Centre for International
Governance Innovation

CIGI Paper No. 345 — December 2025

Platform Governance and the Political Economy of Global AI Regulation

Sabhanaz Rashid Diya

Centre for International
Governance Innovation

CIGI Paper No. 345 — December 2025

Platform Governance and the Political Economy of Global AI Regulation

Sabhanaz Rashid Diya

About CIGI

The Centre for International Governance Innovation (CIGI) is an independent, non-partisan think tank whose peer-reviewed research and trusted analysis influence policy makers to innovate. Our global network of multidisciplinary researchers and strategic partnerships provide policy solutions for the digital era with one goal: to improve people's lives everywhere. Headquartered in Waterloo, Canada, CIGI has received support from the Government of Canada, the Government of Ontario and founder Jim Balsillie.

À propos du CIGI

Le Centre pour l'innovation dans la gouvernance internationale (CIGI) est un groupe de réflexion indépendant et non partisan dont les recherches évaluées par des pairs et les analyses fiables incitent les décideurs à innover. Grâce à son réseau mondial de chercheurs pluridisciplinaires et de partenariats stratégiques, le CIGI offre des solutions politiques adaptées à l'ère numérique dans le seul but d'améliorer la vie des gens du monde entier. Le CIGI, dont le siège se trouve à Waterloo, au Canada, bénéficie du soutien du gouvernement du Canada, du gouvernement de l'Ontario et de son fondateur, Jim Balsillie.

Credits

Research Director, Transformative Technologies Tracey Forrest
Director, Programs Dianna English
Program Manager Grace Wright
Publications Editor Christine Robertson
Manager, Publications Jennifer Goyder
Graphic Designer Sepideh Shomali

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org

Table of Contents

vi About the Author

1 Executive Summary

1 Introduction

4 Accountability Grounded in Pluralistic Risk Assessments

6 Rights as a Multi-Levelled Framework

7 Governance Through Existing Policy Instruments

8 Global Majority as Norm-Shapers

10 Policy Recommendations

11 Works Cited

About the Author

Sabhanaz Rashid Diya is a CIGI senior fellow and the founder of Tech Global Institute, a global tech policy think tank focused on reducing equity and accountability gaps between technology companies and the global majority. She has advised governments in 20 countries, including leading closed-door briefings with the White House, the US Department of State and the Office of the United States Trade Representative, multilateral international organizations such as the World Bank and the United Nations, bilateral donors, and a variety of global startups and corporations, on policy and law questions related to global internet and platform governance, responsible artificial intelligence (AI) and human rights.

A computational social scientist by training, Sabhanaz has more than 17 years of experience at the intersection of technology policy, ethics and international development. She was most recently the head of public policy for Bangladesh at Meta, where she engaged policy makers and led on various regulatory and legislative issues, including hate speech, privacy, data protection and the data economy, online harms and algorithmic transparency. Sabhanaz also worked at the Bill & Melinda Gates Foundation, leading policy and advocacy efforts in multidisciplinary digital identity and economy, data and AI. Her career spans the private and public sectors in the United States, Asia and Africa, including work with the United States Agency for International Development and the World Bank, on encryption policy, digital trade, AI applications in the global majority and internet governance. She is the founding board director for the US-Bangladesh Business Council at the US Chamber of Commerce.

Sabhanaz holds a master's degree in public policy from the University of California, Berkeley. She is an Asia 21 leader at the Asia Society and a corporate leader at the Council on Foreign Relations. Her interviews and writing have appeared in the *Financial Times, Wired,* Thomson Reuters Foundation, BBC News, France 24, Global Voices, *The Straits Times, The Daily Star, Dhaka Tribune* and *The Business Standard.*

Executive Summary

The rapid development of artificial intelligence (AI) presents both opportunities and challenges for global governance. While there is a growing body of research on AI governance, relatively little has emerged that delves into what lessons AI governance can adopt from well-documented policy work on other existing and emerging technologies. AI governance debates grappling with ethical considerations, human rights and equitable distribution of benefits are not *sui generis;* many of these same concerns on policy, politics and ethics have been debated in other technology fields (Ulnicane et al. 2021). Existing social science literature not only provides critical insights into governance as a discipline, but also explores policy frameworks in areas such as biomedical ethics, computing, intercultural digital ethics, communication and internet network infrastructure.

Over the past decade, online intermediary — specifically social media — governance has presented diverse perspectives into managing complex, rapidly evolving technologies. These debates have underscored the need for accountability, inclusivity and a rights-based approach from the outset to balance innovation with effective oversight. As AI increasingly intersects with social media intermediaries through direct and indirect overlaps in technical design and corporate ownership, examining the similarities and dissimilarities between their governance approaches become essential. Moreover, many social media platforms have either evolved into major AI companies themselves or deeply embedded AI into their design and operations, blurring the boundaries between platform and AI governance and making their oversight increasingly interdependent.

To explore this convergence and divergence, the Centre for International Governance Innovation (CIGI) convened a virtual workshop last year, bringing together global experts across policy, media, academia and civil society. Through this discussion, the workshop aimed to inform current and future discourse on global AI governance, identifying best practices and regulatory gaps. When analyzed through frameworks such as digital imperialism and colonialism, it becomes evident how technological infrastructures, data governance and internet regulations are disproportionately shaped by a handful of companies and states from the Global North, making them "norm-shapers" and everyone else "norm-takers." This paper builds on key takeaways from the discussion on the intertwined nature of platform and AI governance with an emphasis on the need to introduce a multilevel rights framework, unpack inequalities in the global AI supply chain and address the lack of regulatory capacity in the Global Majority, as well as the challenges of being norm-takers in the global system.

Introduction

The early 2000s signalled a pivotal shift to web 2.0 applications, where "the user" evolved from a passive consumer to a participant of the internet (Obar and Wildman 2015). Some scholars argued that the new "user" is both a consumer and producer of information (Ritzer and Jurgenson 2010) with "user-generated content" fuelling the new era of "interactive internet" (Obar and Wildman 2015).

Web 2.0 was defined in large part by the rapid rise of social media intermediaries, such as Facebook and Twitter. However, digital interactions enabled through user-generated content encompassed a wider range of online intermediaries, including search engines, marketplaces, ridesharing and app platforms. This diversity presents the first major policy challenge: defining what constitutes an "intermediary" or even a "social media intermediary." While recent academic and policy discourse has coalesced around the term "platform" to capture the distinct dynamics of user-to-user interaction on social media intermediaries and its governance, earlier debates revealed a range of competing definitions (Helmond and van der Vlist 2019; González-Tosat and Sádaba-Chalezquer 2021). Some scholars define social media intermediaries as web 2.0 applications that allow for user-generated content (Kaplan and Haenlein 2010). Others argue that their role is to facilitate interactive information exchange among groups of recipients (Hogan and Quan-Haase 2010). The lack of consensus on definitions has led to the governance of social media intermediaries being fragmented and domain specific. Furthermore, it raises questions on how existing and distinctive

concepts — such as intellectual property (IP), privacy, competition and speech — should be regulated within a complex technological architecture that touches on all aspects of national statutory mechanisms and international legal instruments (DeNardis and Hackl 2015).

A review of legislative and regulatory case studies from 2015 highlights significant variation in the legal definition of "social media intermediaries" (Gasser and Schulz 2015). Unlike the approach to broadcasting or telecommunication laws, policy makers tend to avoid forming strict criteria for what constitutes a social media intermediary, or social media platform, and struggle to clearly define their functions and responsibilities. Platforms operate fluidly and evolve rapidly by blending the roles of host, publisher, infrastructure and marketplace, making it difficult to classify them under a single legal or regulatory category. Moreover, they employ their allies and users, in addition to seasoned political lobbyists, to influence policy through grassroots campaigns, coalition building and acting as political entrepreneurs across multiple governance levels (Yates 2023). This allows platforms to exploit institutional gaps and frame themselves as champions of innovation, making it challenging for regulators to impose coherent oversight or hold them liable.

In the United States, section 230 of the Communications Decency Act and section 512 of the Digital Millennium Copyright Act established explicit liability regimes for online intermediaries, granting them "safe harbour" — conditional protection from liability for user-generated content (Lagg 2018). In Brazil, the Marco Civil da Internet provides similar immunity to online intermediaries for user-generated content with the notable exception of a derogatory notice-and-takedown regime for revenge porn (Souza, Viola and Lemos 2015). However, Brazilian courts have a long tradition of interpreting the intermediary liability regime, adding complexity to its enforcement. India also includes safe harbour protections under sections 71 and 89 of the Information Telecommunication Act, but the Information Telecommunication Rules of 2011 introduced a detailed notice-and-takedown regime. In 2021, these rules were further expanded to regulate social media platforms, over-the-top platforms and digital media (Gupta and Srinivasan 2023). Similar to Brazil, Indian courts have played an outsized role in interpreting the intermediary liability regime in the past two decades, resulting in significant challenges to its enforcement and operational predictability for platforms.

The second major policy challenge arises from privatized governance, wherein platforms are shaping governance through their technical design and user policies. This represents governance *by* intermediaries rather than governance *of* intermediaries (DeNardis and Hackl 2015), and raises critical questions about the political ecology of platforms. By positioning themselves as "platforms," social media intermediaries frame their technologies and services as neutral facilitators of information exchange. This discursive meaning suggests a progressive and egalitarian arrangement to support their users, while in reality, these platforms enjoy a privileged legal position — benefiting from legislative protections while sidestepping obligations that otherwise apply (Gillespie 2010).

For example, Google has long been vocal about net neutrality (Slater 2008) and free expression, while simultaneously positioning itself as a marketing tool for advertisers and commercial media producers. Google's business model determines what content it hosts, how it is organized and who can participate with distinct technical features meant to serve advertisers (van Dijck 2009). Data is a by-product of the information exchange between users, and platforms act as third-party observers, extracting and monetizing observational data from user-generated content (Zuboff 2023). This creates a vested interest in shaping technical design and affording communication that maximizes data extraction for profit (ibid.), therefore undermining the notion of neutral arbiters or "platforms" for information exchange. In 2020, 80 percent of Google's US$183 billion in revenue came from its targeted advertising programs.[1]

Shaping governance through technical design highlights the role of platform governance within the broader framework of internet governance. Platforms rely on identity infrastructure, metadata aggregation and network connectivity, making their operating model integral to the free flow of the information (DeNardis and Hackl 2015). This raises a third major policy challenge: technological infrastructure reflects political power structures and can directly impact civil liberties by infringing

1 See Alphabet Inc. (2020).

upon the free flow of information that is integral to the interoperability of the internet. For instance, many repressive regimes often control network infrastructure to restrict communication or cross-border data transfers, effectively using infrastructure as a tool for censorship.

Further, internet governance is underpinned in interoperability, universality and generativity (Zittrain 2009). However, when a handful of large platforms filter information through technical specifications and user policies, they constrain users' ability to exchange information freely, exerting significant power over how information is accessed and consumed. This privatization of information exchange results in private control of civil liberties such as free expression, access to information and individual privacy (DeNardis and Hackl 2015). Additionally, the lack of open technical standards underlying platform design and governance, combined with limited data portability, weakens interoperability of the internet.

Notably, these aforementioned policy challenges are not unique to social media platforms and have resurfaced with growing public discourse around AI governance. What constitutes AI? In the broadest sense, an AI system[2] 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. Different AI systems vary in their levels of autonomy and adaptiveness after deployment (Organisation for Economic Co-operation and Development 2024). The European Commission's High-Level Expert Group on Artificial Intelligence defines AI as "[autonomous] systems that analyze their surroundings and act to reach specific objectives, exhibiting intelligent behavior" (Carrillo 2020). The anthropomorphization of AI has led to conflating ideas about AI and robotics (Watson 2019). Claims that AI resembles human cognition warrants skepticism; in reality, these models offer a different form of inference, excelling in some areas while falling short in others. The absence of academic consensus on AI's definition has resulted in a lack of policy alignment on its governance (Birkstedt et al. 2023).

Despite these past deficits, there is an increasingly growing alignment among policy makers about what constitutes an AI system — a welcome change from the contested definitional evolution of platforms. However, there remain gaps between how to operationalize a theoretical definition and the operationalization of its oversight. There is often confusion between ethical and legal aspects of AI governance (Carrillo 2020). Philosophically, historically, geographically or materially, there are no universal or homogenous sets of ethics, although some principles, such as transparency and fairness, are common across policy documents. Despite this fragmentation, there is widespread agreement to "implement" ethics in AI design that some scholars argue is the new industry self-regulation or "soft power" (Wagner 2018; Diya 2025). Contrarily, legal norms are common, mandatory and uniform. They can be applied within or between nation-states with some degree of predictability, but are constrained by how clearly the different AI typologies can be explained (Carrillo 2020). The cause and grounds for wrongful — or unlawful — acts can vary not just between typologies, but also between the political systems in which they operate.

There is a growing trend toward automating decision making in public and private services using the latest powerful AI system that raises concerns about privatization of governance (Rookard 2024). By their nature, private actors and automated decision making flatten complex policy deliberations, prioritize efficiency over public interest and entrench existing power and colonial structures. Privatization prompts critical questions about the future of state and administration, and whose perspectives matter as more of the state's authority is devolved into the hands of private actors and automated systems (ibid.).

These parallels between the political and policy ecologies of platforms and AI systems set the stage for the virtual workshop. Expert participants observed that rhetoric around ambiguities in technical design and business models, once central to platform governance, are resurfacing in AI governance. Similar to how social media intermediaries were framed as neutral platforms (Gillespie 2010), the AI private sector employs discursive verbiage to mask the ambiguity and opacity of its own systems, highlighting how the models are complex and composed of millions of micro-decisions that are extremely difficult to trace and therefore would make it impossible to regulate. However, AI systems are not inherently

2 See Organisation for Economic Co-operation and Development (2024).

opaque — they are the products of deliberate choices that involve human decision making that determines design choices, data selection and model training. One expert on the public sector use of AI noted that "AI isn't just a sum of upstream components — data, compute, logic and talent. AI should be treated as how each of these components interact with each other, and the connection of existing components with new forms of compute." Most policy conversation to date, however, has narrowly focused on the application and models, but ignored the "AI stack." This provides a different starting point for addressing market concentration, vertical integration and power asymmetries. As such, experts argue that AI systems fall under the same legal instruments as any other technology.

This paper will explore key discussion points from the workshop, organized into four sections, including policy options and pitfalls. Each section expands on key lessons learned from social media governance, as identified by expert participants, and how these insights can meaningfully inform AI governance — particularly in addressing existing power inequities and policy fragmentation.

Accountability Grounded in Pluralistic Risk Assessments

Platform governance has underscored the importance of pluralistic risk assessments for emerging technologies such as AI. Any accountability instrument needs to address the *impact* of AI and algorithmic decision-making systems, and the impact varies across target groups: individuals, communities and states. The European Union's AI Act (AIA), for example, includes a risk-based regulatory framework; however, it takes a static view of risks that focuses on technological features and broad-use cases. It does not consider the interactions between the source of risks, vulnerability profiles, severity of consequences and exposed values (Novelli et al. 2024). Moreover, it does not address proportionality — how different communities experience risks and harms differently — and the uncertainty in reviewing risk categorization (Smuha et al. 2021).

Although the AIA is underpinned by European fundamental rights, the operationalization model does not reflect on the comparability and proportionality of the weight of risks across different groups and contexts. Some scholars argue that by assigning fixed risk levels (unacceptable, high risk, medium risk and minimal risk) to AI systems based on their *intended* purpose, the AIA fails to evaluate the interactions between various factors. Instead, a dynamic risk classification model would allow the same AI system to be assessed as unacceptable, high risk, medium risk or minimal risk depending on how it is applied in the real world, who the intended audiences are and the impact on their fundamental rights (Novelli et al. 2024).

An expert on human rights highlighted that legislation such as the AIA needs to further consider the business models driving AI development. Many of the leading AI unicorns, similar to social media intermediaries, are built around data extraction as a core business model. Current regulatory and policy frameworks differentiate AI and their risks based on the size of the business — revenue and users. This approach fails to address a deeper issue: the development of an entire industry based on extractive, rights-violating business models. This industry extracts value through behavioural surveillance, personalized advertising, content ownership and psychological manipulation. They "personalize" realities and experiences, altering users' perception of truth and reinforcing behavioural conditioning (Zuboff 2023). Privacy and consumer rights are typically primary laws; however, the scale of surveillance raises concerns about consumer autonomy not only at the application layer, but also in AI design and development phases. Therefore, policy makers need to reorient their thinking to upstream components of AI systems such as data and compute that allow them to evaluate valuation and market capitalization and curb start-ups with a harmful business model early on.

Participants at the workshop suggested an alternate model for risk assessments. AI system risks can be categorized as *gray rhinos* (evident and high impact), *black swans* (rare but significant) and frontier risks (unknown and unpredictable). While grey rhinos and black swans represent opposite ends of the risk spectrum, frontier risks surface as technologies significantly shift human or societal forces. Identifying and addressing

frontier risks require a wide range of interventions, from horizon scanning and scenario planning to working with reorganizing organizational and regulatory structures (Effoduh 2023).

Identifying frontier risks, rather than frontier AI that can become central to many policy discourses, will afford an AI governance approach that is comprehensive, tiered and pragmatic rather than predictive and unenforceable. It takes the rapid pace of AI development and deployment into account and assesses their differential impact on marginalized and vulnerable communities. The unchecked use of AI algorithms in social media intermediaries should fall within this framework and interrogate how algorithmic decision making and filtering has facilitated information manipulation and polarization.

Drawing on parallels between platforms and AI models, a national security expert at the workshop highlighted five well-documented and multi-faceted areas of technology-mediated risks to national security and geopolitics: data privacy, critical infrastructure, psychological manipulation, criminal coordination and espionage. These risks will be exacerbated as AI systems advance without restrictions or safeguards. The 2019 Cambridge Analytica data breach exposed the dangers of personal data being harvested and marketed without explicit consent to manipulate political outcomes. As more data is collected, psychological manipulation is exacerbated, as well as the risks of democratic backsliding through the diffusion of propaganda and influence operations.

Another significant risk is the vulnerabilities of digital and critical infrastructures. Exploitation of digital codes, especially those deployed in the public sector, can lead to cyberattacks, data breaches and system manipulation that impacts entire populations. In 2015, Russian cyberattackers launched a coordinated attack on Ukraine's power grid, causing widespread power outages that affected more than 200,000 people. The attackers were believed to be part of Russia's military intelligence and infiltrated the grid through phishing emails and malware, exploiting vulnerabilities in the system's network management software (Whitehead et al. 2017).

Moreover, criminal actors and networks routinely exploit the anonymity offered by information intermediaries to globally coordinate illegal activities such as drug trafficking, human trafficking and terrorism. Between 2022 and 2023, the Asia-Pacific region experienced a 1,530 percent increase in deepfake fraud (Dickson and Preputnik 2024). According to the UN Office of Drugs and Crime,[3] there is a growing use of deepfake technologies by scammers to implement social engineering scams and severely harm users.

States are increasingly adding cyber espionage to their national security strategies — both as an offensive and defensive tactic. In most cases, third-party cyber spies are responsible for triggering national cyberattacks, for example, in Kyrgyzstan (2005) and Belarus (2006). However, a 10-month investigation by researchers at Information Warfare Monitor exposed alleged Chinese spying against Tibetan institutions (Deibert et al. 2009). In 2014, the US Department of Justice unsealed an indictment[4] involving seven Chinese nationals — allegedly part of a hacking group backed by the People's Republic of China — for a 14-year-long cyber espionage campaign targeting US and foreign critics, businesses and officials.

Given the vast spectrum of risks, it is imperative that risk evaluations centre on who is impacted and at what stage of the AI stack or product cycle. Based on these questions, AI risks can be tied to three categories of harm: individual, collective and societal (Smuha 2021a). Individualized harm can occur through the use of biased facial recognition technologies in law enforcement that can result in discrimination against a person of colour. Although the harm is shaped by collective and political contexts, measurable harm can be narrowed down to individual impact. Collective harm arises when a group of individuals are *collectively* wronged, for example, systemic discrimination through biased AI job applications against entire groups of women of colour, or AI used in immigration applications that discriminate against low-income or highly vulnerable groups from Global Majority regions (Martín del Río 2024).

Societal harm extends beyond individuals or specific groups to impact society as a whole. It involves the erosion of broader societal values, such as trust in institutions or democracy. Unlike collective harm, societal harm transcends individual experiences, affecting entire social fabrics, rather than

3 See United Nations Office on Drugs and Crime (2024).

4 See US Department of Justice (2024).

target AI-facilitated discrimination or harm. One expert on human rights highlighted that AI risk assessments need to expand to include "society-in-the-loop" — especially for high-risk models or systems — so it embeds a moral choice within the evaluation process.

Rights as a Multi-Levelled Framework

There has been long-standing debate on a human rights-centred approach to AI governance; the AIA explicitly states its objective to safeguard fundamental rights in the European Union.[5] Some scholars have criticized the European or American imagination of human rights for being rooted in Western values, viewed as a tool of cultural imperialism rather than a reflection of global pluralism (Talbott 2007). This view can be challenged by noting the participation of non-Western nations in drafting the Universal Declaration of Human Rights, the diplomatic nature of human rights agreements and the global similarities in regional human rights instruments (Huber 2014). Others argue that prioritizing individualism in human rights privileges one category of rights over another, and comes at the expense of collective benefits, for example in health care, where protecting personal medical data might hinder AI-driven advancements in disease detection (Taddeo 2016). Similar conflicts arise in environmental protection. This raises concerns about whether human rights, with their strong individualistic focus, are sufficient to address broader communal and ecological challenges (Smuha 2021a).

These arguments overlook how individual freedoms interact with social contracts and toward societal benefits. In fact, social citizenship is a prominent concept in European countries — individual freedoms based on civil and political rights with a "social-sharing" component (Ferrera, Corti and Keune 2024). The European Union's role in social rights can be understood through three layers of intervention. The first layer consists of EU social rights established through hard law, forming a legal framework that protects citizens against risks and needs. The second layer includes Europeanized social rights, shaped by soft law principles and objectives, which influence national policies but do not create enforceable rights. The third layer comprises strictly national social rights, adhering to anti-discrimination, equal treatment and social insurance or benefits (ibid.).

Experts at the workshop emphasized that a comprehensive AI governance framework must consider rights as a multilevelled concept, encompassing human rights, social rights, economic rights, political and civil rights, and collective rights. It is insufficient to privilege one category of rights over another, or one country or community's interpretation of rights over others. Diverse regional contexts influence the prioritization, interpretation and realization of rights. For example, American jurisprudence often emphasizes individual rights, while African nations may focus more on collective rights.

Collective rights arise from the shared concerns of a group safeguarding its members against discrimination and abuse (Sanders 1991). These rights are not merely the sum of individual claims but exist specifically because the group, as a whole, holds them (Chandra 2017). Such groups are often connected by common experiences of discrimination as well as shared cultural, religious or linguistic heritage. In Canada, for example, Indigenous people and French Canadians assert collective rights, while in the United States, American Indians may fall within this framework. Unlike individual rights, collective rights aim beyond ensuring equality for members — they focus on the survival and cultural continuity of the group itself (Sanders 1991). This underscores the broader purpose of collective rights: to protect the integrity and existence of marginalized communities rather than just securing equal treatment for individuals within them. Some scholars argue that it is the responsibility of states to shelter marginalized communities from majority decisions, achieved through the implementation of collective rights (Kymlicka 1998).

The debate over a human rights-centred approach to AI governance highlights important concerns regarding the balance between individual and collective rights, as well as regional interpretations of these rights. It is imperative that AI policy making follows a pluralistic approach to rights

5 EC, *Artificial Intelligence Act*, [2024] OJ, L 2024/1689 at art 27, online: <https://artificialintelligenceact.eu/article/27/>.

while being rooted in international human rights instruments to strengthen collective bargaining and compliance across jurisdictions.

Governance Through Existing Policy Instruments

The monopolization of AI technologies, driven by network effects and data centralization, has resulted in a feedback loop that disproportionately benefits large companies, namely social media intermediaries, that have amassed massive amounts of data. In turn, this stifles competition and innovation from smaller players (Tirole 2017). Monopolization is particularly concerning because of the transnational nature of these companies, making it difficult for individual countries to effectively regulate their global power. Dominant AI companies continue to consolidate their market power through exclusive and continuous access to proprietary data sets, computing infrastructures and strategic mergers and acquisitions. As one expert on competition policy and international law argued, anti-trust laws are central to effective AI governance, particularly in jurisdictions where these companies are based. The European Union's Digital Markets Act, for example, designates "gatekeepers" and imposes obligations to prevent self-preferencing and promote fair competition.

In addition to antitrust laws, IP regimes play a crucial role in AI governance. An expert specializing in technology and international law highlighted that the application of IP laws is not uniform across jurisdictions, leading to inequities in how AI technologies are developed and deployed. When applied unevenly, IP laws can suppress traditional and Indigenous knowledge and common ownership, disproportionately affecting communities in the Global Majority (Rai 2016).

Moreover, IP regimes raise questions about the balance between protecting innovation and promoting open access to knowledge in AI governance. While IP laws encourage innovation by giving developers, creators and communities exclusive rights to their work, they can also stifle competition by granting monopolistic control over technological advancements and proprietary data sets (Aertker 2022).

An expert on public sector use of AI at the workshop raised a critical point about the role of procurement in AI governance, an often-overlooked aspect in the broader conversation about AI policy and regulation. Governments are among the largest procurers of AI systems and technologies, and this purchasing power plays a significant role in shaping AI development. In the United States, federal procurement markets amount to US$1.8 trillion per year, roughly 10 percent of the country's GDP.[6] This substantial figure highlights how procurement policies not only influence the technologies governments use but also help to steer the direction of AI research and development. Governments' procurement decisions can encourage or hinder the development of certain technologies, including AI, by either promoting specific vendors or providing incentives for innovation in particular areas (Hufbauer and Jung 2021).

Governments also face infrastructural dependency on major technology firms, such as Microsoft, Amazon and Google. These corporations play a pivotal role in providing the underlying infrastructure and cloud solutions for national systems, which means that governments — while attempting to regulate these companies — are simultaneously dependent on them for critical functions. This dependency complicates the relationship between state regulators and technology firms, potentially undermining efforts to enforce stringent governance policies on the technology sector (Katz 2020). In this context, procurement becomes a tool not just for acquiring technology, but also for shaping the power dynamics between states and private corporations.

In light of these challenges, experts raised several salient questions regarding the procurement of AI systems that can inform how policy makers can approach AI governance. These questions interrogate the fairness and inclusivity of AI procurement processes. For example:

- Who trained the data that qualifies a government agency to procure a specific AI system? This question challenges the transparency and accountability of AI systems, particularly with respect to the sources and biases inherent in training data sets. Given that AI is only as good as the data it is trained on, understanding the provenance of data and the

6 See Open Contracting Partnership (2020).

AI supply chain is crucial for ensuring fair and equitable outcomes (Eubanks 2018).

- How can governments create a level playing field among solution providers? Ensuring that procurement policies do not disproportionately favour large, well-established companies is essential to fostering competition and innovation in the AI market. This can be achieved by promoting policies that encourage diverse vendor participation and safeguard against monopolistic practices (Bandi et al. 2020).

Furthermore, as one expert on international policy noted, addressing inequities using existing policy instruments requires a cradle-to-grave life cycle assessment of AI systems, encompassing environmental, social and economic impacts.

Global Majority as Norm-Shapers

Experts observed that the Global Majority often functions as a norm-taker rather than a norm-setter within the digital policy ecosystem, reflecting broader patterns of power asymmetry in global governance (Couldry and Mejias 2019; Milan and Treré 2019). This dynamic is particularly evident in Southeast Asian and African nations, where policy makers prioritize integration into global markets, often at the cost of adopting digital standards and policies set by dominant Western or Chinese tech powers (Nothias 2020; Graham 2022).

This norm-taking status, when analyzed through frameworks such as digital imperialism and colonialism, highlights how technological infrastructures, data governance and internet regulations are disproportionately shaped by companies and states from the Global North (Zuboff 2023; Birhane 2021). As digital dependency deepens, Global Majority countries risk perpetuating economic and epistemic dependence, reinforcing structural inequalities in the digital economy (Couldry and Mejias 2019; Obi 2024).

The AI supply chain is characterized by significant inequities with a handful of AI companies dominating upstream components such as data, compute and talent (Couldry and Mejias 2019). This concentration of power creates barriers to entry for smaller players, particularly from the Global Majority. For instance, a vast majority of AI systems used in Africa are developed outside the continent, perpetuating dependency on foreign technologies (Centre for Intellectual Property and Information Law 2023). Datafication — the historical conversation of information to data — functions within a colonial political economy to produce knowledge, power and value (Gray 2023). Data is not inherently neutral, but rooted in epistemological violence that upholds a colonial legacy of erasing or appropriating non-Western models of knowing. Technological advancement in the West that relies on datafication and data extraction results in abysmal thinking, algorithmically filtering what is valid knowledge and what should be disregarded as void (Mignolo 2012). In other words, datafication erases marginalized Global Majority communities and realities.

AI and machine learning rely on capitalist imperatives, rather than what is true about the world, that further accelerate the commodification of people's lives. They create new hierarchies of worth, where certain non-Western people, places and histories are devalued while select dominant Western groups are hyper-commodified (Gray 2023). This results in continuing colonial practices by reinforcing global inequalities through the manipulation of data, knowledge and value. Moreover, AI's reliance on large data sets perpetuates the exploitation of underpaid data annotators, many of whom work in precarious conditions in the Global Majority for companies based in the Global North (Gray and Suri 2019).

Inequities in the AI supply chain are further exacerbated by exploitative practices. The extraction of raw materials for AI hardware, such as rare earth metals, often occurs under conditions that violate labour rights and environmental standards (Obi 2024). Many mines in the Democratic Republic of the Congo, for example, rely on child labour and unsafe working conditions to extract cobalt, a critical component in AI hardware and lithium-ion batteries (Amnesty International 2016). Moreover, e-waste from obsolete AI hardware disproportionately affects countries in the Global Majority, where electronic waste is often dumped due to lax environmental regulations (Schluep et al. 2009).

This dynamic not only undermines local innovation but also limits the ability of Global Majority countries to influence global governance norms (Birhane 2021). AI regulation and ethical frameworks are primarily set by institutions in the Global North, leaving the Global Majority to adopt policies without having shaped them (Gwagwa 2024). These structural imbalances reinforce digital colonialism, where control over AI infrastructure and IP remains concentrated in a few powerful economies (Milan and Treré 2019).

Similar to the European General Data Protection Regulation, there are speculations that the AIA will trigger the Brussels effect — the global diffusion of the European Union's approach to regulation. In some cases, AI companies may align their global operations with the AIA's stringent requirements and compliance framework (de facto Brussels effect), while in others, countries may adopt national regulations that are modelled after the European Union's approach (de jure Brussels effect) (Bradford 2020). However, the possible diffusion of European standards among Global Majority countries poses several concerns. Global Majority communities operate within vastly diverse political, legal, cultural and societal contexts, each with its own unique normative values and jurisprudence. Therefore, a de jure or de facto Brussels effect across countries can backfire, failing to meaningfully regulate AI systems while also dissociating from the real-world needs of, and harms on, users.

This haphazard cookie-cutter approach to AI governance in the Global Majority extends to deliberations in global governance fora. One expert on international law and policy noted how Global Majority nations are often relegated to the position of passive participants rather than active contributors. Although global institutions such as the United Nations and the World Trade Organization claim to promote inclusivity, their mechanisms often fail to deliver meaningful representation for the Global Majority. For example, the participation of Global Majority countries is frequently limited to observing or providing inputs that are ultimately disregarded in the decision-making process. This creates a façade of inclusivity while maintaining the status quo of dominance by the Global North (Pogge 2005).

Additionally, Global Majority countries face structural obstacles in shaping outcomes at international fora. These obstacles include limited access to key information, technical expertise and financial resources, which undermine their ability to influence international policy effectively. Furthermore, the power dynamics in institutions such as the UN Security Council, where permanent members hold veto power, reveal the deep structural inequalities embedded in the global governance system (Higott 2004).

In recent years, Global Majority countries such as Brazil, India, Indonesia and South Africa — with growing GDPs — have become more critical of Western hegemony, especially in digital innovation and multilateral governance. Since 2022, starting with Indonesia's presidency of the Group of Twenty (G20), there has been a slow, yet significant, shift in the G20+[7] countries adopting priorities and policy concerns of Global Majority communities, for example, digital public infrastructure and equitable AI benefits. The full admission of the African Union to the G20 under India's 2023 presidency marked a critical geopolitical win, both for the G20+ and African nations. Their expanded representation will force increased strategic cooperation among the 55 African countries, particularly on achieving the sustainable development goals, addressing debt vulnerabilities and accelerating shared priorities on digital innovation and economic growth.

Experts at the workshop emphasized that it is encouraging to observe Global Majority countries progressing toward becoming norm-setters; however, it is important to distinguish between harmonization and homogenization in the context of AI governance. This distinction is critical when considering the diverse approaches to AI across the Global Majority, where countries and regions are tackling the digital economy in ways that reflect their unique social, economic and political contexts.

For example, the African Union's Continental Artificial Intelligence Strategy [8] reflects a growing commitment to fostering regional collaboration in AI governance. The strategy calls for the revision of existing legal frameworks, especially data protection and IP, to govern AI and better address its risks. Moreover, it advocates for the use of tools such as ethical impact assessments and regulatory sandboxes, which allow for the testing of AI technologies in controlled environments. The strategy emphasizes the importance of supporting

7 The G20 is now often referred to as G20+ because its membership shifts over time and does not always remain fixed at 20 countries.

8 See African Union (2024).

African-led research initiatives and encourages the development of agile, forward-thinking, risk-based regulations at the national level.

In contrast, Southeast Asia's digital economy strategy focuses on creating an inclusive, region-specific ecosystem that emphasizes digital access, entrepreneurship and capacity building (Hourn 2025). By adopting a pluralistic approach, these regions can ensure that their AI governance frameworks are more reflective of their needs and aspirations, allowing for more localized decision making and innovation. Moreover, this approach allows for greater flexibility in integrating diverse models of governance, such as collective rights in Africa and in parts of Asia (Smuha 2021b).

Policy Recommendations

Adopt Dynamic and Contextual Risk Assessment Models

Policy makers should move away from static, one-size-fits-all risk assessments, and adopt more dynamic frameworks that account for the evolving nature of AI technologies. This includes developing risk assessments that consider the impact of AI on different communities and contexts, factoring in vulnerability profiles, severity and consequences. AI systems should be evaluated not only based on their intended purpose but also based on the specific environment and the group being impacted. A tiered approach to risk classification, recognizing the differentiated risks to individuals, communities and society, can help to more accurately assess and mitigate AI-related harms as they emerge.

Strengthen Regulatory Focus on Upstream AI Development Components

To address the root causes of problematic AI applications, policy makers must direct attention to upstream components such as data collection, computation power and the business models of AI developers. The dominance of extractive business models of AI companies exacerbates privacy violations, digital imperialism and societal harm. By focusing on the ethical implications of AI systems from development to deployment, including the treatment of data and algorithmic design, governments can curtail harmful business models early on.

Governments, as major procurers of AI systems, have significant leverage to promote ethical practices within the AI supply chain. Public procurement policies should require vendors to demonstrate compliance with relevant labour rights, environmental standards and data protection laws. In particular, governments should prioritize contracts with vendors that conduct comprehensive life cycle assessments of their AI systems.

Incorporate Multi-Levelled Human Rights Frameworks in AI Governance

Policy makers should adopt a pluralistic, multi-levelled approach to human rights in AI governance. Recognizing the need to balance individual, collective and societal rights, AI regulation should not prioritize one category of rights over others. For example, while individual privacy is crucial, collective rights (such as the protection of marginalized groups) must also be considered to ensure that AI systems do not perpetuate systemic discrimination. A nuanced understanding of rights — incorporating economic, social and cultural considerations — should be integrated into AI policy making. This will help ensure that AI governance reflects a global understanding of rights, including diverse regional perspectives, and mitigates the risks posed by AI technologies on vulnerable communities.

Strengthen Inclusive and Participatory Governance

Developing and implementing robust accountability mechanisms to strengthen AI governance is more pressing now than ever. Policy makers should explore existing legislative instruments, for example, antitrust and intellectual property laws, to prevent monopolistic practices that may stifle innovation and limit access to AI technologies. AI systems, particularly those controlled by large tech corporations, often benefit from network effects, making it difficult for smaller players to enter the market.

Furthermore, governments and international organizations must create mechanisms that ensure meaningful participation from marginalized communities in decision-making processes, while ensuring AI policy making is centred on safeguarding multilevel and multifaceted rights of communities. Integrating Indigenous and community knowledge and perspectives into policy discussions can offer unique insights into sustainable, community-centred AI development, challenging dominant Western paradigms that often overlook cultural diversity and risk perpetuating digital imperialism.

Acknowledgement

This paper was developed following discussions at a virtual workshop, hosted by CIGI, bringing together experts from diverse fields worldwide. The ideas and recommendations outlined in the paper are a collaborative effort of numerous expert opinions and debates and aimed at taking a historical view of intermediary governance to inform and influence the discourse on AI policy making.

The following experts participated in the workshop: Aaron Shull, Courtney Radsch, Samantha Bradshaw, Justin Hendrix, Jiahao Chen, Frederike Kaltheuner, Mishi Chaudhary, Christabel Randolph, Elina Noor, Jake Okechukwu Effoduh, Tracey Forrest and Dana Cramer.

Works Cited

Aertker, Mary. 2022. "International Copyright's Exclusion of the Global South." *Michigan Journal of International Law* (blog), February. www.mjilonline.org/international-copyrights-exclusion-of-the-global-south/.

African Union. 2024. *Continental Artificial Intelligence Strategy: Harnessing AI for Africa's Development and Prosperity*. August 9. https://au.int/en/documents/20240809/continental-artificial-intelligence-strategy.

Alphabet Inc. 2020. "Form 10-K: Annual Report Pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934." Washington, DC: US Securities and Trade Commission. https://abc.xyz/assets/investor/static/pdf/20210203_alphabet_10K.pdf?cache=b44182d.

Amnesty International. 2016. *This Is What We Die For: Human Rights Abuses in the Democratic Republic of the Congo Power the Global Trade in Cobalt*. London, UK: Amnesty International.

Bandi, Rajendra K., Stefan Klein, Shirin Madon, Eric Monteiro and Ranjini C.R. 2020. "The Future of Digital Work: The Challenge of Inequality." In *IFIP Joint Working Conference on the Future of Digital Work: The Challenge of Inequality*, edited by Rajendra K. Bandi, Ranjini C.R., Stefan Klein, Shirin Madon and Eric Monteiro, 3–10. Cham, Switzerland: Springer. https://doi.org/10.1007/978-3-030-64697-4_1.

Birhane, Abeba. 2021. "Algorithmic Colonization of Africa." *Scripted* 18 (2): 1–17. https://doi.org/10.1093/oso/9780192865366.003.0016.

Birkstedt, Teemu, Matti Minkkinen, Anushree Tandon and Matti Mäntymäki. 2023. "AI governance: themes, knowledge gaps and future agendas." *Internet Research* 33 (7): 133–67. https://doi.org/10.1108/INTR-01-2022-0042.

Bradford, Anu. 2020. *The Brussels Effect: How the European Union Rules the World*. Oxford, UK: Oxford University Press.

Carrillo, Margarita Robles. 2020. "Artificial intelligence: From ethics to law." *Telecommunications Policy* 44 (6): 101937. https://doi.org/10.1016/j.telpol.2020.101937.

Centre for Intellectual Property and Information Technology Law. 2023. *The State of AI in Africa Report*. Strathmore University. https://cipit.strathmore.edu/wp-content/uploads/2023/05/The-State-of-AI-in-Africa-Report-2023-min.pdf.

Chandra, Rakesh. 2017. "Collective rights vs. Individual rights." *International Journal of Multidisciplinary Research and Development* 4 (7): 51–55. www.allsubjectjournal.com/assets/archives/2017/vol4issue7/4-6-199-649.pdf.

Couldry, Nick and Ulises A. Mejias. 2019. *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism*. Stanford, CA: Stanford University Press.

Deibert, Ron, Rafal Rohozinski, Arnav Manchanda, Nart Villeneuve and Greg Walton. 2009. *Tracking GhostNet: Investigating a Cyber Espionage Network*. Information Warfare Monitor, March 29. https://citizenlab.ca/wp-content/uploads/2017/05/ghostnet.pdf.

DeNardis, Laura and Andrea M. Hackl. 2015. "Internet governance *by* social media platforms." *Telecommunications Policy* 39 (9): 761–70. https://doi.org/10.1016/j.telpol.2015.04.003.

Dickson, Julia and Lauren Burke Preputnik. 2024. "Cyber Scamming Goes Global: Unveiling Southeast Asia's High-Tech Fraud Factories." Center for Strategic and International Studies, December 12. www.csis.org/analysis/cyber-scamming-goes-global-unveiling-southeast-asias-high-tech-fraud-factories.

Diya, Sabhanaz Rashid. 2025. "Applying International Human Rights Principles for AI Governance." Policy Brief No. 196. Waterloo, ON: CIGI. www.cigionline.org/publications/applying-international-human-rights-principles-for-ai-governance/.

Eubanks, Virginia. 2018. A*utomating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. New York, NY: St. Martin's Press.

Effoduh, Okechukwu Jake. 2021. "Preparing for frontier risks in the new economy." In *Building Back Broader: Policy Pathways for an Economic Transformation*, 58–70. White Paper. June. Centre for the New Economy and Society, World Economic Forum. https://rshare.library.torontomu.ca/articles/report/Preparing_for_Frontier_Risks_in_the_New_Economy/24242971?file=42560350.

Ferrera, Maurizio, Francesco Corti and Maarten Keune. 2024. "How to conceptualise EU social rights and EU social citizenship? A multi-level resource-based framework." In *The State of European Social Rights and European Social Citizenship*, edited by Maarten Keune, 16–33. https://doi.org/10.5281/zenodo.10840424.

Gasser, Urs, and Wolfgang Schulz. 2015. "Governance of Online Intermediaries: Observations from a Series of National Case Studies." *Korea University Law Review* 18: 79. http://dx.doi.org/10.2139/ssrn.2566364.

Gillespie, Tarleton. 2010. "The politics of 'platforms.'" *New Media & Society* 12 (3): 347–64. https://doi.org/10.1177/1461444809342738.

González-Tosat, Clara and Charo Sádaba-Chalezquer. 2021. "Digital Intermediaries: More than New Actors on a Crowded Media Stage." *journalism and media* 2 (1): 77–99. https://doi.org/10.3390/journalmedia2010006.

Graham, Mark. 2022. *Digital Empires: The Global Battle to Regulate Technology*. Oxford, UK: Oxford University Press.

Gray, Catriona. 2023. "More than Extraction: Rethinking Data's Colonial Political Economy." *International Political Sociology* 17 (2): olad007. https://doi.org/10.1093/ips/olad007.

Gray, Mary L. and Siddharth Suri. 2019. *Ghost Work: How to Stop Silicon Valley from Building a New Global Underclass*. Boston, MA: Houghton Mifflin Harcourt.

Gupta, Indranath and Lakshmi Srinivasan. 2023. "Evolving scope of intermediary liability in India." *International Review of Law, Computers & Technology* 37 (3): 294–324. https://doi.org/10.1080/13600869.2022.2164838.

Gwagwa, Arthur. 2024. "Resisting colonialism – why AI systems must embed the values of the historically oppressed." In *Artificial intelligence and the challenge for global governance*. Chatham House. June. www.chathamhouse.org/sites/default/files/2024-06/2024-06-07-ai-challenge-global-governance-krasodomski-et-al.pdf.

Helmond, Anne and Fernando N. van der Vlist. 2019. "Social Media and Platform Historiography: Challenges and Opportunities." *TMG Journal for Media History* 22 (1): 6–34. https://doi.org/10.18146/tmg.434.

Higott, Richard A. 2004. "Multilateralism and the Limits of Global Governance." Centre for the Study of Globalisation and Regionalisation Working Paper 134. University of Warwick. May. https://wrap.warwick.ac.uk/id/eprint/1980/1/WRAP_Higgott_wp13404.pdf.

Hogan, Bernie and Anabel Quan-Haase. 2010. "Persistence and Change in Social Media." *Bulletin of Science, Technology & Society* 30 (5): 309–15. https://doi.org/10.1177/0270467610380012.

Hourn, Kao Kim. 2025. "Why ASEAN's new Digital Economy Framework Agreement is a game-changer." World Economic Forum, May 26. www.weforum.org/stories/2025/05/asean-digital-economy-framework-agreement-a-gamechanger/.

Huber, Wolfgang. 2014. "Human rights and globalisation – Are human rights a 'Western' concept or a universalistic principle?" *Dutch Reformed Theological Journal* 55 (1–2): 117–37. https://doi.org/10.5952/55-1-2-518.

Hufbauer, Gary Clyde and Euijin Jung. 2021. "Scoring 50 years of US industrial policy, 1970–2020." Peterson Institute for International Economics Briefing 21-5. November. www.piie.com/publications/piie-briefings/2021/scoring-50-years-us-industrial-policy-1970-2020.

Kaplan, Andreas M. and Michael Haenlein. 2010. "Users of the world, unite! The challenges and opportunities of Social Media." *Business Horizons* 53 (1): 59–68. https://doi.org/10.1016/j.bushor.2009.09.003.

Katz, Ariel. 2020. "The Chicago School and the Forgotten Political Dimension of Antitrust Law." *The University of Chicago Law Review* 87 (2). https://lawreview.uchicago.edu/print-archive/chicago-school-and-forgotten-political-dimension-antitrust-law.

Kymlicka, Will. 1998. "Ethnic Associations and Democratic Citizenship." In *Freedom of Association*, edited by Amy Gutmann, 177–213. Princeton, NJ: Princeton University Press.

Lagg, Emily. 2018. "Stormy Waters for the Internet's Safe Harbor: The Future of Section 230." *Rutgers University Law Review* 71: 763–94. http://rutgerslawreview.com/wp-content/uploads/2020/04/07_Lagg.pdf.

Martín del Río, Marina. 2024. "The Use of Digital Technologies at Borders: a Migrant-centred Analysis." Universitat Ramon Llull. https://dau.url.edu/handle/20.500.14342/4519.

Mignolo, Walter D. 2012. *Local Histories/Global Designs: Coloniality, Subaltern Knowledges, and Border Thinking*. Princeton, NJ: Princeton University Press.

Milan, Stefania and Emiliano Treré. 2019. "Big Data from the South(s): Beyond Data Universalism." *Television & New Media* 20 (4): 319–35. https://doi.org/10.1177/1527476419837739.

Nothias, Toussaint. 2020. "Access granted: Facebook's free basics in Africa." *Media, Culture & Society* 42 (3): 329–48. https://doi.org/10.1177/0163443719890530.

Novelli, Claudio, Federico Casolari, Antonino Rotolo, Mariarosaria Taddeo and Luciano Floridi. 2024. "AI Risk Assessment: A Scenario-Based, Proportional Methodology for the AI Act." *Digital Society* 3 (1). https://doi.org/10.1007/s44206-024-00095-1.

Obar, Jonathan A. and Steve Wildman. 2015. "Social media definition and the governance challenge: An introduction to the special issue." *Telecommunications Policy* 39 (9): 745–50. https://doi.org/10.1016/j.telpol.2015.07.014.

Obi, Paul A. 2024. "Labouring and Smiling: Re-imagining Digital Colonialism in Africa, Silicon Valley Big Techs, and the Politics of Prosumer Capitalism in Nigeria." *tripleC* 22 (1): 381–95. https://doi.org/10.31269/triplec.v22i1.1451.

Open Contracting Partnership. 2020. *How governments spend: Opening up the value of global public procurement.* www.open-contracting.org/wp-content/uploads/2020/08/OCP2020-Global-Public-Procurement-Spend.pdf.

Organisation for Economic Co-operation and Development. 2024. "Explanatory Memorandum on the Updated OECD Definition of an AI System." Artificial Intelligence Paper No. 8. March. www.oecd.org/content/dam/oecd/en/publications/reports/2024/03/explanatory-memorandum-on-the-updated-oecd-definition-of-an-ai-system_3c815e51/623da898-en.pdf.

Pogge, Thomas. 2005. *Global Justice: A Theory of Social Institutions.* Oxford, UK: Oxford University Press.

Rai, Arti K. 2016. *Intellectual Property and the Public Domain in Developing Countries.* Cambridge, UK: Cambridge University Press.

Ritzer, George and Nathan Jurgenson. 2010. "Production, consumption, prosumption: The nature of capitalism in the age of the digital 'prosumer.'" *Journal of Consumer Culture* 10 (1): 13–36. https://doi.org/10.1177/1469540509354673.

Rookard, Landyn Wm. 2024. "The Common Threats of Artificial Intelligence and Privatization." *Texas A&M Law Review* 12 (2): 831–89. https://doi.org/10.37419/LR.V12.I2.8.

Sanders, Douglas. 1991. "Collective Rights." *Human Rights Quarterly* 13 (3): 368–86. https://doi.org/10.2307/762620.

Schluep, Mathias, Christian Hagelüken, Ruediger Kuehr and Federico Magalini. 2009. *Recycling – From E-Waste to Resources.* United Nations Environment Programme. July. www.researchgate.net/publication/278849195_Recycling_-_from_e-waste_to_resources.

Slater, Derek. 2008. "Rep Markey's net neutrality legislation." *Google Policy Blog*, February 13. https://publicpolicy.googleblog.com/2008/02/rep-markeys-net-neutrality-legislation.html.

Smuha, Nathalie A. 2021. "Beyond a Human Rights-Based Approach to AI Governance: Promise, Pitfalls, Plea." *Philosophy & Technology* 34 (1): 91–104. https://doi.org/10.1007/s13347-020-00403-w.

— — —. 2021b. "Beyond the individual: governing AI's societal harm." *Internet Policy Review* 10 (3). https://doi.org/10.14763/2021.3.1574.

Smuha, Nathalie A., Emma Ahmed-Rengers, Adam Harkens, Wenlong Li, James MacLaren, Riccardo Piselli and Karen Yeung. 2021. "How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act." LEADS Lab at University of Birmingham, August 5. https://pure.strath.ac.uk/ws/portalfiles/portal/163032961/Smuha_etal_SSRN_2021_How_the_EU_can_achieve_legally_trustworthy_AI.pdf.

Souza, Carlos Affonso Pereira, Mario Viola and Ronaldo Lemos. 2015. *Understanding Brazil's Internet Bill of Rights.* Rio de Janeiro, Brazil: Instituto de Tecnologia e Sociedade do Rio de Janeiro. https://itsrio.org/wp-content/uploads/2015/11/Understanding-Brazils-Internet-Bill-of-Rights.pdf.

Taddeo, Mariarosaria. 2017. "Data Philanthropy and Individual Rights." *Minds and Machines* 27 (1): 1–5. https://doi.org/10.1007/s11023-017-9429-2.

Talbott, William J. 2007. *Which Rights Should Be Universal?* Oxford, UK: Oxford University Press.

Tirole, Jean. 2017. Economics for the Common Good. Princeton, NJ: Princeton University Press.

Ulnicane, Inga, Damian Okaibedi Eke, William Knight, George Ogoh and Bernd Carsten Stahl. 2021. "Good governance as a response to discontents? Déjà vu, or lessons for AI from other emerging technologies." Interdisciplinary Science Reviews 46 (1–2): 71–93. https://doi.org/10.1080/03080188.2020.1840220.

United Nations Office on Drugs and Crime. 2024. "Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia: A Hidden and Accelerating Threat." Technical Policy Brief. January. www.unodc.org/roseap/uploads/documents/Publications/2024/Casino_Underground_Banking_Report_2024.pdf.

US Department of Justice. 2024. "Seven Hackers Associated with Chinese Government Charged with Computer Intrusions Targeting Perceived Critics of China and U.S. Businesses and Politicians." Press release, March 25. www.justice.gov/archives/opa/pr/seven-hackers-associated-chinese-government-charged-computer-intrusions-targeting-perceived.

Van Dijck, José. 2009. "Users like you? Theorizing agency in user-generated content." *Media, Culture & Society* 31 (1): 41–58. https://doi.org/10.1177/0163443708098245.

Wagner, Ben. 2018. "Ethics As An Escape From Regulation. From 'Ethics-Washing' To Ethics-Shopping?" In *Being Profiled: COGITAS ERGO SUM. 10 Years of Profiling the European Citizen*, edited by Emre Bayamlıoğlu, Irina Baraliuc, Liisa Janssens and Mireille Hildebrandt, 84–88. Amsterdam, The Netherlands: Amsterdam University Press.

Watson, David. 2019. "The Rhetoric and Reality of Anthropomorphism in Artificial Intelligence." *Minds and Machines* 29: 417–40. https://doi.org/10.1007/s11023-019-09506-6.

Whitehead, David E., Kevin Owens, Dennis Gammel and Jess Smith. 2017. "Ukraine cyber-induced power outage: Analysis and practical mitigation strategies." *2017 70th Annual Conference for Protective Relay Engineers*, 1–8. https://doi.org/10.1109/CPRE.2017.8090056.

Yates, Luke. 2023. "How platform businesses mobilize their users and allies: Corporate grassroots lobbying and the Airbnb 'movement' for deregulation." *Socio-Economic Review* 21 (4): 1917–43. https://doi.org/10.1093/ser/mwad028.

Zittrain, Jonathan. 2009. *The Future of the Internet and How to Stop It. London*, UK: Penguin UK.

Zuboff, Shoshana. 2023. "The Age of Surveillance Capitalism." In *Social Theory Re-wired: New Connections to Classical and Contemporary Perspectives*, edited by Wesley Longhofer and Daniel Winchester, 203–13. New York, NY: Routledge.

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org