make it conscious of its own role and to carry it from common sense toward good sense [Gra71]. This common sense is made more difficult to overturn because it is taken for granted rather than held as a view, with technological domination presented as an a-normative, statistical process. Before any progress toward good sense can begin, organic intellectuals have to name the norms that technological processes silently apply, politicizing algorithmic governmental-

[2]It is worth noting that a counter-hegemonic war of position relies on a developed civil society [Gra71]. In regimes like China's, the primary hegemonic power requiring contestation is the authoritarian state, not just the digital capitalist class, and any such war has to assume a radically different form. The strategy we present here instead focuses on countries where revolution primarily means challenging capitalism in a democratic system, not wholesale regime change of an outwardly illiberal order.

https://doi.org/10.33774/apsa-2026-7606t **ORCID:** https://orcid.org/0009-0003-7784-5415 Content not peer-reviewed by APSA. **License:** CC BY 4.0

ity and forcing it back into the discourse of the public sphere [CM19]. Workers across seemingly unrelated professions already hold grievances with large platform monopolies, spawning "thousands of issues waiting to be turned into a movement" [GD22]. For such a movement to materialize, the affected parties have to recognize the digital capitalist class as a shared adversary and the root cause of many of these issues.

One path to such recognition lies in systematically analyzing what a technology does and whom its applications serve, even if these consequences do not appear to be directly tied to its design. All too often, the anger that algorithmic systems provoke is directed at the machine itself rather than at the politicians and engineers advancing their interests through it [CLL25]. However, making these interests legible is a challenge because algorithms form a closed system that only a handful of technical specialists can currently navigate [Non24]. Many of these specialists work for the digital capitalist class itself, placing them in a unique position where they have access to both power and knowledge. In Foucauldian terms, they are "specific intellectuals" [Fou80]—experts whose knowledge allows them to contest the technological hegemony of these systems and undermine the dominant class's power. They could, in theory, serve as the organic intellectuals of the proletariat, but without a larger supporting movement, any objections of theirs rarely travel beyond their own professional circles. A crucial part of this movement, therefore, is making the normative order consciously imposed through these systems recognizable to everyone else. This role of making exploitation legible is open to a wider range of people than the current circle of specialists, but it is imperative to remember that this work can only achieve a measure of success by working with a healthy and functioning public sphere [Hab01].

Fundamentally, a healthy public sphere depends on people who are still able to think for themselves—a capacity threatened by the digital capitalist class's own war of position. A dominant class achieves hegemonic rule by reshaping people's everyday beliefs to reflect its outlook, making its influence and control appear intrinsic to the ordinary functioning of society [Gra71]. At the extreme end of things, we have recently seen this phenomenon take the form of [Non24]'s proletarianization of the mind, as people normalize offloading cognitive tasks to AI. In doing so, they steadily cede the critical faculties needed for any viable resistance to the technology of the class being resisted. This dynamic is far from accidental—Big Tech deliberately builds its products to facilitate surveillance and foster the dependence of its users in such a way that they "delegate ever more decision-making power" to major platforms [GD22].

Even so, Gramsci's account of hegemony leaves us room for resistance. This process of naturalization must be a constant effort—people's beliefs are also shaped by their own daily experiences, and whenever these conflict with the outlook of the hegemonic order, the dominant class begins to lose its hold [Gra71]. The digital capitalist class, especially in the age of AI, eliminates many of these experiences as people transfer their responsibilities to its technology and fail to learn anything in the process. Resistance has to begin with a sustained, collective effort to reclaim the autonomy that we have surrendered to technology.

We should be championing a vision of a better world—one in which we meet people and communities on their own terms, and at their own skill levels. AI, in contrast, takes us to a sanitized view of hollow perfection, as we outsource our very cognition to the same technologies that have become critical infrastructure in the modern economy. A recurring theme throughout this paper is that the power of the digital capitalist class is predicated on the fact that Big Tech has made itself indispensable to both society and the state. Only once we and the institutions that we engineer are able to free ourselves from its grasp can we forge ahead with a counter-hegemonic war of position.

Acknowledgements

L.M.B.V. thanks Loralea Michaelis for helpful conversations about political philosophy; Erika Tuttle for helpful conversations about international politics; and Naomi A. Schoeck for contributions to the wording and the rhetoric of the conclusion.

https://doi.org/10.33774/apsa-2026-7606t **ORCID:** https://orcid.org/0009-0003-7784-5415 Content not peer-reviewed by APSA. **License:** CC BY 4.0

References

[AJ23] Daron Acemoglu and Simon Johnson. *Power and Progress: Our Thousand-Year Struggle Over Technology and Prosperity*. PublicAffairs, 2023. 16

[Akk26] Buse Akkaya. War, artificial intelligence and fetishism: Reflections on Gaza, Iran and Pentagon. *Critical Sociology*, 52(7–8):1625–1633, 2026. 11, 12

[Alc26] Gabriel Alcaras. Beyond severance: The entangled economies of free software, open source and the high-tech industry. *Big Data & Society*, 13(4):1–15, 2026. 14, 16

[And25] Emelie Andersin. The use of the 'Lavender' in Gaza and the law of targeting: AI-decision support systems and facial recognition technology. *Journal of International Humanitarian Legal Studies*, 16(2):336–370, 2025. 5

[AR24] Marco Almada and Anca Radu. The Brussels side-effect: How the AI Act can reduce the global reach of EU policy. *German Law Journal*, 25(4):646–663, 2024. 9, 10

[AvOS17] Elena Aronova, Christine von Oertzen, and David Sepkoski. Introduction: Historicizing Big Data. *Osiris*, 32(1):1–17, 2017. 5

[BBS+25] Hamsa Bastani, Osbert Bastani, Alp Sungu, Haosen Ge, Özge Kabakcı, and Rei Mariman. Generative AI without guardrails can harm learning: Evidence from high school mathematics. *Proceedings of the National Academy of Sciences*, 122(26):e2422633122, 2025. 15

[Bla24] Elizabeth Blakey. The day data transparency died: How Twitter/X cut off access for social research. *Contexts*, 23(2):30–35, 2024. 14

[Blo26] Kayla Blomquist. Racing for recognition? Theorizing emerging status hierarchies and prestige competition in the AI era. *International Affairs*, 102(3):949–970, 2026. 6, 7, 12

[Bos25] Jens Bostrup. Caroline Stage udfaser Microsoft i Digitaliseringsministeriet [Caroline Stage phases out Microsoft in the Ministry of Digitalization]. Politiken, June 2025. https://politiken.dk/viden/tech/art10437680/Caroline-Stage-udfaser-Microsoft-i-Digitaliseringsministeriet. 16

[Bra20] Anu Bradford. *The Brussels Effect: How the European Union Rules the World*. Oxford University Press, 2020. 9

[CC22] Anne S. Y. Cheung and Yongxi Chen. From datafication to data state: Making sense of China's social credit system and its implications. *Law & Social Inquiry*, 47(4):1137–1171, 2022. 7

[CCG25a] Andrea Coveri, Claudio Cozza, and Dario Guarascio. Big Tech and the US digital-military-industrial complex. *Intereconomics*, 60(2):81–87, 2025. 12

[CCG25b] Andrea Coveri, Claudio Cozza, and Dario Guarascio. Blurring boundaries: An analysis of the digital platforms-military nexus. *Review of Political Economy*, 37(4):1632–1663, 2025. 11

[CG22] Mo Chen and Jens Grossklags. Social control in the digital transformation of society: A case study of the Chinese social credit system. *Social Sciences*, 11(6), 2022. Article 229. 6

https://doi.org/10.33774/apsa-2026-7606t **ORCID:** https://orcid.org/0009-0003-7784-5415 Content not peer-reviewed by APSA. **License:** CC BY 4.0

[Cha15] Grégoire Chamayou. *A Theory of the Drone*. The New Press, 2015. Translated by Janet Lloyd. 11

[CIBS26] Kate Conger, Mike Isaac, Julian E. Barnes, and David E. Sanger. Anthropic agents tried to fill out visa forms on State Dept. website. The New York Times, October 2026. https://www.nytimes.com/2026/10/09/technology/anthropic-rogue-ai-agents.html. 9

[CL25] Athena Chapekis and Anna Lieb. Google users are less likely to click on links when an AI summary appears in the results. Pew Research Center, July 2025. https://www.pewresearch.org/short-reads/2025/07/22/google-users-are-less-likely-to-click-on-links-when-an-ai-summary-appears-in-the-results/. 14

[CLL25] Vassilis Charitsis, Mikko Laamanen, and Tuukka Lehtiniemi. Towards algorithmic Luddism: class politics in data capitalism. *Information, Communication & Society*, 28(6):971–988, 2025. 2, 3, 6, 15, 17

[CM19] Nick Couldry and Ulises A. Mejias. Data colonialism: Rethinking big data's relation to the contemporary subject. *Television & New Media*, 20(4):336–349, 2019. 2, 3, 5, 13, 17

[Coe26] Mark Coeckelbergh. Technofascism: AI, Big Tech, and the new authoritarianism. *AI & Society*, 41(5):5163–5176, 2026. 2, 3, 13

[Coh19] Julie E. Cohen. *Between Truth and Power: The Legal Constructions of Informational Capitalism*. Oxford University Press, 2019. 8, 10

[Col80] David Collingridge. *The Social Control of Technology*. Frances Pinter, 1980. 9

[Cou24] Council of Europe. Chart of signatures and ratifications of Treaty 225, September 2024. Accessed 1 November 2026. https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=225. 10

[Cra21] Kate Crawford. *Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence*. Yale University Press, 2021. 8

[DIN26] DINUM. Souveraineté numérique : l'État accélère la réduction de ses dépendances extra-européennes [Digital sovereignty: the State accelerates the reduction of its extra-European dependencies], April 2026. https://www.numerique.gouv.fr/sinformer/espace-presse/souverainete-numerique-reduction-dependances-extra-europeennes/. 16

[Dra24] Mario Draghi. The future of European competitiveness. European Commission, September 2024. https://commission.europa.eu/topics/competitiveness/draghi-report_en. 10

[DT19] Nora A. Draper and Joseph Turow. The corporate cultivation of digital resignation. *New Media & Society*, 21(8):1824–1839, 2019. 4

[Dut17] Dutch Data Protection Authority. Investigation findings re: Windows 10 data collection, October 2017. https://www.autoriteitpersoonsgegevens.nl/uploads/imported/public_version_dutch_dpa_informal_translation_summary_of_investigation_report.pdf. 5

https://doi.org/10.33774/apsa-2026-7606t **ORCID:** https://orcid.org/0009-0003-7784-5415 Content not peer-reviewed by APSA. **License:** CC BY 4.0

[Eur24] European Parliament and Council of the European Union. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). Official Journal of the European Union, July 2024. OJ L, 2024/1689, 12.7.2024. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32024R1689. 9

[FCT24] Benjamin Farrand, Helena Carrapico, and Aleksei Turobov. The new geopolitics of EU cybersecurity: security, economy and sovereignty. *International Affairs*, 100(6):2379–2397, 2024. 12

[Fee92] Andrew Feenberg. Subversive rationalization: Technology, power, and democracy. *Inquiry*, 35(3–4):301–322, 1992. 4, 14

[FN19] Henry Farrell and Abraham L. Newman. Weaponized interdependence: How global economic networks shape state coercion. *International Security*, 44(1):42–79, 2019. 12

[Fou80] Michel Foucault. Truth and power. In *Power/Knowledge: Selected Interviews and Other Writings 1972–1977*, pages 109–133. Pantheon Books, 1980. Translated and edited by Colin Gordon. 14, 17

[Fou07] Michel Foucault. *Security, Territory, Population: Lectures at the Collège de France, 1977–78*. Palgrave Macmillan, 2007. Edited by Michel Senellart. Translated by Graham Burchell. 2, 3

[FTL+25] Yizhou Fan, Luzhen Tang, Huixiao Le, Kejie Shen, Shufang Tan, Yueying Zhao, Yuan Shen, Xinyu Li, and Dragan Gašević. Beware of metacognitive laziness: Effects of generative artificial intelligence on learning motivation, processes, and performance. *British Journal of Educational Technology*, 56(2):489–530, 2025. 15

[Fuc21] Christian Fuchs. History and Class Consciousness 2.0: Georg Lukács in the age of digital capitalism and big data. *Information, Communication & Society*, 24(15):2258–2276, 2021. 3, 15

[Gar17] David Garcia. Leaking privacy and shadow profiles in online social networks. *Science Advances*, 3(8):e1701172, 2017. 5

[GD22] Rebecca Giblin and Cory Doctorow. *Chokepoint Capitalism: How Big Tech and Big Content Captured Creative Labor Markets and How We'll Win Them Back*. Beacon Press, 2022. 3, 7, 9, 12, 14, 15, 17

[Gra71] Antonio Gramsci. *Selections from the Prison Notebooks of Antonio Gramsci*. International Publishers, 1971. Edited and translated by Quintin Hoare and Geoffrey Nowell-Smith. 2, 4, 13, 14, 15, 16, 17

[Hab01] Jürgen Habermas. *The Postnational Constellation: Political Essays*. MIT Press, 2001. Translated and edited by Max Pensky. 10, 13, 16, 17

[HB25] Reid Hoffman and Greg Beato. *Superagency: What Could Possibly Go Right with Our AI Future*. Authors Equity, 2025. 9

https://doi.org/10.33774/apsa-2026-7606t **ORCID:** https://orcid.org/0009-0003-7784-5415 Content not peer-reviewed by APSA. **License:** CC BY 4.0

[HR19] Rodrigo Hernández-Ramírez. On false augmented agency and what surveillance capitalism and user-centered design have to do with it. *Journal of Science and Technology of the Arts*, 11(2):18–27, 2019. 5

[Hu23] Krystal Hu. ChatGPT sets record for fastest-growing user base—analyst note. Reuters, February 2023. https://www.reuters.com/technology/chatgpt-sets-record-fastest-growing-user-base-analyst-note-2023-02-01/. 8

[HZ25] Yujia He and Ka Zeng. A geopolitical economy analysis of China and India's approaches to transnational data governance. *Politics and Governance*, 13, 2025. Article 10361. 6, 7

[IA22] Andrew Iliadis and Amelia Acker. The seer and the seen: Surveying Palantir's surveillance platform. *The Information Society*, 38(5):334–363, 2022. 6

[Ind25] Independent International Commission of Inquiry on the Occupied Palestinian Territory, including East Jerusalem, and Israel. Legal analysis of the conduct of Israel in Gaza pursuant to the Convention on the Prevention and Punishment of the Crime of Genocide. United Nations Human Rights Council, September 2025. Conference room paper A/HRC/60/CRP.3. https://www.ohchr.org/sites/default/files/documents/hrbodies/hrcouncil/sessions-regular/session60/advance-version/a-hrc-60-crp-3.pdf. 5

[Jia24] Mark Jia. Authoritarian privacy. *The University of Chicago Law Review*, 91(3):733–809, 2024. https://lawreview.uchicago.edu/print-archive/authoritarian-privacy. 7

[JIV19] Anna Jobin, Marcello Ienca, and Effy Vayena. The global landscape of AI ethics guidelines. *Nature Machine Intelligence*, 1(9):389–399, 2019. 8

[JSS26] David Jeans, Mike Stone, and Deepa Seetharaman. Anthropic digs in heels in dispute with Pentagon, source says. Reuters, February 2026. https://www.reuters.com/world/anthropic-digs-heels-dispute-with-pentagon-source-says-2026-02-24/. 8

[Kar26] İbrahim Berkan Karataş. Three modalities of algorithmic forgetting: Over-capture, curated, and preemptive. *Memory Studies*, 19(4):1268–1285, 2026. 5

[KLSH+21] Anastasia Kozyreva, Philipp Lorenz-Spreen, Ralph Hertwig, Stephan Lewandowsky, and Stefan M. Herzog. Public attitudes towards algorithmic personalization and use of personal data online: evidence from Germany, Great Britain, and the United States. *Humanities and Social Sciences Communications*, 8(1), 2021. Article 117. 14

[KWW24] Heidy Khlaaf, Sarah Myers West, and Meredith Whittaker. Mind the gap: Foundation models and the covert proliferation of military intelligence, surveillance, and targeting. *arXiv preprint arXiv:2410.14831*, 2024. 11

[KZ25] Alexander C. Karp and Nicholas W. Zamiska. *The Technological Republic: Hard Power, Soft Belief, and the Future of the West*. Crown Currency, 2025. 13

[Lep26] Jill Lepore. *The Rise and Fall of the Artificial State*. Liveright, 2026. 9, 10

https://doi.org/10.33774/apsa-2026-7606t **ORCID:** https://orcid.org/0009-0003-7784-5415 Content not peer-reviewed by APSA. **License:** CC BY 4.0

[Lev18] Yasha Levine. *Surveillance Valley: The Secret Military History of the Internet*. PublicAffairs, 2018. 11

[LGY+25] Jiawei Li, Yang Gao, Yizhe Yang, Yu Bai, Xiaofeng Zhou, Yinghao Li, Huashan Sun, Yuhang Liu, Xingpeng Si, Yuhao Ye, Yixiao Wu, Yiguan Lin, Bin Xu, Bowen Ren, Chong Feng, and Heyan Huang. Fundamental capabilities and applications of large language models: A survey. *ACM Computing Surveys*, 58(2), 2025. Article 38. 8

[Luo22] Yadong Luo. Illusions of techno-nationalism. *Journal of International Business Studies*, 53(3):550–567, 2022. 4, 10, 12

[Maa25] Matthijs M. Maas. *Architectures of Global AI Governance: From Technological Change to Human Choice*. Oxford University Press, 2025. 9, 10

[MAH11] Gary E. Marchant, Braden R. Allenby, and Joseph R. Herkert, editors. *The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight: The Pacing Problem*. Springer Dordrecht, 2011. 9

[Mah25] Adnan Mahmutovic. The EU AI Act: a proactive framework for comprehensive AI regulation. *International Journal of Law and Information Technology*, 33:eaaf028, 2025. 9

[Mal23] Irja Malmio. Ethics as an enabler and a constraint – narratives on technology development and artificial intelligence in military affairs through the case of Project Maven. *Technology in Society*, 72, 2023. Article 102193. 11

[Mar76] Karl Marx. *Capital: A Critique of Political Economy*, volume 1. Penguin, 1976. Translated by Ben Fowkes. 2, 4, 15

[Maz15] Mariana Mazzucato. The US entrepreneurial state. In *The Entrepreneurial State: Debunking Public vs. Private Sector Myths*, pages 79–92. PublicAffairs, revised edition, 2015. 11

[Moi26] Sami Moisio. On geopolitics and geoeconomics of technology: towards a critical geopolitical economy analysis of transnational infrastructures. *Globalizations*, 2026. Ahead of print. 12, 13

[Moy21] Samuel Moyn. *Humane: How the United States Abandoned Peace and Reinvented War*. Farrar, Straus and Giroux, 2021. 11

[MS17] Geoff Martin and Erin Steuter. *Drone Nation: The Political Economy of America's New Way of War*. Lexington Books, 2017. 11

[Muh24] Thomas Muhr. Gramsci and hegemonic struggle in a globalized world. In William K. Carroll, editor, *The Elgar Companion to Antonio Gramsci*, pages 406–426. Edward Elgar Publishing, 2024. 13

[Mun23] Luke Munn. The uselessness of AI ethics. *AI and Ethics*, 3(3):869–877, 2023. 8

[Non24] Anaïs Nony. Proletarianization of the mind: A media theory of artificial intelligence after Simondon and Stiegler. *Trópos. Rivista di ermeneutica e critica filosofica*, 16(1):116–136, 2024. 15, 17

[Pal26] Rosario Palese. Artificial truth: Algorithmic power, epistemic authority, and the crisis of democratic knowledge. *Societies*, 16(3), 2026. Article 102. 3, 14, 15

https://doi.org/10.33774/apsa-2026-7606t **ORCID:** https://orcid.org/0009-0003-7784-5415 Content not peer-reviewed by APSA. **License:** CC BY 4.0

[Per26] Billy Perrigo. Exclusive: Anthropic drops flagship safety pledge. TIME, February 2026. https://time.com/7380854/exclusive-anthropic-drops-flagship-safety-pledge/. 8

[RB13] Antoinette Rouvroy and Thomas Berns. Algorithmic governmentality and prospects of emancipation: Disparateness as a precondition for individuation through relationships? *Réseaux*, 177(1):163–196, 2013. Translated by Liz Carey-Libbrecht. 1, 3, 6, 7, 14

[Rob20] William I. Robinson. Global capitalism post-pandemic. *Race & Class*, 62(2):3–13, 2020. 13

[Roo26] Kevin Roose. Why the Hugging Face hack should make you worry more about A.I. The New York Times, September 2026. https://www.nytimes.com/2026/09/03/technology/openai-hugging-face-hacking.html. 9

[RR20] Anaïs Rességuier and Rowena Rodrigues. AI ethics should not remain toothless! A call to bring back the teeth of ethics. *Big Data & Society*, 7(2):1–5, 2020. 8

[RS16] Antoinette Rouvroy and Bernard Stiegler. The digital regime of truth: From the algorithmic governmentality to a new rule of law. *La Deleuziana*, 3:6–29, 2016. Translated by Anaïs Nony and Benoît Dillet. 9, 14

[RSV24] Ondřej Rosendorf, Michal Smetana, and Marek Vranka. Algorithmic aversion? Experimental evidence on the elasticity of public attitudes to "killer robots". *Security Studies*, 33(1):115–145, 2024. 12

[Run26] Natalie Runyon. Honing legal judgment: The AI era requires changes to how lawyers are trained during and after law school. Thomson Reuters Institute, April 2026. https://www.thomsonreuters.com/en-us/posts/legal/honing-legal-judgment-training-lawyers/. 15

[Sar26] Advait Sarkar. Searching for European alternatives: Digital sovereignty, digital patriotism, and the emerging geopolitics of software adoption. *arXiv preprint arXiv:2604.15767*, 2026. 14, 16

[Sch99] Dan Schiller. *Digital Capitalism: Networking the Global Market System*. MIT Press, 1999. 2

[Sha02] Martin Shaw. Risk-transfer militarism, small massacres and the historic legitimacy of war. *International Relations*, 16(3):343–359, 2002. 11

[Soy94] Yasemin Nuhoğlu Soysal. *Limits of Citizenship: Migrants and Postnational Membership in Europe*. University of Chicago Press, 1994. 10, 13

[Spo25] Ken Spours. Socialized systems of generative artificial intelligence and the roles of technological organic intellectuals. *Systems*, 13(11), 2025. Article 944. 13

[Srn17] Nick Srnicek. *Platform Capitalism*. Polity Press, 2017. 2, 6

[SS26] Kohei Saito and Ryuji Sasaki. Rentier capitalism, technofascism and the destruction of the common. *Area Development and Policy*, 11(1):1–15, 2026. 2, 3, 4, 6, 15, 16

https://doi.org/10.33774/apsa-2026-7606t **ORCID:** https://orcid.org/0009-0003-7784-5415 Content not peer-reviewed by APSA. **License:** CC BY 4.0

[Sta25] Staatskanzlei Schleswig-Holstein. Digitale Souveränität ist möglich und wirtschaftlich [Digital sovereignty is possible and economical], December 2025. https://www.schleswig-holstein.de/DE/landesregierung/ministerien-behoerden/I/_startseite/Artikel2025/IV/251204_cds_digitale_souveraenitaet. 16

[TDV25] Nitasha Tiku and Gerrit De Vynck. Google drops pledge not to use AI for weapons or surveillance. The Washington Post, February 2025. https://www.washingtonpost.com/technology/2025/02/04/google-ai-policies-weapons-harm/. 8

[Tim21] Scott Timcke. *Algorithms and the End of Politics: How Technology Shapes 21st-Century American Life*. Bristol University Press, 2021. 13, 16

[Tof70] Alvin Toffler. *Future Shock*. Random House, 1970. 9

[TPSS26] Leo Thüer, Julia Pohle, Milan Schröder, and Alissa Steer. Exporting the European third way: strategic narratives of a value-based digital order. *European Politics and Society*, 2026. Ahead of print. 16

[Tri25] Jennifer Tridgell. Justice recoded? Why it matters that the International Criminal Court embraced open-source software and ditched Microsoft. EJIL:Talk!, November 2025. https://www.ejiltalk.org/justice-recoded-why-it-matters-that-the-international-criminal-court-embraced-open-source-software-and-ditched-microsoft/. 14, 16

[Var23] Yanis Varoufakis. *Technofeudalism: What Killed Capitalism*. The Bodley Head, 2023. 2

[Ver24] Pieter Verdegem. Dismantling AI capitalism: the commons as an alternative to the power concentration of Big Tech. *AI & Society*, 39(2):727–737, 2024. 2, 3, 15

[Wag18] Ben Wagner. Ethics as an escape from regulation. From "ethics-washing" to ethics-shopping? In Emre Bayamlioğlu, Irina Baraliuc, Liisa Janssens, and Mireille Hildebrandt, editors, *Being Profiled: Cogitas Ergo Sum. 10 Years of Profiling the European Citizen*, pages 84–89. Amsterdam University Press, 2018. 8

[Wan25] Dan Wang. *Breakneck: China's Quest to Engineer the Future*. W. W. Norton & Company, 2025. 6, 11

[WHKB25] Jennifer Wang, Kayla Huang, Kevin Klyman, and Rishi Bommasani. Do AI companies make good on voluntary commitments to the White House? *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society*, 8(3):2625–2636, 2025. 8

[WWW24] David Gray Widder, Meredith Whittaker, and Sarah Myers West. Why 'open' AI systems are actually closed, and why this matters. *Nature*, 635(8040):827–833, 2024. 15

[Zha24] Kevin Honglin Zhang. Geoeconomics of US-China tech rivalry and industrial policy. *Asia and the Global Economy*, 4(2), 2024. Article 100098. 10, 12

[Zub19] Shoshana Zuboff. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs, 2019. 4, 5, 6

https://doi.org/10.33774/apsa-2026-7606t **ORCID:** https://orcid.org/0009-0003-7784-5415 Content not peer-reviewed by APSA. **License:** CC BY 4.0