

Governing AI innovation under EU-style capitalism

ROBIN MANSELL

DEPARTMENT OF MEDIA AND COMMUNICATIONS, LONDON SCHOOL OF ECONOMICS AND POLITICAL SCIENCE, UK

ABSTRACT

In seeking a leading position in the artificial intelligence (AI) space through EU legislation aimed at securing innovation and market leadership and fundamental human rights, the European Commission's ambition is to ensure that AI systems benefit all. In this chapter, I critically assess this ambition by historicising efforts to govern digital technologies and examining the characteristics of the contemporary "AI industry" and the discourses of selected governing texts. I argue that the prevailing imaginary of a technologically mediated future that frames governance in this space clashes with governing in the name of justice and the protection of human rights. Current governance initiatives are likely to restrain some excesses of a capitalist-inspired "AI industry". If the prevailing imaginary of progress is not dislodged by resistance strategies, however, neither corporate-led technology innovation nor state-led governance measures are likely to yield a future consistent with their claimed support for human rights and greater equality.

KEYWORDS: artificial intelligence, digital governance, regulation, human rights, digital future imaginaries

Mansell, R. (2026). Governing AI innovation under EU-style capitalism. In A. Balčytienė, P. Bajomi-Lázár, & H. Sousa (Eds.), *Digital media shadowing democracy: Technology, communication, and power* (pp. 197–218). Nordicom, University of Gothenburg. <https://doi.org/10.48335/9789189864290-10>

Introduction

It is always tricky to assess the likely outcomes of governance in the making especially when governance is understood broadly to encompass patterns of rules that underpin social orders (Puppis et al., 2024). The EU's Artificial Intelligence (AI) Act was transposed into law which became applicable in 2025 (European Union, 2024). In this chapter I interrogate the contradictory ambitions embedded in this approach to "AI system" governance. My aim is to assess the likelihood that respect for human rights, justice, and equality can be achieved in practice by the governance measures that are being put in place. "AI systems" are implicated along with the datafication practices of digital platforms in creating havoc in societies around the world, so much so that elite state and corporate leaders who frequent the World Economic Forum (WEF) are worried. The WEF's *Global Risks Report 2024* ranked spiralling mis- and disinformation as risk number one, noting that current and future digital systems are implicated in a "vicious cycle that could trigger civil unrest and possibly confrontation" (World Economic Forum, 2024: 88). Ranked first again in the Forum's 2025 report, the rise of digital platforms, growing volumes of AI-generated content, algorithmic biases, and the ease with which government surveillance can be conducted were all linked to risks associated with mis- and disinformation (World Economic Forum, 2025). The WEF has called for proportionate responses that do not stand in the way of the innovations that are key to "unlocking a multitude of the world's problems" (World Economic Forum, 2024: 88).

In the institutional political economy of media and communication tradition (Mansell, 2023; Winseck, 2024), my analysis highlights how the prevailing imaginary of technologically mediated progress works to normalise recourse to risk mitigation governance strategies that align "AI systems" principally with capitalist ambitions for profit, even as they champion the protection of human rights. These "AI systems" are progressively becoming embedded in digital societies and they are used to augment existing processes of datafication and platformisation, providing new means of surveillance, amplifying mis- and disinformation and threatening the very foundations of democracy.

I begin by renaming. The consensus definition of an "AI system", agreed by OECD member states and accepted by the EU, is "a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments" (OECD, 2023: 7). Instead, I employ the label systems for statistical propositions (SSPs) in this chapter (except when I refer to specific documents that use AI language). The term "SSP" was proposed at a UNESCO conference in 2024 as part of a glossary of terms to support discussion of the benefits and harms of technological advances more transparently (Frau-Meigs, 2024). The rationale for this renaming is that it draws attention to what large language models

(LLMs) actually do, and it signals that advances in “AI systems” have a long history of using anthropomorphic language to imply that these systems are approaching, or about to exceed, human cognitive abilities (Chokshi & Mansell, 2026; Natale & Ballatore, 2020). It might be argued that the language of AI or machine learning is indicative of an emergent science that must name its insights even if this results in “an impoverished reductionist view” of what “intelligence” is. It might also be suggested that “nobody can swim against” these namings once they take hold in policy discourse (Floridi & Nobre, 2024: 9–10). I suggest, however, that renaming can work as an essential act in destabilising the prevailing imaginaries that guide innovation and governance in this field.

In the face of claims that recent “accidental” SSP innovations might be “the Copernican trauma that shifts us from a design career as the authors of the Anthropocene to the role of supporting actors in the arrival of the post-Anthropocene” (Bratton, 2015: 365), scholars are exploring governance approaches – both state-initiated and local strategies – that might secure the accountability of SSP providers (Crawford, 2021; Katzenbach & Ulbricht, 2019; Mejias & Couldry, 2024; Zuboff, 2022). Most agree that “AI system” governance approaches are nascent and that how they are applied will influence the way societal, political, cultural, and economic conditions are mediated. My analysis is developed first by historicising SSPs and (Western) governance responses. I then briefly profile the marketisation of SSPs, attending to some of the characteristics of the market where SSP tools and applications are being deployed. This is followed by a parsing of contemporary SSP governance actions based on a critical examination of discourse emphasising the principal imaginaries about SSPs and the outcomes expected of governance measures. In the next section I address reflections on imaginaries and power and discuss why state-led governance measures may mitigate the excesses of capitalist profit-driven SSP innovation to some extent, but are not aligned with strategies aimed at reimagining a just and equitable technologically mediated future.

Historicising SSPs and (Western) governance responses

It is asked again and again whether it is possible to open technology “black boxes” to understand their embeddedness in societies. The imaginary of these technological systems as revolutionary and disruptive, and as requiring societal adaptation, flourishes with each innovation that makes its way to the market. This is especially the case for digital technologies. In the 1970s, the technologies of direct broadcasting, cable television, discs, cassettes, and the fax machine were touted as revolutionary. In the late 1980s, digital hardware and software were expected to yield transformative revolutionary AI expert systems. In the 1990s, major strides in natural language processing, computer graphics (virtual reality), and intelligent agents were acclaimed for their potential benefits. In 2005, it was envisaged that cybercrime “will often involve no human

interface, being completely automated” (United Nations Conference on Trade and Development, 2005: 235). It was noted that security and trust concerns would have to be addressed if the full benefits of these innovations were to be realised (International Telecommunication Union, 2006).

There was discussion about what to do about malicious botnets and about the privacy implications of photo identification and, by 2010, cloud computing and “AI-as-a-service” were already being marketed. Whether designated as the future Internet, the Internet of Things, ambient computing, affective computing, bioelectronics, neuro-electronics, or human-computer symbiosis, risks to privacy and data protection, social justice and equity, safety, security, and trust were clearly on the policy agenda. EU official Gérald Santucci imagined in 2011 that “by year 2060, a biot (an object at the interface of cybernetics, biotechnology), and cognition” would enable Internet-aware “social objects” as facilitators of human interaction (Santucci, 2011: para. 5). In 2013, the WEF was “passionate” about the power of data analytics, and robots operating in unstructured environments were prominent in policy discourses, all raising ethical concerns (Bibao-Osorio et al., 2013: 79; Van Woensel et al., 2016). In 2016, the National Science and Technology Council (2016: 2) in the US strongly emphasised that AI would require “a data-literate citizenry”.

As digitised SSPs spread through Western countries, guidelines on the protection of personal data and transborder data flows (1980) and on information system security (1992) were published by the OECD aiming to amplify privacy protection and the safety of computational systems. The Council of Europe agreed a convention on protecting individuals regarding the automatic processing of personal data in 1981. The EU had a regulation in place on the processing of personal data and the free movement of data in 1995 and on the security of information systems in 2002. Throughout these decades, the urgency of achieving control over these technical systems was repeatedly expressed. Thus, it is not credible to suggest that policymakers were caught off guard by more recent challenges presented by SSPs. Before turning to an assessment of current initiatives to govern SSPs, the unfolding marketisation of SSPs is considered.

The marketisation of SSPs

The SSP industry (known as the “AI industry”) is highly concentrated, but it is difficult to draw a clear boundary around the actors in a complex value chain from chip producers to end users of these systems. An indication of the market power of key actors is suggested by focusing on semiconductors. These are the material substrate of an industry dominated by NVIDIA, US-owned, for chip design; ASML, founded by Philips and Dutch-owned, for semiconductor manufacturing equipment; TSMC, Taiwanese-owned, for chip fabrication; and a combination of Amazon Web Services, Microsoft Azure, and Google Cloud, plus others, for computing power. Large companies such as Meta, Alphabet/

Google, and Amazon have their own computing infrastructure, but many other system developers access computing power from infrastructure-as-a-service companies. Many developers of LLMs are subsidiaries of the largest technology companies, or they have partnership agreements with them, for example, Anthropic, Cohere, Google DeepMind, Hugging Face, OpenAI, and Stability AI. Based on various online sources, in 2024, Microsoft's market capitalisation was around 3 trillion US dollars, Alphabet's 1.8 trillion, Amazon's 1.8 trillion, Nvidia's 1.8 trillion, and Apple's and Meta's 1.2 trillion each.

The scale of investment in SSPs is huge. In 2022, private investment in AI companies was estimated at 92 billion US dollars, with the US in the lead (47 billion), followed by China (13 billion) and the UK (4 billion). The top EU country was Germany (2 billion) (Maslej et al., 2023). By 2024, global private investment had reached 130 billion US dollars (Our World in Data, 2025), and the investment profiles of countries and regions with AI startups and large companies continued to trend upwards (Ene, 2025). In 2025, OpenAI alone secured 40 billion US dollars in private financing commitments and was valued at 300 billion US dollars, although it was unclear just how much of this commitment will be met since the full amount is contingent on other companies' fund-raising efforts (Zitron, 2025). EU public investment pales by comparison. Between 2014 and 2020, the EU is estimated to have invested 10 billion euros through its framework programmes, with a further 20 billion euros committed by 2030. Much of this spending is allocated to technology development and a smaller amount to research on the social environment (Galdon-Clavell et al., 2023).

Some companies develop their own "generative AI" models, or they incorporate others' models into their services. Most of these models are proprietary, with companies actively promoting tools for content creation, design and art, software development, language translation, healthcare, and gaming and finance, to name only a few application fields. The news industry and the journalism profession are being reshaped by their increasing use of SSPs in the selection, production, and distribution of news and by new tools supporting audience analytics. The news industry is confronted with asymmetrical power between news organisations and the digital platforms, which threatens the former's traditional revenue streams and the sustainability of many news outlets, also raising concerns about the future of journalism independence and autonomy as the use of "AI system" tools becomes commonplace in the newsroom (Beckett & Yaseen, 2023; Simon, 2022).

As SSPs permeate all segments of societies, the high costs of developing the underlying LLMs means that the search is on for ways to monetise investments. Some companies offer model access to individuals (sometimes vetted) for free; for example, Microsoft based on OpenAI technology offers Bing AI and, from February 2023, started a subscription plan for ChatGPT Plus at 20 US dollars per month. Meta's LLM is open sourced for non-commercial open-science use, ostensibly transparently, but most models are

proprietary with licensing arrangements for use by other companies and states as well as through subscription arrangements. LLM developers have been found to engage in “open-washing”, that is, “selective and self-serving forms of openness”, when they claim to meet open-source criteria but fail to provide access to model training parameters, do not disclose the training data, or place restrictions on source-code modification (Liesenfeld & Dingemans, 2024: 1776). From writing and coding assistants to image generation assistants, the market is expanding rapidly, with companies beyond the most prominent ones mushrooming. The SSP companies’ market prospects depend upon huge datasets scraped from open web sources to create “data lakes”, and copyright infringement cases brought against companies including Anthropic, OpenAI, and Google are making their way through the courts, leading to uncertainty about how long data will be free for the taking (Mishcon de Reya, 2024; Sookman, 2024). LLM developers are also dependent upon the quality of data they harvest, and some companies are using their own internal data sources (Zaharia & Bischoff, 2024). All these companies are expected to ensure that their data uses are compliant with legislation that has been in place for some time, for example, the EU General Data Protection Regulation, but this has not stopped LLM developers from securing data from online sources regardless of whether explicit permission has been granted (Mansell, 2025).

Scholars seeking to map corporate affiliations, ownership linkages, and, indeed, the market niches of companies using the “AI” designation run into difficulties. Reports on finance and ownership yield a messy and often inconsistent picture. Governing this industry is likely to be no less challenging than governing the digital platform market has proven to be, not only because of the growing complexity of SSP systems, but because of the capacity of companies to insist that the priority is rapid innovation to secure their business prospects and the economic growth of countries and regions. Thus, “if AI becomes one of the most economically and strategically important technologies of the 21st century [...], the geographic distribution of access to compute, and therefore the ability to develop and deploy AI without hindrance and oversight from other states” (Sastry et al., 2024: 46), will influence the global distribution of power and prosperity. Most market analysts expect the top-ranked technology companies to hold onto their leading status in the market, although there is speculation that new entrants will disrupt current rankings and the financial prospects of individual companies are likely to wax and wane (Gerard, 2025). In 2024, leading Big Tech figures – Thiel (Palantir), Bezos (Amazon), and Zuckerberg (Meta) among them – started selling off larger-than-usual tranches of their own shares (Temple-West & Kinder, 2024). This may signal that the road ahead is likely to be bumpy as the governance of platforms and the “AI industry” ramps up in Europe and the costs of monetisation increase in terms of both computational resources and mounting fines for departures from globally agreed upon ethical principles (Gibson, 2024; United Nations, 2024a).

What it is unlikely to signal, however, is a substantial change in the prevailing imaginary of a technologically mediated future in which power accrues to technology companies inversely to its accrual to users of their technologies. All these companies are expanding the capabilities of SSP systems and the “use cases” for generative AI. These developments are depicted as “game-changing” (United Nations AI Advisory Board, 2023: 1), with imaginaries of what SSP systems can “do” extending to their potential to ameliorate every crisis. In the case of the EU, for example, its circular economy action plan to respond to the climate change crisis calls for “innovative models [...] powered by digital technologies, such as the internet of things, big data, blockchain and artificial intelligence”, with a view to making Europe less dependent on primary materials (European Commission, 2020: 2).

Innovation policy and governance in this area – as in others – is dominated by supply-push thinking and funding (Borrás & Edquist, 2019). And as Helga Nowotny (2021: 20) has aptly observed, “when self-fulfilling prophecies begin to proliferate, we risk returning to a deterministic worldview in which the future appears as predetermined and hence closed”. Designers and commercial owners of past and present SSP systems are guided by “the fundamental impulse that sets and keeps the capitalist engine in motion” – new goods, new methods of production, and new markets (Schumpeter, 1942: 82–83). The question is how to “incentivize powerful firms to ‘do the right thing’” (Cusumano et al., 2021: 1280), when what the “right thing” is remains contested. Effective governance requires that companies are “hailed in from the unregulated wilderness in which they are free to roam to destroy as they, or rather those who own them, please” (Nowotny, 2021: 160–161). If the prevailing imaginary of SSP systems persists, as depicted by developer Yoshua Bengio, then we should be sceptical about claims that state-led governance will incentivise the larger and smaller technology players to do the “right thing”:

Superhuman AI could give unprecedented power to those who control it, whether individuals, corporations, or governments, threatening democracy and geopolitical stability. [...] In the extreme, a few individuals controlling superhuman AIs would accrue a level of power never before seen in human history. (Bengio, 2023: paras. 12, 5)

Bengio, like others in the technical community, hopes that a combination of self-regulation and state-led governance will provide a counterbalance to the technology owners’ ambitions. The next section explores the traction likely to be achieved in making the current and future SSP systems responsive to non-economic goals by critically examining the discourses of “AI system” or SSP system governance.

Parsing of contemporary SSP system governance

Given the EU AI Act’s explicit aim of balancing corporate interests in market leadership with broader goals linked to human rights and safety, I start with

this Act and then profile some of the governance moves being taken elsewhere. The following is not intended as a legal analysis but as an opportunity to reflect on the principal imaginary of power relations between government and corporate governors and the governed.

The EU Artificial Intelligence Act

The EU's discourse about the governance of SSP systems is clear: "Trustworthy AI" should "serve to maintain and foster democratic processes and respect the plurality of values and life choices of individuals" (High-Level Expert Group on AI, 2019: 11). The AI Act now has the force of law. The Act's purpose is to "improve the functioning of the internal market and promoting the uptake of human-centric and trustworthy artificial intelligence" (European Union, 2024: 44), with a high level of protection for health, safety, and fundamental rights, and with ambitions for promoting innovation. A long list of rights is to be protected, with the expectation being that the regulation will curtail "reasonably foreseeable misuse" of AI (European Union, 2024: 19), including generative systems. A tiered approach – prohibited, high risk (including systemic risk for generative AI), and non-high risk – is adopted. The close reading of the discourse that follows confirms there is considerable room for judgement in this new governance text.

In the prohibited category is a list of SSP tools and applications, including subliminal techniques, that "materially" distort behaviour in a manner that "causes or is likely to cause" physical or psychological harm (European Union, 2024: 50). The use of "real-time" remote biometric identification systems in public spaces for law enforcement is prohibited unless it is "strictly necessary" (European Union, 2024: 52). Various forms of profiling are prohibited if this is the only basis for predicting human behaviours. Other conditional and subjective terms relate to whether the collection or generation of data leads to "unfavourable" treatment or treatment that is "disproportionate". Overall, systems with the aim of "materially" distorting behaviour, or those that are deemed "particularly" dangerous, are forbidden.

For SSP systems deemed to be high risk, effective risk management strategies are required. These are to be developed to ensure that the "relevant" residual risk associated with a hazard and the overall residual risk are "acceptable". SSP systems should be "effectively" overseen by humans, "as appropriate and proportionate" (European Union, 2024: 60). In the case of "general-purpose AI models", these are associated with systemic risk when a LLM involves a "cumulative amount of computation used for its training measured in floating point operations is greater than 10^{25} " (European Union, 2024: 83). This is a measure of the processing performance and complexity of an AI model which may be altered over time, but which neglects the fact that less complex models are also associated with risks. Third parties relying on tools, services, processes, or components under open licences are "encouraged" to implement

good practices. Systems for exclusively military, defence, or national security purposes are not covered by the Act, but when an AI system falls within the scope of the Act, organisations are not prevented from engaging in military activities. Military and security agencies are asking populations to “trust us on AI” (Scott, 2024). Thus, while companies such as Palantir and Clearview AI provide SSP systems for use in war zones, the aim is to achieve “responsible” military use through dialogue and voluntary controls (The White House, 2023).

Compliance with the Act requires judgements by numerous actors. Because standards have yet to be fully developed for advanced SSP systems, a General-Purpose AI Code of Practice, released in July 2025, has been developed by experts including AI providers, government and civil society representatives, and academics (European Commission, 2025). The code is voluntary for non-high-risk systems and addresses issues relating to transparency, copyright, and safety and security. At the time of writing, it had been signed by 27 AI companies, including the industry leaders. Codes of conduct are also being developed by the industry, albeit with the participation of relevant authorities, and they are voluntary for non-high-risk systems. And, new institutions are created by the Act: the European Artificial Intelligence Board, with high-level national supervisory authority representatives including the European Data Protection Supervisor and European Commission authorities; and the AI Office as a centre of expertise (European Union, 2024).

The AI Act calls for investment in “AI literacy”, which is understood as the skills, knowledge, and understanding that allow providers, users, and others affected to “make an informed deployment of AI systems” (European Union, 2024: 49); but, providers are expected to enable literacy only “to their best extent” (European Union, 2024: 51). Literacy should enable individual users to be aware of “automation bias”; they should learn to interpret high-risk SSP system output “correctly” (European Union, 2024: 60). The prevention of harms is to be enabled by instructions for system use. If redress is sought, complaints can be made by SSP users, who should then receive “clear and meaningful explanations” of the role of the system in decision-making (European Union, 2024: 110), and, in line with other legislation, there is a variety of fines for non-compliance.

In summary, the Act’s overall aim is “responsible innovation”, which safeguards by mitigating risk while seeking to “accelerate” the development and marketing of high-risk systems. In complying, system providers should take account of the “generally acknowledged state of the art”, and it is acknowledged that risk management can deal only with “reasonably foreseeable misuse” and “known or foreseeable circumstances” (European Union, 2024: 35–36, 55–56). In addition, new measures should minimise restrictions on international trade (European Union, 2024: 13). For SSP systems already on the market, public authority users have four years to comply and, in the case of “generative AI” models already on the market, they have several years. This account of the discourse signals substantial

opportunities for judgement and dispute. The Act also normalises certain commercial datafication practices – that is, “common and legitimate commercial practices” used in targeted advertising must comply with existing law, but should not “in themselves be regarded as constituting harmful manipulative AI practices” (European Union, 2024: 9).

There are additional ambiguities. Regarding “generative AI”, the full range of capabilities is to be better understood after their release on the market. If innovative SSPs are deemed crucial for health and safety, environment protection, or “society as a whole”, high-risk systems can be deployed without compliance or authorisation, provided requests are made during or after the use and “without undue delay” (European Union, 2024: 33). With these numerous conditionalities, the prevailing imaginary of progress is consistent with expansive commercial datafication, and there is considerable ambiguity around whether the governance regime can align with economic priorities and with the protection of human rights at the same time.

Other governance measures in and beyond the EU

The EU’s SSP system governance initiatives are interwoven with multiple existing measures from the General Data Protection Regulation, applying to the processing of personal data to regulations concerning non-personal data processing and legislation on data security. The AI Act also comes on the heels of the Digital Services Act (European Union, 2022b) and Digital Markets Act (European Union, 2022a), with the former aiming to ensure that the largest digital platform companies provide a safe, rights-respecting digital space, and the latter at creating a level playing field to boost innovation, growth, and competitiveness. In a US context of increasing protectionism and geopolitical tension, the Biden Administration’s Blueprint for an AI Bill of Rights and an AI Risk Management Framework were accompanied by a National Artificial Intelligence Research and Development Strategic Plan. Like the EU’s approach – with the distinction that all measures were voluntary – the aim was to evaluate “AI systems” using yet-to-be-developed standards and benchmarks with a risk mitigation strategy to ensure that investment would serve the public good. Again, there was ambiguity when it was acknowledged that risks are currently “difficult to quantify” (Select Committee on Artificial Intelligence of the National Science and Technology Council, 2023: vii, 17). Nevertheless, the presumption was that governance will ensure that these systems are “valid and reliable, safe, secure and resilient, accountable and transparent, explainable and interpretable, privacy-enhanced, and fair with harmful bias managed” (National Institute of Standards and Technology, 2023: 12). Tougher measures were put in place to govern “industrial-scale compute” targeting the most advanced chips, largest data centres, and frontier “generative AI” model training. This was all still in line with efforts by the US to secure its dominance of the global market. Experts noted, however,

that more research would be needed before efforts to control “compute power” could be effective: “naïve or poorly scoped approaches to compute governance carry significant risks in areas like privacy, economic impacts, and centralization of power” (Sastry et al., 2024: 1).

The SSP governance landscape aligns with a discourse welcoming an imaginary of ever-expanding datafication overseen by risk mitigation measures. A risk mitigation approach is visible in the United Nations Roadmap for Digital Cooperation, which calls for audits and certification schemes to monitor the compliance of SSP systems with (yet-to-be-agreed) engineering standards (United Nations, 2020; see also United Nations, 2024a). Its report, *Governing AI for Humanity*, echoes an ahistorical view of innovation, insisting that “capabilities once hardly imaginable have been emerging at a rapid, unprecedented pace” and should “leave no one behind” as the imaginary of progress unfolds (United Nations AI Advisory Board, 2023: 2–3). When the UN General Assembly adopted its resolution on AI, it acknowledged that the risks and harms of “improper or malicious design, development, deployment and use” of these systems can occur without adequate safeguards (United Nations, 2024b: 3). Consistency with the prevailing imaginary of digitally mediated progress was signalled by the adoption of the text without a vote. The agreed text only “encourages” member states and other stakeholders not to deploy systems that do not comply with human rights law or that pose “undue” risk to people’s enjoyment of their human rights. Similarly, OECD countries call for “responsible stewardship”, respect for “the rule of law, human rights and democratic values”, and safeguards “appropriate to the context and consistent with the state of the art” (OECD, 2023: 7–8). This is echoed in the Council of Europe’s Framework Convention on Artificial Intelligence, Human Rights, Democracy and Rule of Law (Council of Europe, 2024). The Council also updated its Convention on the protection of individuals and the processing of personal data and issued recommendations on media freedom, the right to freedom of expression, the roles and responsibilities of Internet intermediaries, and the protection of journalists. In the American context, with a new Trump Administration, risk mitigation measures seem to be abandoned as President Trump issues executive orders calling for a flexible AI regulatory environment and the removal of barriers to AI innovation at the federal level (The White House, 2025a, 2025b). US states are putting a variety of AI governance measures in the place, but the overriding ambition is to boost US-owned AI company prospects on the global market, and to do so by ramping up the application of SSPs in every facet of the lifeworld.

In view of aspirations for inclusivity and leaving no one behind in SSP use throughout the world, it is worth noting that in March 2024, of 55 African countries, only five had specific “AI strategies” in place. Of these 55 countries, 15 had introduced an AI task force, expert body, agency, council, or committee; some 37 had data protection laws, but only 29 had operational data protection authorities (Tech Hive Advisory Center for Law & Innovation, 2024). The next

section offers a critical evaluation of these multiple initiatives to govern SSPs within the confines of the prevailing imaginary of digitally mediated progress.

Reflections on imaginaries and power

The foregoing discussion amply demonstrates that it is misleading when policymakers seeking to govern SSPs claim to be taken by surprise by the speed of innovation. In practice, today's plethora of SSP governance measures aimed at risk assessment and mitigation bear many similarities to those adopted for earlier generations of digital technology. They embrace ambiguities, and their outcomes will be conditioned by power relations that influence judgements in contexts where the regulatory texts are open to interpretation (Mansell, 2023). The SSP governance instruments discussed in the preceding section are not the only ones, but my aim is to highlight common features of those discussed here.

One commonality is that SSP innovations are positioned as disruptive and inevitably risky because of the speed of change, which it is claimed could not be foreseen. This is so despite the fact that claims about the apparently unforeseen or “emergent” abilities of LLMs could be attributable to a change in the metric that is used to indicate the growing capabilities of these models. The measure currently being used conveys the impression that developments in computer processing performance are discontinuous, whereas earlier metrics might provide a profile of continuous change in LLM performance (Schaeffer et al., 2023). The former discontinuous profile is attractive to an industry agenda intent on promoting unprecedented technological progress as being beneficial to humanity. The logic of unprecedented disruptive and discontinuous progress aligns with economic explanations about the benefits of “disruptive innovation” for economic growth. When Big Tech firms argue that their “AI systems” will bring greater efficiency and increased productivity – and growth – their claims elide with the idea that this is the optimal pathway towards sustainability and global “developmental” equity (Acemoglu & Johnson, 2023). Another commonality is that governance initiatives such as the AI Act are positioned to operate in the context of corporate and state interests in data monetisation and market leadership with ambiguous emphases on individual rights protection and collective interests, since the latter struggle to be balanced with the priority given to attaining market leadership.

Differences in the *locus* of power are sometimes drawn between rights-driven, market-driven, and state-driven governance approaches in the EU, the US, and China (Bradford, 2020; Wang et al., 2024). In practice, these are differences of degree. In China, SSP system legislation explicitly privileges state interests in deploying advanced SSPs to maintain social order; but, arguably, the emphasis on preserving democracy in the EU and US implicitly has a similar intent. In the US, First Amendment speech rights condition governance measures, and there is a strong emphasis on the “free market”, except when competitiveness in the global market is at stake. In the EU, human rights

protection is central, but protections, as indicated in the previous section, are conditioned by multiple ambiguities and must be balanced with the economic interests of the single market.

Notwithstanding these distinctions, they all aim to champion the prevailing imaginary of trustworthy SSPs. The universality of this imaginary was confirmed with the Bletchley Declaration on AI, signed by the EU, the US, the UK, China, and some Majority World countries (e.g., Kenya, Nigeria). They agreed to note the “potential for serious, even catastrophic, harm, either deliberate or unintentional, stemming from the most significant capabilities of these AI models”, and they were happy to claim that “context appropriate” safety testing is the route to achieving market and non-market governance goals (UK Government, 2023: 3).

The prevailing imaginary underpinning SSP governance is that system developer and owner as well as state interests can be aligned with progress that is (ultimately) consistent with human well-being and flourishing. This is informed by a specific imaginary about the efficiency and productivity gains arising from techniques of optimisation and, more generally, the benefits of these gains for society. Critical scholarship, in contrast, finds that these techniques are key to discriminations and surveillance that are at the heart of the calculative practices which are also central to the political economy of capitalism (McGuigan, 2023). In critical scholarship, it is acknowledged that the drive to achieve optimisation is a choice, not a given. It is a choice to reconstruct human behaviour in line with an “assimilation to a transcendent (‘virtual’) order of mathematical formalism” (Agre, 1994: 107). The imaginary of successful reconstruction sits at the heart of the broader SSP project. But if systems could “think rationally” about the “best” action, “the commonsense information possessed by humans would be written as logical sentences and included in the database” (McCarthy, 1987: 1032). This is the aspiration, and it presumes that all forms of knowledge and experience of the everyday lifeworld are calculable and replicable in the digital lifeworld (Noller, 2025). Critical scholarship points out that, in fact, SSPs in practice embody a “mix of institutionalized codes, professional cultures, technological capabilities, social practices, and individual decision making” (Ananny, 2016: 96). Nevertheless, the optimisation imaginary sustains a race to control calculative means, sometimes claiming in the computational sciences to operate in “a non-ideological environment”, eschewing normative or values-based judgements and, at other times, to operate in accord with social or political values, albeit within the parameters of computational models (Mansell, 2024). This imaginary is sustained by promoting epistemologies and methods with “vain pretensions [...] to understand mind as computation” (Winograd, 1990: 167).

The prevailing imaginary of SSP governance assumes that algorithms and LLMs can be assigned specific values and principles that they must adhere to in the expectation that a model will enact the norms of the constitution (Katzenbach, 2021). If it does not, guardrails can be deployed

to avoid outcomes that are harmful or discriminatory. This imaginary of technological “solutionism” recasts “all complex social situations either as neat problems with definite, computable solutions or as transparent and self-evident processes that can be easily optimized – if only the right algorithms are in place” (Morozov, 2013: 5). The political economy question is about where these objectives and values come from (Veale et al., 2023). They are certainly not simply informed by a scientific curiosity about whether “there are imaginable digital computers which would do well in the imitation game” (Turing, 1950: 442); they mainly come from the value preferences of companies and states with their contradictory interests in human rights, marketisation, and securitisation (Burton, 2023).

Investigations of the history of choices taken about technology innovation, markets, and governance are clear: “There is nothing automatic about new technologies bringing widespread prosperity. Whether they do or not is an economic, social and political choice” (Acemoglu & Johnson, 2023: 13), and it is typically the powerful elites that make those choices. Benefits undoubtedly accompany the deployment of SSPs when they contribute to market and organisational efficiency, to improved health diagnostics, or to environmental monitoring. But in the presence of power asymmetries, the biases and harms are rarely detected or reported until SSP developers and their owners are pressed to do so by regulators, the press, or whistle blowers – often after harms have occurred. This is despite efforts to prohibit certain tools and applications and to hold technology developers accountable through numerous voluntary and obligatory compliance requirements. The prevailing view is that the “mindset[s] of the government and people have not adjusted to view the future, even though technology is exploding” (Bill Gates, as cited in Preston, 2017: 101). This technocentric imaginary informs much governance discourse, making critical reflection on what the future holds very challenging because the “established order” is so deeply entrenched and,

what looks like a crisis to an outside observer does not become historically generative until participants in the society see it *as* a crisis [...] [and] they intuit that the pressing problems they experience arise not despite but precisely *because of* the established order and cannot be solved within it. (Fraser, 2022: 132)

How can an intuition that challenges the established order be broadly encouraged at the current juncture in the history of technologically inspired imaginaries?

A first move is to step back from the fixation on the latest SSP innovations, turning attention instead to the whole “data assemblage” (Kitchin & Lauriault, 2018) or to the stack of infrastructural components, including hardware and software and human input (van Dijck, 2020). This shift makes it easier to detect the dependence of SSP development on multiple power-infused

choices about relationships, legal and informal institutions, material objects, and ideas, all of which condition what systems are deployed to what ends under the varieties of capitalism operating around the world (Banet-Weiser, 2018; Griffin, 2023; Taylor et al., 2022). The SSP risk mitigation strategies are imbued with an imaginary future in which these technologies are to be “trusted throughout the world” (Paul, 2023: 1065). Power asymmetries and inequalities, “specifically differences in economic, social, and political status, and especially between different racial and ethnic groups” (Kreiss & McGregor, 2024: 558), are neglected as those in powerful positions use “trustworthy AI” to build “a chain of equivalences around an empty signifier” (Stamboliev & Christiaens, 2024: 44), which then underpins an imagined consensus around future SSP system development.

In this context, governance operates as “performative politics” (Bareis & Katzenbach, 2022), conjuring the prevailing imaginary at every turn. This makes it acceptable to downplay the fact that neither state officials nor designers or owners of SSP technology are in a position to calculate “the probability and adverse impact of AI systems on [...] fundamental rights with any numerical measures or clear indicators”; instead, they rely on the “rule of thumb” dressed up as rational decision-making (Paul, 2023: 1066). Thus, computational authority is privileged, and technologies are treated as a “thing” to be governed (Suchman, 2023: 1), while the outcomes are misaligned with aspirations for the protection of fundamental rights (Mejias & Couldry, 2024). In this context, it is not feasible to undertake the meaningful scrutiny of SSPs that would protect people from harm (Taylor et al., 2022).

A second move calls for an “analytics of power” (Deacon, 2002), including a close examination of how companies claim to be acting responsibly while they work to evade democratic oversight (Caplan, 2023; Obendiek, 2024). They do so partly by diffusing responsibility: “Everybody recognizes that no one tech company, no one government, no one civil society organization is able to deal with the advent of this technology and its possible nefarious use on their own” (Nick Clegg, as cited in O’Brien & Swenson, 2024: para. 3). The technology companies may sign voluntary frameworks, for example, to respond to deepfakes, or Meta may announce a policy promoting improved transparency of digitally manipulated content, but the SSP world continues to be characterised by “creepy inclusion”, and by technology developments inspired by the prevailing imaginary of trustworthy tools and services (Napoli, 2014; Pasquale, 2020). The reality is that these technologies are becoming “a more powerful force capable of perpetrating global violence” (Ricaurte, 2022: 726).

In this context, a rhetoric of objectivity, rationality, and certainty, combined with a governance discourse that is rife with ambiguity, leaves little room for an analytics of power. For this reason, a third move is agonistic resistance, which seeks change through public deliberation and novel practices better aligned with democratic outcomes (Laclau & Mouffe, 1985; Mouffe, 2013).

Governance requirements and fines for regulatory infringements, as well as continuing efforts to reach consensus about appropriate trade-offs among opposing market and human rights goals, can mitigate some harms. But resistance requires not privileging digital technology as a “sentient” actor and, instead, treating it as the embodiment of “propensities” (Latour, 2005). It requires creating conditions for imagining that the non-linearity of innovation can be a basis for radical change.

Hence, novel imaginaries for SSP governance arrangements are emerging through dozens of practices aimed at resisting the power of the Big Tech companies deploying SSPs in the market. Resistance strategies may be present on the individual level when people adopt self-defence practices to minimise the extraction of their data: they may take a collective form, such as initiatives by Indigenous communities and municipalities to set their own norms and guidelines for governing how data is collected and used; they may adopt commons-based approaches, which privilege democratic values and human rights over commerce and profit; and new practices are emerging around decentralised frameworks for data governance, especially in countries in the Global South, and there are increasing instances of litigation by civil society organisations arguing that people’s rights are being infringed (Mansell et al., 2025; Mejias & Couldry, 2024). Many of these initiatives are small-scale, but they illustrate that alternative imaginaries and practices are feasible. There is at least a potential for technological innovations in the digital landscape, and SSPs in particular, to follow norms and practices that are not shaped predominantly by corporate values and aspirations for profit.

Conclusion

Scepticism about the SSP-mediated future that is central to the prevailing imaginary is growing, even apart from those envisaging an existential threat to humanity. However, the predominant risk mitigation approaches discussed in this chapter remain products of a capitalist-inspired normative agenda (Manovich, 2020).

This chapter has highlighted the history of governance initiatives in the space where digital technology innovation has been fostered, demonstrating why struggles to uphold human rights in the face of technology marketisation must continue beyond the formality of state-led governance and implementation. These governance initiatives do not aim to reframe the technology innovation agenda in a way that departs from a fascination with optimisation and the notion that a more robust calculus of human behaviour in all its manifestations is the answer to human problems. Still, there is no basis for claiming that SSPs cannot be governed in line with a different imaginary to better align them with the interests of all. This is unlikely, however, if manifestations of SSP governance remain locked into the dominant imaginary and alternatives do not garner support.

In the light of the proliferation of corporate (and some state-owned) actors in the current “AI industry”, a political economy analysis points to the need for an ongoing and detailed investigation of corporate structure, ownership linkages, investment patterns, and strategies to detect ways to avert, and sometimes accommodate, the state-led governance arrangements that are put in place. It also, crucially, requires a deep analysis of the norms, ideas, and values espoused by relevant actors. This is essential to bring to light variations and to assess which calculative practices potentially can serve the purposes of those engaged in agonistic resistance strategies. In the critical tradition, there are calls for inclusive deliberative governance and for different ownership and common interest governance arrangements for SSP tools and applications. These aim to promote a different imaginary of how digital innovation might serve the interests of adults and children who currently experience the harms of corporate algorithmic assemblages and SSPs that might inspire fairer practices. Missing is the substantial investment needed to sustain resistance activities.

It is relatively easy to call for inclusive consultation that embraces diverse views, but advocacy of alternative imaginaries and practices must be cognisant of asymmetrical power relations inherent in “data-driven consultation practices” (Powell, 2024). Inclusion in “high level” governance deliberations about SSPs with a view to achieving consensus is important to ensure diverse voices are heard. However, it is not likely to bring about a major shift towards an alternative imaginary of an SSP-mediated future that is aligned more closely with human rights protection or with accountable democracy. Instead, agonistic strategies and practices, such as the diverse movements against centralised and corporate controlled SSPs, are needed that “motivate people to act, to imagine alternative political arrangements, and to contribute to long-term collective action” (Crooks & Currie, 2021: 201).

Finally, in the face of an imaginary where the assumption is that “trustworthy AI” – with all its ambiguities – is (or will be) consistent with justice, equality, and human flourishing, proponents of agonistic resistance must search for opportunities to shift towards alternative imaginaries and practices. These will be context-dependent, and they need to favour equity and justice over commercial success and an SSP market growth trajectory that outstrips planetary energy resources. This will mean explicit clashes between proponents of contending imaginaries and, potentially, clashes among elites and others.

A small move is to rename “AI systems” as SSPs, so as to disrupt a discourse that anthropomorphises these systems. In the absence of small steps such as this, the chances of resistance to the prevailing imaginary, its ideology, and its practices, are slim because inequities of the established order “cannot be solved within it” (Fraser, 2022: 132). Relying on state-initiated legislation – such as the EU’s AI Act, even if this and other legislative measures are enforced – leaves prevailing power asymmetries entrenched. Alternative imaginaries and practices of resistance conjured with the help of a different naming discourse are means

of countering prevailing power asymmetries. They also will require some form of mass mobilisation on a substantial scale (Chibber, 2025), if they are to scale up successfully and gain traction on an international scale.

Acknowledgements

I thank the editors of this volume for their comments on earlier drafts and especially Hannu Nieminen for his detailed and very helpful reading. Thanks also to two anonymous reviewers for their helpful reviews. Errors and omissions remain my own.

References

- Acemoglu, D., & Johnson, S. (2023). *Power and progress: Our thousand-year struggle over technology and prosperity*. Basic Books.
- Agre, P. E. (1994). Surveillance and capture: Two models of privacy. *The Information Society*, 10(2), 101–127. <https://doi.org/10.1080/01972243.1994.9960162>
- Ananny, M. (2016). Toward an ethics of algorithms: Convening, observation, probability, and timeliness. *Science, Technology & Human Values*, 41(1), 93–117. <https://doi.org/10.1177/0162243915606523>
- Banet-Weiser, S. (2018). *Empowered: Popular feminism and popular misogyny*. Duke University Press.
- Bareis, J., & Katzenbach, C. (2022). Talking AI into being: The narratives and imaginaries of national AI strategies and their performative politics. *Science, Technology, & Human Values*, 47(5), 855–881. <https://doi.org/10.1177/01622439211030007>
- Beckett, C., & Yaseen, M. (2023). *Generating change: A global survey of what news organisations are doing with AI*. Google News Initiative; LSE; Polis. <https://tinyurl.com/2ed5dy6r>
- Bengio, Y. (2023, September). AI and catastrophic risk. *Journal of Democracy*. <https://www.journalofdemocracy.org/ai-and-catastrophic-risk/>
- Bibao-Osorio, B., Dutta, S., & Lanvin, B. (Eds.). (2013). *The global information technology report 2013: Growth and jobs in a hyperconnected world*. INSEAD; World Economic Forum. https://www3.weforum.org/docs/GITR/2013/GITR_InsideCover_2013.pdf
- Borrás, S., & Edquist, C. (2019). *Holistic innovation policy: Theoretical foundations, policy problems, and instrument choices*. Oxford University Press. <https://doi.org/10.1093/oso/9780198809807.001.0001>
- Bradford, A. (2020). *Digital empires: The global battle to regulate technology*. Oxford University Press. <https://doi.org/10.1093/oso/9780197649268.001.0001>
- Bratton, B. H. (2015). *The stack: On software and sovereignty*. The MIT Press.
- Burton, J. (2023). Algorithmic extremism? The securitization of artificial intelligence (AI) and its impact on radicalism, polarization and political violence. *Technology in Society*, 75, 1–10. <https://doi.org/10.1016/j.techsoc.2023.102262>
- Caplan, R. (2023). Networked platform governance: The construction of the democratic platform. *International Journal of Communication*, 17, 3451–3472. <https://ijoc.org/index.php/ijoc/article/view/20035>
- Chibber, V. (2025). *The class constraints on social democracy*. Polity.
- Chokshi, C. N., & Mansell, R. (Eds.). (2026). *The need to rename tech*. Palgrave Macmillan. <https://doi.org/10.1007/978-3-032-05155-4>
- Council of Europe. (2024). *Council of Europe framework convention on artificial intelligence, and human rights, democracy and the rule of law*. <https://rm.coe.int/ai-convention-brochure/1680afaeba>
- Crawford, K. (2021). *The atlas of AI: Power, politics, and the planetary costs of artificial intelligence*. Yale University Press.
- Crooks, R., & Currie, M. (2021). Numbers will not save us: Agonistic data practices. *The Information Society*, 37(4), 201–213. <https://doi.org/10.1080/01972243.2021.1920081>

- Cusumano, M. A., Gawer, A., & Yoffie, D. B. (2021). Can self-regulation save digital platforms? *Industrial and Corporate Change*, 30(5), 1259–1285. <https://doi.org/10.1093/icc/dtab052>
- Deacon, R. (2002). An analytics of power relations: Foucault on the history of discipline. *History of the Human Sciences*, 15(1), 89–117. <https://doi.org/10.1177/0952695102015001074>
- Ene, D. (2025, March 13). Europe’s AI investment landscape: A deep-dive. *Seedblink*. <https://seedblink.com/blog/2025-03-13-europes-ai-investment-landscape-a-deep-dive>
- European Commission. (2020, March 11). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A new circular economy action plan for a cleaner and more competitive Europe*. <https://tinyurl.com/3bunwhux>
- European Commission. (2025, July 10). *The general-purpose AI code of practice*. <https://digital-strategy.ec.europa.eu/en/policies/contents-code-gpai>
- European Union. (2022a, October 12). *Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act)*. Official Journal of the European Union. <https://tinyurl.com/2j4b94p4>
- European Union. (2022b, October 27). *Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a single market for digital services and amending directive 2000/31/EC (Digital Services Act)*. Official Journal of the European Union. <https://tinyurl.com/3wurem8b>
- European Union. (2024, July 12). *Regulation (EU) 2024/1689 of the European Parliament and of the Council of June 13 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)*. <https://tinyurl.com/y74fu4un>
- Floridi, L., & Nobre, A. C. (2024). *Anthropomorphising machines and computerising minds: The crosswiring of languages between artificial intelligence and brain & cognitive sciences*. SSRN. <https://doi.org/10.2139/ssrn.4738331>
- Fraser, N. (2022). *Cannibal capitalism: How our system is devouring democracy, care, and the planet – And what we can do about it*. Verso.
- Frau-Meigs, D. (2024, March 15). On AI pedagogy [Conference presentation]. *Voice Festival, Florence, Italy*.
- Galdon-Clavell, G., Bertelli, V., Ozen, E. Y., & Lorente Martinez, T. (2023). *How public money is shaping the future direction of AI: An analysis of the EU’s investment in AI development* [Eticas report commissioned by the European AI & Society Fund]. Eticas. <https://tinyurl.com/3e4wa5te>
- Gerard, D. (2025, August 23). *AI winter is in the air! But we think the AI bubble keeps going until 2027*. Pivot to AI. <https://tinyurl.com/2tc9wawb>
- Gibson, E. D. (2024, September 17). The difficulty of AI monetization. *Medium*. <https://medium.com/@deconch30/the-difficulty-of-ai-monetization-3959e37d7840>
- Griffin, R. (2023). The law and political economy of online visibility: Market justice in the Digital Services Act. *Technology and Regulation*, 2023, 69–79. <https://doi.org/10.26116/techreg.2023.007>
- High-Level Expert Group on AI. (2019). *Ethics guidelines for trustworthy AI*. European Commission. <https://ec.europa.eu/futurium/en/ai-alliance-consultation.1.html>
- International Telecommunication Union. (2006). *E-strategies: Empowering development*. <https://tinyurl.com/5ff7ypxp>
- Katzenbach, C. (2021). “AI will fix this” – The technical, discursive, and political turn to AI in governing communication. *Big Data & Society*, 8(2), 1–8. <https://doi.org/10.1177/205395172111046182>
- Katzenbach, C., & Ulbricht, L. (2019). Algorithmic governance. *Internet Policy Review*, 8(4), 1–18. <https://doi.org/10.14763/2019.4.1424>
- Kitchin, R., & Lauriault, T. P. (2018). Toward critical data studies: Charting and unpacking data assemblages and their work. In J. Thatcher, J. Eckert, & A. Shears (Eds.), *Thinking big data in geography: New regimes, new research* (pp. 3–20). University of Nebraska Press.
- Kreiss, D., & McGregor, S. C. (2024). A review and provocation: On polarization and platforms. *New Media & Society*, 26(1), 556–579. <https://doi.org/10.1177/14614448231161880>

- Laclau, E., & Mouffe, C. (1985). *Hegemony and socialist strategy: Towards a radical democratic politics*. Verso.
- Latour, B. (2005). *Reassembling the social: An introduction to actor-network-theory*. Oxford University Press. <https://doi.org/10.1093/oso/9780199256044.001.0001>
- Liesenfeld, A., & Dingemans, M. (2024). Rethinking open source generative AI: Open-washing and the EU AI Act. *FACCT'24: Proceedings of the 2024 ACM Conference on Fairness, Accountability and Transparency* (pp. 1774–1787). Association of Computing Machinery.
- Manovich, L. (2020). *Cultural analytics*. The MIT Press. <https://doi.org/10.7551/mitpress/11214.001.0001>
- Mansell, R. (2023). Digital technology innovation: Mythical claims about regulatory efficacy. *Javnost - The Public*, 30(2), 145–160. <https://doi.org/10.1080/13183222.2023.2198933>
- Mansell, R. (2024). Global communications governance research: Colliding epistemologies and methodologies. In C. Padovani, V. Wavre, A. Hintz, G. Goggin, & P. Iosifidis (Eds.), *Global communication governance at the crossroads* (pp. 353–369). Palgrave Macmillan. https://doi.org/10.1007/978-3-031-29616-1_20
- Mansell, R. (2025). A capitalist contest: The AI industry v. the creative industries. *Journal of the British Academy*, 13(3), 1–19. <https://doi.org/10.5871/jba/013.a38>
- Mansell, R., Durarch, F., Kettemann, M., Lenoir, T., Procter, R., Tripathi, G., & Tucker, E. (2025). *Information ecosystems and troubled democracy: The state of knowledge on news media, AI and data governance*. Nordicom, University of Gothenburg. <https://doi.org/10.48335/9789189864238>
- Maslej, N., Fattorini, L., Brynjolfsson, E., Etchemendy, J., Ligett, K., Lyons, T., Manyika, J., Ngo, H., Niebles, J. C., Parli, V., Shoham, Y., Wald, R., Clark, J., & Perrault, R. (2023). *AI index 2023*. Stanford University Human-Centered Artificial Intelligence. https://aiindex.stanford.edu/wp-content/uploads/2023/04/HAI_AI-Index-Report_2023.pdf
- McCarthy, J. (1987). Generality in artificial intelligence. *Communications of the ACM*, 30(12), 1030–1035. <https://doi.org/10.1145/33447.33448>
- McGuigan, L. (2023). *Selling the American people: Advertising, optimization, and the origins of Adtech*. The MIT Press. <https://doi.org/10.7551/mitpress/13562.001.0001>
- Mejias, U. A., & Couldry, N. (2024). *Data grab: The new colonialism of big tech and how to fight back*. University of Chicago Press.
- Mishcon de Reya. (2024, October 8). *Generative AI – IP cases and policy tracker*. <https://www.mishcon.com/generative-ai-intellectual-property-cases-and-policy-tracker>
- Morozov, E. (2013). *To save everything, click here: Technology, solutionism, and the urge to fix problems that don't exist*. Penguin House.
- Mouffe, C. (2013). *Agonistics: Thinking the world politically*. Verso.
- Napoli, P. (2014). Automated media: An institutional theory perspective on algorithmic media production and consumption. *Communication Theory*, 24(3), 340–360. <https://doi.org/10.1111/comt.12039>
- Natale, S., & Ballatore, A. (2020). Imagining the thinking machine: Technological myths and the rise of artificial intelligence. *Convergence: The International Journal of Research into New Media Technologies*, 26(1), 3–18. <https://doi.org/10.1177/1354856517715164>
- National Institute of Standards and Technology. (2023). *Artificial intelligence risk management framework (AIRMF1.0)*. <https://doi.org/10.6028/NIST.AI.100-1>
- National Science and Technology Council. (2016). *Preparing for the future of artificial intelligence*. Executive Office of the President of the United States.
- Noller, J. (2025). Connectionism about human agency: Responsible AI and the social lifeworld. *AI & Society*, 40(5), 3881–3890. <https://doi.org/10.1007/s00146-024-02133-5>
- Nowotny, H. (2021). *In AI we trust: Power, illusion and control of predictive algorithms*. Polity Press.
- Obendiek, A. S. (2024). The politics of tech responsibility: Understanding companies' responsibility as representative claims. *New Media & Society*, 27(6), 3680–3698. <https://doi.org/10.1177/14614448241229406>
- O'Brien, M., & Swenson, A. (2024, February 16). *Tech giants sign voluntary accord to combat election deepfakes generated with AI*. PBS NewsHour. <https://tinyurl.com/2n598hzw>

- OECD (Organisation for Economic Co-operation and Development). (2023). *Recommendation of the Council on artificial intelligence*.
<https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449%20>
- Our World in Data. (2025). *Annual private investment in artificial intelligence*.
<https://ourworldindata.org/grapher/private-investment-in-artificial-intelligence>
- Pasquale, F. (2020). *New laws of robotics: Defending human expertise in the age of AI*. Belknap Press.
- Paul, R. (2023). European artificial intelligence “trusted throughout the world”: Risk-based regulation and the fashioning of a competitive common AI market. *Regulation & Governance*, 18(4), 1065–1082. <https://doi.org/10.1111/rego.12563>
- Powell, A. B. (2024). Objectivity vs affect: How competing forms of legitimacy can polarize public debate in data-driven public consultation. *Information, Communication & Society*, 28(9), 1523–1540. <https://doi.org/10.1080/1369118X.2024.2329623>
- Preston, A. (2017). What can Tesla Autopilot teach us about business process automation? *European Business Magazine Summer Edition*, 27, 96–106.
https://issuu.com/europeanbusinessmagazine/docs/27_european_business_magazine_summe
- Puppis, M., Mansell, R., & Van den Bulck, H. (2024). Introduction to media and communication governance: From labelling to theorizing and practice. In M. Puppis, R. Mansell, & H. Van den Bulck (Eds.), *Handbook of media and communication governance* (pp. 1–26). Edward Elgar. <https://doi.org/10.4337/9781800887206.00008>
- Ricaurte, P. (2022). Ethics for the majority world: AI and the question of violence at scale. *Media, Culture & Society*, 44(4), 726–745. <https://doi.org/10.1177/01634437221099612>
- Santucci, G. (2011, February 11). The internet of things: A window to our future. *Wired*.
<https://www.wired.com/2011/02/spime-watch-the-internet-of-things-a-window-to-our-future/>
- Sastry, G., Heim, L., Hazell, J., O’Keefe, C., Hadfield, G. K., Ngo, R., Pilz, K., Gor, G., Bluemke, E., Shoker, S., Egan, J., Trager, R. E., Avin, S., Weller, A., Bengio, Y., & Coyle, D. (2024). *Computing power and the governance of artificial intelligence*. Cambridge University; CSER - Centre for Study of Existential Risk.
<https://www.cser.ac.uk/media/uploads/files/Computing-Power-and-the-Governance-of-AI.pdf>
- Schaeffer, R., Miranda, B., & Koyejo, S. (2023). Are emergent abilities of large language models a mirage? *arXiv*. <https://doi.org/10.48550/arXiv.2304.15004>
- Schumpeter, J. A. (1942). *Capitalism, socialism and democracy*. Harper & Row.
- Scott, M. (2024, February 15). ‘Trust us on AI,’ says the military. Politico.
<https://www.politico.eu/newsletter/digital-bridge/trust-us-on-ai-says-the-military/>
- Select Committee on Artificial Intelligence of the National Science and Technology Council. (2023). *National artificial intelligence research and development strategic plan 2023 update*.
<https://tinyurl.com/4zxtxn94>
- Simon, F. M. (2022). Uneasy bedfellows: AI in the news, platform companies and the issue of journalistic autonomy. *Digital Journalism*, 10(10), 1832–1854.
<https://doi.org/10.1080/21670811.2022.2063150>
- Stamboliev, E., & Christiaens, T. (2024). How empty is trustworthy AI? A discourse analysis of the ethics guidelines of trustworthy AI. *Critical Policy Studies*, 19(1), 39–56.
<https://doi.org/10.1080/19460171.2024.2315431>
- Suchman, L. (2023). The uncontroversial ‘thingness’ of AI. *Big Data & Society*, 10(2), 1–5.
<https://doi.org/10.1177/20539517231206794>
- Sookman, B. (2024, January 3). *Resolving GenAI copyright infringement questions: 4 court decisions*. Barry Sookman. <https://tinyurl.com/mwd5shkn>
- Taylor, L., Mukiri-Smith, H., Petročnik, T., Savolainen, L., & Martin, A. (2022). (Re)making data markets: An exploration of the regulatory challenges. *Law, Innovation and Technology*, 14(2), 355–394. <https://doi.org/10.1080/17579961.2022.2113671>
- Tech Hive Advisory Center for Law & Innovation. (2024). *State of AI regulation in Africa: Trends and developments report*. <https://tinyurl.com/2kfb7kn>
- Temple-West, P., & Kinder, T. (2024, March 24). Thiel, Bezos and Zuckerberg join parade of insiders selling tech stocks. *The Financial Times*. <https://tinyurl.com/mr6jsscv>

- The White House. (2023, March 27). *Prohibition on use by the United States government of commercial spyware that poses risks to national security*. <https://tinyurl.com/rk3nsyym>
- The White House. (2025a, January 23). *Removing barriers to American leadership in artificial intelligence*. <https://tinyurl.com/bdrnyshb>
- The White House. (2025b, July). *Winning the race: America's AI action plan*. <https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf>
- Turing, A. M. (1950). Computing machinery and intelligence: Can machines think? *Mind*, LIX(236), 433–460. <https://doi.org/10.1093/mind/LIX.236.433>
- UK Government. (2023, February 13). *The Bletchley declaration by countries attending the AI Safety Summit, 1-2 November 2023*. <https://tinyurl.com/bdh7brfh>
- United Nations. (2020). *Report of the Secretary-General: Roadmap for digital cooperation*. <https://tinyurl.com/bdz4r7pu>
- United Nations. (2024a). *Pact for the future, global digital compact, and declaration on future generations*. https://www.un.org/sites/un2.un.org/files/soft-pact_for_the_future_adopted.pdf
- United Nations. (2024b). *Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development*. https://digitallibrary.un.org/record/4043244/files/A_RES_78_265-EN.pdf?ln=en
- United Nations AI Advisory Board. (2023). *Governing AI for humanity*. https://www.un.org/sites/un2.un.org/files/ai_advisory_body_interim_report.pdf
- United Nations Conference on Trade and Development. (2005). *Information economy report 2005*. https://unctad.org/system/files/official-document/sdteecd20051_en.pdf
- van Dijck, J. (2020). Seeing the forest for the trees: Visualizing platformization and its governance. *New Media & Society*, 23(9), 2801–2819. <https://doi.org/10.1177/1461444820940293>
- Van Woensel, L., Kurrer, C., & Kritikos, M. (2016). *Ethical aspects of cyber-physical systems: Scientific foresight study*. European Parliament; Science and Technology Options Assessment. <https://tinyurl.com/4fd32vjp>
- Veale, M., Matus, K., & Gorwa, R. (2023). AI and global governance: Modalities, rationales, tensions. *Annual Review of Law and Social Science*, 19, 255–275. <https://doi.org/10.1146/annurev-lawsocsci-020223-040749>
- Wang, J., Milne, C., Hu, J. Z., & Khan, F. (2024). *Navigating geopolitics in AI governance*. Oxford Global Society. <https://tinyurl.com/585pt87u>
- Winograd, T. (1990). Thinking machines: Can there be? Are we? In the foundations of artificial intelligence. In D. Partridge, & Y. Wilks (Eds.), *The foundations of artificial intelligence* (pp. 167–189). Cambridge University Press.
- Winseck, D. (2024). The political economies of communication, ‘big tech’ and cultural industries from the ‘industrial age’ to the ‘internet era’. In M. Puppis, R. Mansell, & H. Van den Bulck (Eds.), *Handbook of media and communication governance* (pp. 73–87). Edward Elgar.
- World Economic Forum. (2024). *Global risks report 2024*. <https://www.weforum.org/publications/global-risks-report-2024/>
- World Economic Forum. (2025). *Global risks report 2025*. <https://www.weforum.org/publications/global-risks-report-2025/>
- Zaharia, A., & Bischoff, P (2024, November 8). *300+ terrifying cybercrime and cybersecurity statistics*. Comparitech. <https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/>
- Zitron, E. (2025, April 14). OpenAI is a systemic risk to the tech industry. *Where's your Ed at?* <https://www.wheresyoured.at/openai-is-a-systemic-risk-to-the-tech-industry-2/>
- Zuboff, S. (2022). Surveillance capitalism or democracy? The death match of institutional orders and the politics of knowledge in our information civilization. *Organization Theory*, 3(3), 1–79. <https://doi.org/10.1177/26317877221129290>