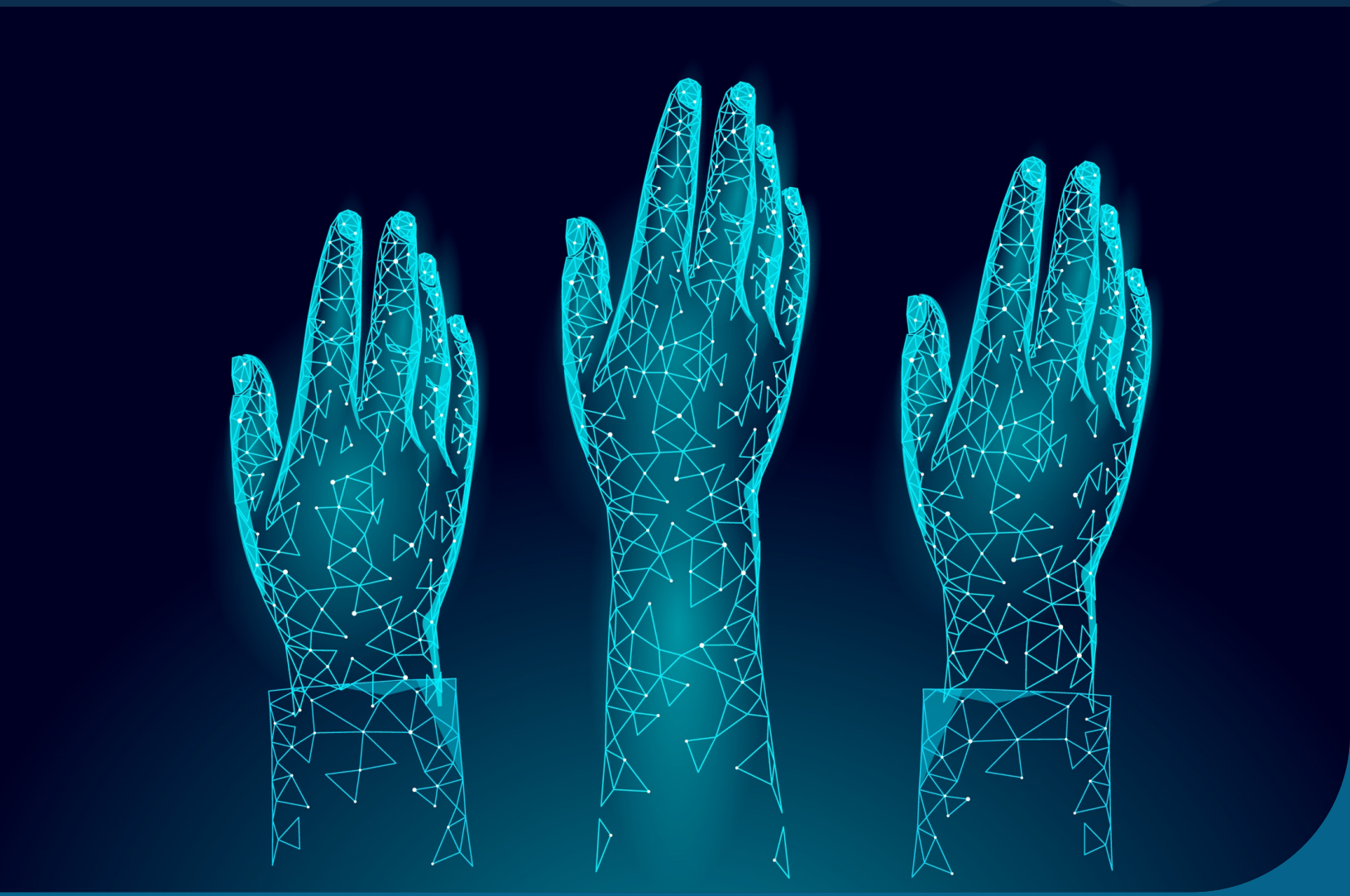
SETTING DEMOCRATIC GROUND RULES FOR AI

CIVIL SOCIETY STRATEGIES

// BETH KERLEY



NED NATIONAL ENDOWMENT FOR DEMOCRACY
SUPPORTING FREEDOM AROUND THE WORLD

FORUM INTERNATIONAL FORUM FOR DEMOCRATIC STUDIES

// REPORT / OCTOBER 2023

SETTING DEMOCRATIC GROUND RULES FOR AI

CIVIL SOCIETY STRATEGIES

CONTENTS

NED NATIONAL ENDOWMENT FOR DEMOCRACY
SUPPORTING FREEDOM AROUND THE WORLD

FORUM INTERNATIONAL FORUM FOR DEMOCRATIC STUDIES

ABOUT THE REPORT

On May 11-12, 2023, the International Forum for Democratic Studies ("The Forum") held a private, expert workshop in Buenos Aires, Argentina, hosted by Chequeado, to consider how civil society can advance approaches to governing artificial intelligence (AI) that uphold democratic principles and follow democratic processes. The Forum brought together a group of roughly forty experts including civil society practitioners from the digital rights and open data communities, academic researchers, and select private sector representatives. The majority of participants were based in Latin America, although several joined us from other regions.

In recent years, many organizations rooted in traditional digital issues such as internet freedom, data privacy, and information space integrity have begun tracking challenges from AI advances to democratic values. These include the erosion of privacy; gaps in accountability for decisions made by automated systems; algorithmic bias and discrimination; and growing public cynicism as AI-generated content floods the information space. With AI rising on the agendas of national governments as well as institutions such as the UN and the G-7, this workshop provided an opportunity to take stock of where we stand on the road to democratic AI governance. Discussions focused on knowledge gaps in different stakeholder communities; privacy implications of AI; challenges linked to AI fairness, bias, and explainability; and opportunities for democratic actors to level the balance by harnessing their own AI tools.

The following analysis, compiled by Forum program officer Beth Kerley, distills key workshop takeaways with the aim of providing a starting point for colleagues in the democracy community and beyond thinking through AI's intersections with democratic norms; the conceptual and strategic challenges of this emerging field; and potential avenues for civil society engagement. Discussion points are drawn from our expert participants, but do not necessarily reflect a consensus among the group and should not be taken as official positions of the Forum or of the National Endowment for Democracy. Rather, they are intended to survey key areas of focus, frequent concerns, and preferred strategies of researchers and practitioners working for democratic governance of artificial intelligence.

FORUM | INTERNATIONAL FORUM FOR DEMOCRATIC STUDIES

HIGHLIGHTS: SETTING DEMOCRATIC GROUND RULES FOR AI

Advances in artificial intelligence (AI) are transforming political landscapes, impacting how people exercise their rights, and presenting new challenges to democratic principles such as privacy, transparency, accountable governance, and non-discrimination. Democratic AI governance is critical, yet significant barriers to engagement in this area remain. Drawing upon conversations from a private workshop in Buenos Aires, Argentina, the International Forum for Democratic Studies compiled an overview of eight key challenges to and opportunities for the democratic governance of AI.

1. **AI technologies reflect the human choices and structures behind them.** The wide range of technologies described by the term "AI" are shaped by human choices about design and deployment, as well as the social and political contexts that feed into training data. Like all human products, they must be open to challenge by democratic activists and institutions.

2. **The risks and harms associated with AI challenge traditional assumptions.** These impacts can arise at all stages of the AI pipeline, from development to procurement to use, and they may demand new ways of thinking about issues like data protection.

3. **Opacity around AI hinders democratic engagement.** AI systems from surveillance cameras to social-media algorithms already work in the background of our daily lives, and the institutions that deploy them often prefer not to share the details. This reluctance, as well as the inherent complexity of AI systems, can make it hard to map the impacts of these tools.

4. **Addressing AI impacts will require more than just technical expertise.** Because AI risks and harms have social and political roots, they will also require social and political responses. Moreover, these responses may sometimes demand trade-offs between competing democratic values.

5. **Democracies must close institutional gaps and widen participation in AI governance.** Democratic institutions remain broadly unprepared to manage AI harms. Technical expertise on AI is concentrated in the private sector, which places democracies and their publics at a disadvantage in key decision-making processes—many of which exclude civil society and marginalized communities.

6. **New mechanisms and enduring democratic principles both have important roles to play.** Democratic governance of AI may require building specialized institutions, but it also hinges on finding ways to apply existing democratic laws and principles effectively when AI tools enter the picture.

7. **Tech expertise within civil society can help influence the trajectory of AI technologies.** Cutting-edge civil society groups are leveraging their technical skills to pinpoint government or corporate systems' vulnerabilities; model more inclusive, representative, and responsible approaches to design; and develop AI tools to support civic accountability activities.

8. **The complexity of AI governance makes cross-sectoral collaboration crucial.** AI governance challenges cut across traditional sectoral boundaries. New partnerships and knowledge-sharing initiatives that bring together digital rights groups, traditional human rights groups, journalists, trade unions, teachers, and others can enable civil society organizations to address these issues more effectively.

For more on the Forum's research on emerging technologies in areas like surveillance, AI and government accountability, and smart cities, go to .

INTRODUCTION

Advances in artificial intelligence (AI) are changing the playing field for democracy. Since social media's emergence as a tool of protest, commentators have regularly stressed how our evolving technological landscape is transforming our political world. The digital tools on which we rely help to determine how people express themselves, find like-minded communities, and initiate collective action. As the International Forum has tracked in our "Making Tech Transparent" series examining AI surveillance,[1] smart cities,[2] and the digitalization of governance,[3] these technologies also affect how governments monitor people, administer services, and dole out repression. AI systems—which include interactive language models such as ChatGPT, but also facial recognition software, predictive policing technologies, and analytical tools designed to make sense of public procurement documents or assess social benefit applications—have potentially transformative impacts across these fronts.

If it is clear that AI will shape the political world we inhabit, however, there remain many questions around how democratic norms and institutions will shape the trajectory of AI. Since the "liberation technology" buzz of the early 2010s, experts and publics alike have grown more skeptical of assumptions that technological development will automatically advance values such as free expression, freedom of association, and a level playing field for civic engagement.[4] Digital advances that foster open communication can also

make it easier for repressive regimes to surveil and harass opponents, or skew public debate by amplifying conspiracy theories and state propaganda disproportionately.

With recent leaps in the development of large language models (LLMs), the global proliferation of AI surveillance tools,[5] and growing enthusiasm for the automation of governance processes,[6] we are poised for another seismic shift in the balance of power between people and governments. Recognizing that digital advances themselves do not work to democracy's benefit inevitably, prodemocratic stakeholders must engage proactively to erect guardrails around AI development and deployment; ensure consultation with communities whose democratic rights may be impacted by AI systems; and chart development trajectories that infuse AI technologies with democratic values. The consolidation in dictatorships of authoritarian models for the integration of AI—which reject privacy, popular input, and rights-based frameworks in favor of top-down-control—heightens the urgency of this task.

The following analysis, drawn from contributions at the May 2023 workshop "Closing Knowledge Gaps, Fostering Participatory AI Governance: The Role of Civil Society" in Buenos Aires, Argentina, presents some initial reflections from expert stakeholders—chiefly within the digital rights and open government communities—about the present state of the AI governance landscape and potential avenues for civil society intervention. These reflections address the narratives and structures steering AI development; current obstacles to upholding democratic norms in this domain; and strategies for collaboration, communication, and institution-building to advance democratic AI governance.

Several major themes emerged from our discussion. These key points include, first, the need for stakeholders across government, media, civil society, and the private sector to ***see the human agency, relationships, and structures behind AI models***—whether the social inequalities that produce biases in data and design, or the political relationships that underpin surveillance deals. Recognizing the human factors and choices that determine how AI systems affect us, rather than seeing these impacts as inevitable, is critical to maintaining democratic *accountability* for the policy makers, developers, and others who exercise power over and through AI technologies.

"AI models impact human rights, particularly the free and full enjoyment of freedom of expression and the right to privacy. And because these fundamental rights are a cornerstone for democracy, I do not have any doubt that good governance of AI is a democracy issue."

— Eduardo Bertoni, Inter-American Institute of Human Rights (Argentina)

Second, these contributions underscore the urgency of ***equipping democratic societies and institutions to keep up with a constantly evolving set of AI harms and risks***. The absence of established norms, learning processes, and institutions to address these impacts challenges governments looking to regulate AI as much as it does civil society organizations (CSOs) considering whether they can use AI tools responsibly. Even as processes such as algorithmic impact assessments (AIAs) become more institutionalized, the underlying technical landscape is changing. Recent advances in LLMs, for instance, are not only lowering the costs of influence operations and making it even harder to explain how AI systems work, but they are also posing new threats to online anonymity by making it possible to deduce personal attributes using semantic cues.

Finally, participants stressed the importance of ***developing new strategies, processes, and collaborations to give real force to principles such as AI transparency, accountability, and privacy by design***. Participants faced serious challenges both in engaging with the private-sector actors responsible for much of the decision-making around AI, and in translating state transparency and accountability mechanisms into meaningful rights protections. Deeper involvement by affected stakeholders, especially marginalized communities, at earlier stages of regulatory and design processes was a recurring demand.

At the same time, the complex tasks of mapping AI use, assessing system risks, advocating across institutions, and clarifying the competing values at stake in AI deployments demand multiple forms of expertise that defy any clear boundaries between digital and traditional human rights. Such work will require new collaborations bringing together the digital rights and open government communities as well as traditional human rights organizations, professional "gatekeepers" such as journalists and academics, labor unions, and others, as well as efforts to develop a shared vocabulary on AI across these diverse stakeholder communities. Building up internal capacities on AI and identifying synergies across organizations can help CSOs in turn to more effectively promote informed engagement by society at large.

While the following reflections are by no means an exhaustive survey of ways in which AI will impact democratic societies, they will offer a starting point for others in the democracy community and beyond thinking about where to engage in the AI governance domain, what obstacles they might face, and how CSOs might position themselves to address this evolving challenge.

STARTING POINTS FOR DEMOCRATIC DEBATE

The challenge of AI governance sits at the crossroads of the political and the technical. What aspects of AI impinge upon democratic norms, and what types of institutions are needed to govern these systems democratically? What competing values are at stake in AI governance, and how might local context affect these trade-offs? The following are key imperatives which our discussants emphasized across three fronts: **(1) understanding the technical nature, possibilities, and requirements of AI systems; (2) understanding the social and political structures that give shape to AI design, deployment, and norms;** and **(3) understanding the risks and harms from AI technologies, and the efforts that will be required to mitigate them.** Deeper and broader understanding in each of these areas can help lay the groundwork for an all-of-society approach to ensuring that AI works for democracy.

Know What AI Is and Is Not

In order to meaningfully use and regulate AI in a way that protects democratic values, stakeholders across government, civil society, and relevant professional communities need a clear understanding of both what AI systems are, and how social and political structures shape their workings. The term AI covers a wide range of applications, with specific strengths and weaknesses that may be obscured when commentators talk about AI systems as if they were human, or mystify the technology behind them, or overuse this description as a marketing

tactic. A clearer understanding of the tools and capabilities in question can help to lay the foundations for democratic deliberation on AI, as well as help to identify where this technology might advance CSOs' work in defense of democracy. At the same time, effective AI governance requires awareness of the human decisions, assumptions, and power structures that feed into AI systems—factors which, like all flawed human structures and choices, must be open to scrutiny by democratic activists and institutions.

> "I reject the notion of responsible or ethical AI. It is not the computer program that is supposed to be responsible and ethical, but rather the people and institutions that create and implement it. It is incumbent on them to be transparent and to protect human rights."
> — Krzysztof Izdebski, Stefan Batory Foundation (Poland)

The term AI encompasses a broad set of technologies with distinct strengths and limits

- The term "AI," whose definition is itself a subject of debate, encompasses a complex variety of technologies from chatbots to robots to facial-recognition software.[7] Public discussion often treats "AI" as a unitary entity. Yet, while some common technical foundations and rights challenges are common across systems—for example, most AI relies on machine learning, and many systems raise data privacy concerns—different applications present distinct risks and benefits, and may require different governance approaches. Many of the AI systems currently impacting democracy both online and on the ground do not resemble large language models (LLMs) such as OpenAI's GPT-4, although experts believe that LLMs and other large and generalized "foundation models" will increasingly serve as the bases upon which other, more customized systems are built.[8]
- **Better awareness of the strengths and limits of AI technologies can help governments as well as CSOs to engage critically with developers, and to incorporate AI in ways that respect rights and make sense for their operations.** While this field is evolving rapidly, one experienced practitioner singled out three categories of relevant applications: organizing and sorting to quickly make sense of a mass of information that otherwise would not be comprehensible; detecting threats (such as deepfakes or cyberattacks) and anomalies (such as in government procurement); and making predictions. Analytical and detection tools hold promise for organizations working in a range of fields, from gender equality to data protection to anti-corruption, to counter antidemocratic practices. Nonetheless, human intervention remains key to translate data-driven insights into programmatic and policy advances.

Social and political context are critical to AI development as well as AI governance

- Rather than thinking of technology itself as an agent, participants emphasized the need to keep in mind how social and political factors drive choices around AI development and deployment. These choices, in turn, help to determine who AI development serves.
- At the most basic technical level, AI models reflect the histories of the societies which produce their training data, the inequalities that shape who is or is not represented in datasets, and the choices or assumptions of developers who optimize for certain priorities and not others. Thus, **models may fall short when used in contexts not reflected in their training data, or fail to serve marginalized populations who have faced historical injustice.** One Latin American participant warned others in the group to "beware of datasets designed in the Global North."
- More broadly, how AI tools work depends greatly on the context in which they are deployed: For instance, a government watchdog or a CSO looking to leverage AI insights will need the right data infrastructure in place in order to do so effectively.[9] AI systems designed in one country often perform unreliably—and may cause unexpected harms—when exported to settings with different governance structures, or simply different digital or data infrastructure.
- Relationships between vendors and officials, especially in the public sector, shape how AI is deployed and used. AI-enabled tools for law enforcement, for instance, may sometimes serve political or commercial ends as much as or more than public safety, despite likely exaggerated claims around their crime-fighting benefits.[10] To better understand the logic and vision behind the deployment of Huawei facial recognition cameras in Belgrade, activists in Serbia unpacked the broader Serbia-China cooperative relationship that underpinned this deployment.[11] Enterprising CSOs have similarly traced relationships between surveillance vendors and officials in Argentina and Mauritius.[12] Follow-the-money initiatives can similarly help to illuminate power relationships that help to shape AI norms.

Recognize the Complexity of AI Risks and Harms

AI presents a complex array of risks and harms—near-, mid-, and long-term—that are evolving with the technology itself. These impacts challenge traditional conceptual frameworks, and they involve not only user interactions with tools but also the broad ecosystem of AI production, which is often invisible to the user. For example, the data used to train models, the outputs they generate, and the inferences they draw can all endanger privacy—a pillar of democracy that ensures individuals the "space to think, speak, and develop their voice."[13] AI's privacy risks are growing in scope thanks to recent advances, and they include but are broader than the hazards presented by particular systems likely to put data in authoritarian hands (most prominently technologies produced by PRC-based companies).

AI presents a complex array of risks and harms—near-, mid-, and long-term—that are evolving with the technology itself.

Other fundamental democratic principles such as government accountability, equality under the law, and labor rights are also implicated in AI development. Critically, many of these challenges do not lend themselves to straightforward technological solutions. The measures needed to address them will be social and political as much as technical, and in some cases demand complex trade-offs between competing values.

"In order to democratize AI, we first need to have a proper discussion on what that means in terms of data governance: How data is created and distributed, how privacy laws and open data are regulated, and how data quality can affect AI. The CSOs working on digital rights, open data, and privacy have many lessons to add to this discussion."

— Natalia Carfi, Open Data Charter (Argentina)

AI systems present complex and evolving challenges to democratic principles

- AI models can endanger privacy in ways not foreseen by traditional concepts of data protection (which emphasize a specific category of "personally identifiable information"). These systems can piece together other types of data, such as location—even when anonymized—to determine someone's identity or the demographic group to which they belong, enabling algorithmic discrimination. Recent AI advances also undermine the foundations of online anonymity, long a valuable shield for dissidents facing repression and harassment, by making it possible to determine personal attributes of an author based on subtle textual cues.
- Though often misleadingly hailed as impartial, algorithmic systems can end up amplifying bias and exclusion. Trained to recognize common patterns and associations, AI tools often do not work appropriately for users whose situations fall too far from the statistical mean. The algorithmic distribution of public benefits, for instance, can leave behind people whose circumstances are not adequately captured by the model, who lack digital IDs,[14] or who are flagged as fraud risks falsely.[15] Since training data and design choices (e.g., what variable to optimize for) reflect social inequalities, members of marginalized groups are more likely to be misidentified by facial-recognition cameras or penalized by automated hiring systems.
- The current direction of AI development—with LLMs enabling more use of qualitive data and organizations stacking their own systems on top of these "foundation models"—creates new opportunities for the embedding of human biases. These same trends amplify the challenge of explainability and make it harder to assign responsibility if something goes wrong. Taken together, these factors can jeopardize citizens' right to fair and accountable decision making.

- AI systems used as labor management tools, whether in the gig economy or by traditional managers, can pose new challenges to labor rights. One participant recounted an instance where a delivery worker was penalized by an algorithmic management tool for stopping in an accident. In such cases, **the absence of a meaningful "human in the loop" can make it challenging to appeal wrongful penalties.** Labor rights issues also arise during the training of AI models, as when contracted "crowdworkers" in global majority countries who label data and moderate content face low pay, arbitrary management, and psychological harm from the work they perform.

Democratic values can point in conflicting directions with regard to AI governance

- Addressing these wide-ranging risks and harms requires more than just technological strategies. Computational strategies to "de-bias" systems will not address deeper concerns of fairness rooted in the social context where these tools are being used. Moreover, they may fail to work even on a technical level if developers fail to recognize how deeply embedded biases are in the assumptions underlying a model's design. *Transparency* is needed around the full infrastructure of systems and the process whereby they are developed or adopted—meaning not just source code, but also data, ethical procedures, stakeholder consultation, and contracts.
- **Given these complex demands, engaging civil society and prioritizing democratic values, while crucial, will not yield simple answers on mitigating AI harms.** Democratic principles can be in tension: For instance, privacy benefits when systems collect only the minimum data required ("data minimization"), but equity may be better served by collecting sensitive demographic data in order to be able to test for bias. Similarly, closed models that keep AI development within a few large companies raise concerns about opacity and the concentration of power. Yet open models might more easily be coopted for antidemocratic projects, such as generating hate speech; smaller entrepreneurs might have fewer resources to invest in mitigating AI risks and harms. Given these value conflicts, prodemocratic actors have valid disagreements about AI policy.
- If digital policies and regulations are not carefully tailored, governments and malign actors can abuse them for purposes contrary to democratic values (as with officials in Brazil[16] seeking to resist sharing public information, or kleptocratic enablers[17] attempting to chill critical reporting).
- Although some challenges are global in nature, vulnerabilities, priorities, and ways of relating to AI will differ across communities. Digital and economic divides, for example, affect the opportunities people have for to join conversations about AI governance, but also the relative importance they place on this issue compared to other challenges (such as internet access or basic labor rights).

OBSTACLES TO ENGAGEMENT

Institutional and public attention to AI is growing, with extensive media commentary, national and global regulatory discussions, and civil society initiatives to deepen understanding of the challenge and advocate for human rights. **Efforts to apply democratic principles and processes to AI, however, crash up against both conceptual challenges that impede understanding of these technologies and structural challenges that impede access to decision-making fora.** Power imbalances that place civil society at a disadvantage vis-à-vis developers contribute to these obstacles, as does the novelty of the AI governance challenge, which can strain existing conceptual and institutional frameworks. The following reflections outline key challenges that may arise in applying democratic norms to the AI space.

Understanding AI and Its Impacts Can Be Challenging

In conceptual terms, AI can be a difficult object to define, map, and ultimately govern. Despite a flurry of conversation around ChatGPT and speculation about AI's long-term implications, **many of the ways in which AI tools are already transforming social and political landscapes are far from obvious**. Systems from social media recommendation algorithms to public surveillance cameras function in the background of our digital or physical lives, and governments and companies which deploy them are often reluctant to disclose details. Mapping AI use and harms requires multidisciplinary expertise, spanning technical and social fields, that is beyond the individual capacities of most CSOs.

Moreover, **some of the modes in which AI is currently discussed actively impede engagement**. Participants felt that popular commentary tends to fall at the far ends of the spectrum, either treating AI as a silver bullet able to provide ready-made solutions to complex social and economic problems or predicting imminent doom.[18] Narratives centering development and efficiency can crowd out attention to limits and guardrails, leading governments to embrace AI systems with little scrutiny. Simplistic narratives and opaque institutions, alongside the complexity of the technology itself, all make it challenging to define the stakes for democracy clearly.

> "While the perils of AI are increasingly pervasive, sometimes its impacts are gradual and diffuse. Civil society organizations, journalists, and other like-minded stakeholders can counteract this lack of visibility by showing concrete cases where people's behavior and lives are affected."
>
> — Eduardo Ferreyra, Asociación por los Derechos Civiles (Argentina)

AI uses and AI harms are often difficult to see

- Civil society and the general public often do not know when, where, or how AI systems are in use. AI explainability presents an inherent technical challenge, with systems having become complex enough that even developers struggle to unpack why models arrive at particular conclusions. On the social side, opaque dealmaking and complex re-seller ecosystems can obscure the commercial relationships behind AI deployments.[19] Intellectual property (IP) protections are often privileged over transparency, even when systems are used for sensitive public functions. **Moreover, too much emphasis on the "black box" nature of AI systems may close off discussion on those elements we *can* scrutinize**—such as AI development and deployment processes, the actors involved, and the impacts on communities.
- While some AI harms are readily apparent, others are not, especially when these issues involve diffuse impacts such as changes to public behavior due to awareness of being surveilled. Advocates may struggle to call attention to dangers in between the immediate (damages to an individual, as with misidentification by a facial-recognition tool) and the distant (runaway "superintelligent" AI), or to find a suitable accountability framework to address more distributed harms.
- Existing conceptual frameworks may be poorly suited to understanding some of AI's transformative impacts. For instance, linking privacy to an individual's personal home or belongings can obscure the harms that emerge as AI makes public spaces and society writ large easier for governments, companies, and others to scrutinize. As theorists of collective data rights have noted, people

or communities may be harmed by the inferences companies draw and the power they acquire using other people's data, even if those others consent to this use.[20]

Popular narratives, framings, and vocabularies hinder understanding of AI risks and harms

- Popular narratives can obscure the complex ways in which AI systems affect the playing field for democracy. For example, these accounts may misattribute agency to systems themselves, rather than the people who design and deploy them (some participants saw this tendency as inherent in the term "accountable AI" or even "AI" itself). Media coverage came under particular criticism for relying too much on narratives from a handful of AI "godfathers," and veering between consumerism and talk of existential risk. Journalists were seen as disproportionately preoccupied with risks AI systems might pose to their own jobs. Even within civil society, some felt that the range of perspectives explored is limited by the preferred narratives of tech policy funders.[21]
- Publics and governments are often inclined to focus on the convenience, efficiency, labor savings, or entertainment offered by AI systems. Technosolutionism (a reflexive belief that technical fixes hold the answer to social challenges) remains widespread. Politicians may be reluctant to stop and consider harms because they want to show constituents they are doing something (e.g., by adopting predictive policing technologies when there is a high-profile crime). **Users in the moment may be focused more on immediate convenience than on down-the-road concerns such as where their data will go, or they may simply have no choice other than to use AI systems.**
- Stakeholders still lack a common, accessible vocabulary to discuss AI benefits and harms. Terms used to describe desirable qualities in AI, for instance, have different, narrower connotations in the technical community than they do in common parlance or policy conversations. In technical communities, "trustworthy AI" often signifies speed, accuracy, and even social acceptance rather than fairness. Among the public, "explainable AI" means the ability to explain the workings of a system in plain text, whereas among computer scientists, it means the decipherability of algorithms (XAI).

Institutional Gaps and Asymmetries Hinder Democratic Action

Despite the wide-ranging impacts of AI technologies on people's relationships with governments and one another, participants felt that current institutions fall short of giving affected people and communities a meaningful say in setting AI norms—whether at the legislative and policy level or within companies and the technical community. Across many democratic institutions, the competencies and procedures needed to effectively manage AI harms are still nascent, if not entirely lacking. Informational asymmetries mean that members of the public

Across many democratic institutions, the competencies and procedures needed to effectively manage AI harms are still nascent, if not entirely lacking.

and their democratic representatives are at a disadvantage when seeking to regulate, purchase, or simply use AI systems.[22] Moreover, key AI governance conversations still exclude civil society groups and marginalized communities. In principle, traditional democratic guardrails such as open procurement as well as innovations such as algorithmic impact assessments (AIAs) both can help to mitigate AI-related human rights harms. Yet, particularly amid global democratic backsliding, loopholes, institutional shortcomings, and back-channel dealings can hollow out these constraints.

> "The current situation means that there is a big asymmetry. We need multistakeholder engagement, but the capabilities of the state, academia or civil society are so far behind that we seem condemned to deal with the consequences [of AI development] and not to think about how to change the initial logic."
>
> — Carolina Botero, Fundación Karisma (Colombia)

Institutional gaps and resource constraints impede effective action on AI governance

- Private companies can pay more to retain talent and have exclusive access to proprietary information. This informational asymmetry places governments and CSOs at a disadvantage as both shapers of AI norms and customers for AI products: On the first front, CSO representatives felt themselves to be competing with better-resourced companies that dominate the conversation on AI laws and norms. On the second, CSOs and public agencies sometimes end up procuring AI tools which are promoted by vendors, but not necessarily aligned with client needs.
- Due to the novelty of AI issues, institutions within government often still need to work out who is responsible for handling them. Government agencies may outsource various aspects of AI procurement (such as designing requests for proposals and AIAs) to companies, despite the conflict of interest this dynamic presents. Legislatures can be uncomfortable addressing technical topics or unequipped to do so. Specialized institutions that might add clarity—such as processes to allow for audits or a scorecard to evaluate how systems are built and trained—are usually lacking. **Even where requirements to conduct AIAs or follow privacy-by-design principles exist on the books, officials may lack the training and resources to follow these guidelines.**
- Loopholes can hollow out nominal protections for privacy, transparency, and other democratic principles, as can a lack of leverage or enforcement mechanisms that would put real power behind these guidelines. Irregular relationships or transactions with government clients (such as free trials), for instance, allow vendors to circumvent public procurement rules.[23]

State-security carveouts may mean that digital privacy laws do little to prevent repressive applications of predictive policing technologies or biometric surveillance tools. Where data protection impact assessments are not public by default, developers have little incentive to actually mitigate any risks they identify. Requirements for consent to data collection—often liable to become formalities—may have especially little impact when physical spaces where people have no meaningful opportunity to withhold consent (such as refugee camps) are used as AI testing grounds.

- Finally, some regulatory guidelines and policies may unduly emphasize *process* (the mere fact of consulting civil society or affected communities) over *outcomes* (whether such input results in any meaningful action). Some civil society groups were hesitant to engage with companies in assessing new digital systems because they found that developers used such involvement as a token of legitimacy, yet continued to disregard CSO recommendations.

CSOs and vulnerable communities face barriers to engagement

- Civil society participants noted that some fora where AI governance is discussed (such as trade negotiations) do not traditionally include civil society, and some governments were uninterested in engaging. Even some "multistakeholder" consultations were seen to involve simply bringing in academics with unrepresentative views. **Several participants cited a disconnect between digital rights advocates working on AI policy, and the traditional human rights groups that might be better positioned to frame the policy agenda.** On a more foundational level, participants charged that decision makers often failed to recognize the knowledge that marginalized groups (such as African diaspora communities) possess about AI and algorithmic harms, resulting in the erasure of critical perspectives.

> "[AI governance] requires multi-disciplinary, co-ordinated expertise that cuts across silos—that is not currently natural to civil society. We're working within the realm of our reality, as labor rights, human rights organizations, for example. But we need a broad look at AI governance and how it impacts our lives, building on the strengths of siloed expertise."
>
> — Vidushi Marda, REAL ML, (India)

- Participants were concerned by the **lack of engagement between civil society and the private sector**. Some attributed this situation to private sector disinterest in joining civil society fora and to the many barriers to CSO engagement in the AI development process, especially for organizations from the global majority. One participant shared their difficulties gaining access to policy deliberations at the distant headquarters of a multinational company; another suggested that a lack of training in ethics and governance issues might leave the technical community less attuned to rights and democracy concerns. A few participants felt that CSOs needed to find ways to engage the private sector more effectively, given the latter's outsized role in shaping the evolution of AI.
- CSOs seeking to develop their own AI tools have thus far faced an uphill struggle: As with many civic tech projects, resource constraints make it difficult to ensure sustainability, and a lack of high-quality datasets relevant to the geographic and thematic contexts where activists work exacerbates this challenge. Global-majority clients must do extra work to make commercial tools such as chatbots fit for their purposes (for instance, by functioning effectively in languages other than English, especially lower-resourced languages and dialects). The quantity and quality of information available about AI systems also varies across languages. Moreover, absent clear normative guidance on AI, some rights-conscious CSOs may be hesitant to adopt AI tools.

IDEAS FOR COMMUNICATION, AWARENESS-RAISING, AND ACCOUNTABILITY

What strategies for networking, communication, and engagement in digital design hold promise for bringing democratic principles closer to center of AI development? While the current global momentum toward legislation and norm-crafting on AI and other automated decision making systems (ADMs) presents opportunities to elevate democratic principles, the task ahead is complex. AI governance is a challenge at many different levels, from regulation to company policies. One participant stressed the need to find opportunities for ongoing public engagement on AI rather than simply delegating the task to legislators, since "democracy does not end with elections."

Civil society leaders are already pioneering approaches that range from strategic litigation and creative public communication, to tailored trainings, to deepening CSOs' capacities to develop their own AI tools and model democratic accountability. However, participants widely perceived a need for greater collaboration, capacity building, and amplification of these efforts.

Key Fronts for Engagement on AI Norms

Applying democratic norms to AI governance is a task that cuts across the private sector, government, different segments of civil society, and the general public. For CSOs, potential avenues of engagement include awareness-raising, strategic litigation, engagement with government institutions on laws and policies, and promoting responsible approaches to development. Strategic

communication can help convey the importance of democratic AI norms to government interlocutors and the wider public. Traditional as well as specialized governance mechanisms such as rules for AI procurement can ensure that democratic principles are applied across administrations. **CSOs with strong technical capacities can bring these skills to bear to assess AI harms, or go on the offense by pursuing new directions in AI development.** The following reflections outline key ways in which new thinking, policies, and approaches might move the needle on AI development, as well as strategies to make mechanisms already in place more robust and participatory.

> "It is all too easy, even in a participatory democracy, to see AI as a way to reduce the messiness of democracy. Because AI can automate out public involvement, government needs to ensure that the public has an ongoing role to potentially influence AI policy and protect human engagement."
>
> — Renee Sieber, McGill University (Canada)

Communicate strategically about AI rights impacts

- Since it can be challenging to communicate to the public about diffuse impacts such as erosions of privacy or unaccountable decision making, advocates found it useful to leverage specific events of concern in the headlines—such as celebrity data leaks or legal cases[24]—as touchstones for broader conversations. In Argentina, for instance, activists seized the moment created by the widely publicized expert "letter" calling for a six-month AI "pause" to engage with tech researchers. On-the-ground approaches can also help messages to break through; the SHARE Foundation in Serbia, for example, has done creative work with a public art installation that conveys the sense of being surveilled.[25]

- Despite the new challenges AI presents, rooting discussion in familiar democratic values can help to illuminate the stakes. For instance, **if a government agency cannot explain a decision it has made with the help of an AI system, then such a decision violates principles of due process and government accountability that are enshrined in many democracies' constitutional frameworks.** Some participants also felt that publics were particularly responsive to messages emphasizing business irregularities around AI procurement, such as corruption risks and high costs.
- One participant argued that to avoid having their messages dismissed, activists need to meet people where they are and communicate in a balanced way about harms, recognizing that people see AI tools as "fun" and that governments are enthusiastic about efficiency gains. Formulating a positive, democratic digital agenda (beyond "just saying no") is one component of this approach. Such pragmatic strategies might also involve recognizing domestic political incentives, engaging with officials at different points on the political spectrum, and focusing in on specific pieces of the AI governance puzzle that prove amenable to action at a given moment.

Leverage existing democratic institutions while building new ones

- Existing laws, especially around privacy and data governance, offer a basis for challenging rights-violating applications. Strategic litigation (as with facial recognition in Buenos Aires), potentially engaging data protection authorities, or class actions in defense of vulnerable groups can both set legal precedents and challenge misconceptions about AI.
- Traditional mechanisms for government transparency and accountability also have important applications in this field. Access to information policies (to the extent that officials abide by them) can be an asset when monitoring AI in the public sector. **Democracies can leverage public procurement as a site for ensuring that AI adoption follows human rights guidelines, introducing audits, or potentially penalizing companies whose products fuel digital authoritarianism abroad.**[26] Where governments set rules for AI systems in the public sector, these directives may provide normative guidelines for responsible development in the wider society. CSOs can help to level up governments' capacity to address AI issues by providing targeted trainings for officials.
- New institutions and approaches such as public repositories of information on algorithmic harms; requirements for third-party AI audits; and support mechanisms for vulnerable communities also have roles to play in shoring up AI accountability. Experimenting with AI tools in contained spaces (such as sandboxes where the use of specific data sets can be tested, then dropped if it proves too difficult to protect privacy) before public deployment can help to protect people's rights, although there is also a risk of communities being selected for "sandbox" testing without meaningful consent.[27] Several participants argued that legally binding regulation on AI,

as opposed to "soft law" in the form of normative guidelines followed by companies, was critical to ensure that developers and deployers follow human-rights principles.

- Some corporations have conducted initiatives for focused discussion across civil society, academia, and the public and private sectors about AI impacts. Additional research, potentially drawing on ideas from within the tech community and self-regulation models, can help to make ideas like privacy-by-design and algorithmic transparency more concrete. New initiatives, such as the South Africa–based Global Index on Responsible AI, are emerging that center global-majority and human rights perspectives.[39]

Leverage technical knowledge in the civil society space

- For CSOs with limited influence on powerful foreign companies, internal technical capacities can provide an alternate entry point to the AI development world. CSOs can pinpoint the vulnerabilities of government or corporate systems; model more inclusive, representative, and responsible approaches to design; and develop AI tools expressly intended to support civic activity. One participant noted that organizations with experience using AI to track malign information operations online might serve as resources on this technology for others in civil society.
- To conduct assessments of public AI infrastructures, civil society experts might audit source code, build their own systems on top, or analyze information from data leaks. CSOs can also identify vulnerabilities, biases, and other rights risks in corporate systems, through official pressure-testing ("red-teaming") of corporate AI products or by designing generative adversarial networks (GANS) to "break" these systems. Some civil society groups have produced specialized, easy-to-understand digital tools for evaluating AI bias,[28] or to identify when AI systems are being used.[29] These tools can empower other CSOs and affected communities to engage on AI governance regardless of technical expertise or direct access to companies.
- CSO-led projects have explored new, participatory approaches to AI design for the public good.[30] Open data activists are considering how datasets specially curated for civic purposes in the Global South might result in tools that better serve democratic institutions. **From Hungary[31] to Brazil[32] and Peru,[33] CSOs working for accountability have designed AI tools to help citizens make sense of public information or identify indicators of corruption.** AI tools can also be a resource for mapping power networks. Such projects can even help to counter information asymmetries around AI itself—for instance, by enabling researchers to identify facial recognition purchases in procurement documents. Meanwhile, academic and private-sector researchers are exploring the use of AI for "collective intelligence," enabling new forms of public engagement in decision making. Civic tech initiatives can help scale such projects and lend them visibility.[34]

Public institutions and CSOs can model responsible approaches to AI development

- Participants emphasized that responsible development involves first carefully assessing whether AI is right for a given project, and whether the organization is in a position to implement it successfully (e.g., are there relevant labeled datasets to train the model? Does the organization have somewhere to store data outputs? What are the potential harms?) Sometimes, this assessment may lead to the conclusion that the best choice is simply not implementing the system at all. Similarly, officials and project managers will need to make judgment calls about the line between intrusive surveillance and socially valuable data collection—for instance, to help communities more effectively address health and safety issues, environmental risks, and other pressing social challenges. As one participant noted, "Not everything needs to be a dataset."
- When collaborating with developers, participants stressed, it is important for CSO and government clients to understand the technology and its risks, consider privacy and data security, and invest in infrastructure to make projects sustainable. Clients should inspect both data inputs and system outcomes. To avoid vendor lock-in and uphold norms for responsible and rights-respecting development, they ideally might set conditions for their private-sector partners (for instance, that code must be open source, auditable, and interoperable with other platforms). Given the previously mentioned asymmetries facing governments and civil society institutions in their interactions with the private sector, these recommendations may require capacity-building, or innovative efforts to articulate common standards for public-sector tech.[35]
- **Including people and communities likely to be impacted from the ground up when building new systems, rather than waiting for adverse impacts, can help to ensure more robust rights protections.** Civil society participation can help ensure the effectiveness of AIAs or data protection impact assessments, as can incentivizing companies to make them public (for example, through rankings) and making these assessments part of a continuous cycle, involving the review of outputs and not just inputs. Impact assessments can be linked to direct engagement with affected communities and their lived experience: Even where it's not possible to explain exactly how specific AI systems work, decision makers can benefit from hearing what people have to say about how systems affect their lives. Finally, it is important to ensure that these assessments reach the people who are actually in a position to make decisions about projects.

Opportunities for Cross-Sectoral Collaboration

As AI governance challenges touch on many different aspects of social and political life, CSOs will need to forge new partnerships and knowledge-sharing initiatives. These initiatives might include collaborating strategically with independent journalists, lawyers, and labor unions; engaging affected communities directly; and closing divides between traditional and digital human rights groups. **Such collaborations can close gaps in knowledge-sharing on AI, providing a fuller picture of the intersection between emerging technologies and democratic norms.** They can also offset the resource asymmetries confronting CSOs and facilitate effective engagement in AI norms advocacy.

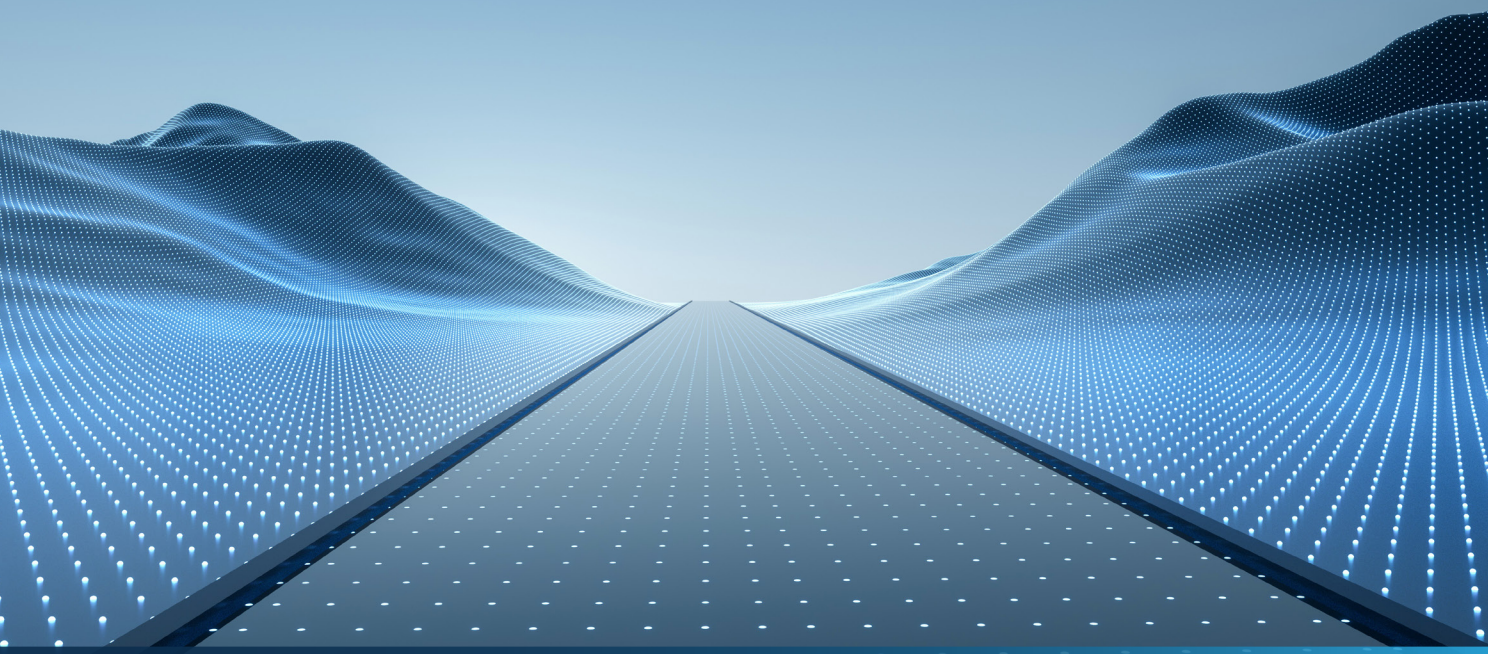
> "It is vital to forge a networked approach to AI governance, rather than relying solely on the private and public sectors as enforcers. Academia and civil society have a critical role to play as watchdogs, producing research and carrying out civic audits in order to reduce the asymmetry of information on the benefits and risks from AI deployments."
>
> — Bruno Bioni, Data Privacy (Brazil)

Identifying potential partners

- CSOs have formed impactful partnerships with rights-minded professionals in "gatekeeper" positions, such as journalists, lawyers, academic researchers, and teachers.[36] Such cooperation might entail launching strategic litigation, exerting intellectual pressure through advocacy coalitions, raising awareness among students and society writ-large, or providing data that yields a more realistic view of AI systems. Participants emphasized that independent or specialist media, even if less widely followed than mainstream outlets, were also more open to featuring sober discussions of AI.
- Many participants felt it was desirable to bring unions deeper into AI governance conversations, given their political strength in Latin America and the many impacts of AI systems on labor. Several felt that traditional human rights groups could be more closely engaged in AI discussions. Other potential collaborators include small businesses, which might support a more open and transparent approach to government acquisition of digital systems.
- Participants emphasized the need to broaden conversations about AI and recognize nontraditional forms of expertise—knowledge from those on the "receiving end" of AI (e.g., ride-hailing drivers with Uber or Lyft), for instance, or the qualitative evidence of discrimination collected by projects such as Fairwork.[37]

Leveraging collaborations

- Opportunities to level up on AI knowledge are important for many potential partners, and some digital rights groups have already taken the initiative by bringing trainings to newsrooms or legal offices. Traditional CSOs still grappling with last-generation tech challenges (like social media impacts) may also benefit from trainings that better position them to field questions on AI from governments or the public. Understanding how to interact with systems like ChatGPT safely and effectively may become part of basic digital trainings for civil society.
- Partnerships can amplify the effectiveness of advocacy on AI and human rights. Digital rights groups that forge coalitions with traditional human rights groups, as well as other prodemocratic actors, can leverage their partners' relationships with government institutions.[38] CSOs that lack the resources to be everywhere at once can collaborate to engage across the many different forums in the UN system, OECD, EU, Open Government Partnership, and beyond where AI governance conversations take place. Short-duration, low-lift actions (such as a protest on a single day) can also be a fruitful approach when non-digital groups struggle to find the bandwidth to engage on AI.
- Knowledge-sharing is another benefit of collaboration. **CSOs can work together to map different dimensions of the problem, learn what approaches have and haven't worked for others, and gain a fuller understanding of the conversation (for example, with open data advocates also learning to think about privacy).** Groups that do not focus mainly on digital issues can bring to bear subject matter knowledge relevant to specific AI harms, for instance on racial justice, especially within the framework of sector-specific discussions of AI. Models such as environmental impact assessments can offer insights for applying human rights guidelines to AI systems.
- Engagement in a variety of global fora, in the view of one participant, can provide CSOs based in global majority countries with an opportunity to "live in the future," addressing issues that are just over the horizon in their own home countries. Such engagement offers a chance to think ahead and strategize about how to defend vulnerable populations.



CONCLUSION

The preceding reflections underscore that the AI governance challenge is closely connected to the vibrancy of democratic principles in societies where AI technologies are developed and deployed. **As AI use grows more pervasive, our expectations of privacy, access to public goods, and opportunities to challenge injustice from the courtroom to the workplace are likely to increasingly depend on the rules and norms we establish for AI systems. At the same time, the ways in which AI impacts us will depend on how well democratic mechanisms are working to uphold government transparency, support deliberation, and engage affected communities in decision making.** AI's trajectory depends in part on the health of democratic institutions, and the health of democracy will be affected by our choices around AI.

The novelty and complexity of AI technologies, as well as the knowledge and power asymmetries involved in their production, make this issue an especially challenging front for civil society engagement. Nonetheless, CSO leaders are already pioneering promising approaches to deepening awareness around AI harms and establishing new legal, social, and technical safeguards. Whether by training professional gatekeepers who shape public opinion or by modeling rights-respecting approaches to AI deployment, civil society has an important role to play in determining how democratic societies will utilize and live with AI.

The complex intersections of AI and democracy are far too broad to be covered comprehensively in any one conversation or set of conversations, particularly given the rapid evolution of AI systems themselves. The far-reaching implications of generative AI in the information space, for instance, fell largely outside the parameters of our discussion. Open-source models and the ability to process more qualitative data may alter the cost-benefit equation for organizations thinking of leveraging AI technologies. New categories of democratic risks may emerge as institutions deploy LLMs in new ways. We hope, however, that this report might provide an initial series of guideposts to promising opportunities for civil society engagement in AI, as well as the enduring relevance of democratic principles in this space.

ENDNOTES

The following references are provided for further reading and reflection on the point discussed in this report. They do not necessarily reflect the original sources for contributors during the workshop discussion.

1 Steve Feldstein, Eduardo Ferreyra, Danilo Krivokapić, and Beth Kerley, *The Global Struggle over AI Surveillance: Emerging Trends and Democratic Responses,* National Endowment for Democracy, 7 June 2022, www.ned.org/global-struggle-over-ai-surveillance-emerging-trends-democratic-responses/.

2 Beth Kerley, Roukaya Kasenally, Bárbara Simão, and Blenda Santos, *Smart Cities and Democratic Vulnerabilities,* National Endowment for Democracy, 15 December 2022, www.ned.org/smart-cities-and-democratic-vulnerabilities/.

3 Krzysztof Izdebski, Teona Turashvili, Haykuhi Harutyunyan, and Beth Kerley, *The Digitalization of Democracy: How Technology Is Changing Government Accountability,* National Endowment for Democracy, 27 March 2023, www.ned.org/digitalization-democracy-technology-changing-government-accountability/.

4 Larry Diamond, "Liberation Technology," *Journal of Democracy*, 21, 3 (July 2010): 69-83, www.journalofdemocracy.org/articles/liberation-technology/.

5 Feldstein et al., *The Global Struggle over AI Surveillance.*

6 Izdebski et al., *The Digitalization of Democracy.*

7 Agustina Del Campo, "Call for Papers on Global AI Governance: Office of the UN Secretary General's Envoy on Technology," Centro de Estudios en Libertad de Expresión y Acceso a la Información, 28 September 2023, https://observatoriolegislativocele.com/wp-content/uploads/CELE_ai_submission_v2.pdf,

8 "Huge 'Foundation Models' are Turbo-Charging AI Progress," *the Economist*, 11 June 2022, www.economist.com/interactive/briefing/2022/06/11/huge-foundation-models-are-turbo-charging-ai-progress.

9 Izdebski et al., *The Digitalization of Democracy.*

10 Jonathan E. Hillman and Maesea McCalpin, *Wathcing Huawei's "Safe Cities,"* Center for Strategic and International Studies, 4 November 2019, www.csis.org/analysis/watching-huaweis-safe-cities.

11 Feldstein et al., *The Global Struggle over AI Surveillance.*

12 Kerley et al., *Smart Cities and Democratic Vulnerabilities.*

13 "Privacy and Freedom of Expression in the Age of Artificial Intelligence," Article 19, April 2018, www.article19.org/wp-content/uploads/2018/04/Privacy-and-Freedom-of-Expression-In-the-Age-of-Artificial-Intelligence-1.pdf.

14 Quito Tsui and Teresa Perosa, "Digital Ids Rooted in Justice: Lived Experiences and Civil Society Advocacy Towards Better Systems," The Engine Room, January 2022, www.theengineroom.org/wp-content/uploads/2022/01/Engine-Room-Digital-ID-2022.pdf.

15 Matt Burgess, Evaline Schot, and Gabriel Geiger, "This Algorithm Could Ruin Your Life," 6 March 2023, *Wired*, www.wired.com/story/welfare-algorithms-discrimination/.

16 Bruno Bioni, Rafael Zanatta, and Fernanda Campagnucci, "LGPD and Transparency: It's Time to Hit the Pace," *Folha de São Paulo*, 4 May 2022, www1.folha.uol.com.br/opiniao/2022/05/lgpd-e-transparencia-e-hora-de-acertar-o-passo.shtml. (Original source material in Portuguese; for English-language summary, please see here: www.dataprivacybr.org/en/documentos/lgpd-and-transparency-its-time-to-hit-the-pace/).

17 Oliver Bullough, "Why Oligarchs Love European Data-Protection Laws," *the Economist* (1843 Magazine), 4 May 2022, www.economist.com/1843/2022/05/04/why-oligarchs-love-european-data-protection-laws.

18 Henry Farrell, Abraham Newman, and Jeremy Wallace, "Spirals of Delusion: How AI Distorts Decision-Making and Makes Dictators More Dangerous," *Foreign Affairs,* September/October 2022, www.foreignaffairs.com/world/spirals-delusion-artificial-intelligence-decision-making.

19 Gaspar Pisanu et al., "Surveillance Tech in Latin America: Made Abroad, Deployed at Home," Access Now, 10 August 2021, www.accessnow.org/cms/assets/uploads/2021/08/Surveillance-Tech-Latam-Report.pdf.

20 Martin Tisne, "Collective Data Rights Can Stop Big Tech from Obliterating Privacy: Protecting Individual Data Is Not Enough When the Harms Are Collective," *MIT Technology Review*, 25 May 2021, www.technologyreview.com/2021/05/25/1025297/collective-data-rights-big-tech-privacy/.

21 Juan Ortiz Freuler, Ana Brandusescu, and Will Orr, "Unpacking Funder Influence over Digital Rights Nonprofits: Reflections from a Workshop (Part 1)," Open Global Rights, 24 August 2023, www.openglobalrights.org/unpacking-funder-influence-digital-rights-nonprofits/.

22 "Privacy and Freedom of Expression in the Age of Artificial Intelligence."

23 Kerley et al., *Smart Cities and Democratic Vulnerabilities.*

24 Mike Moore, "Lionel Messi Personal Data Stolen and Leaked in Major Data Breach," Tech Radar Pro, 19 October 2021, www.techradar.com/news/lionel-messi-personal-data-stolen-and-leaked-in-major-data-breach.

25 Filip Milošević, "The Making of an Anti-Biometric Mass Surveillance Campaign," SHARE Foundation, November 2022, https://kit.exposingtheinvisible.org/en/anti-biometric.html.

26 Izdebski et al., *The Digitalization of Democracy.*

27 Helena Secaf, Eduardo Carrillo, and Nathan Paschaolini, "Technologies and Human Rights in the Triple Border Area: An Exploratory Study of the Security Programmes Muralha Inteligente (Brazil) and the Automated Migratory System for Facial Recognition (Paraguay)," The Association of Technology, Education, Development, Research and Communiaction (TEDIC), February 2023, www.tedic.org/wp-content/uploads/2023/02/Technologies-and-Human-Rights-in-the-Triple-Border-Area.pdf.

28 "Workshop en la Cumbre Mundial Rightscon," Fundación Vía Libre, 8 June 2023, www.vialibre.org.ar/workshop-en-la-cumbre-mundial-rightscon/. (Original source material in Spanish).

29 For more information, please consult the "Algorithmic Equity Toolkit," ACLU Washington, www.aclu-wa.org/AEKit.

30 To see an example, please see ILDA's information page about the "Empatía" project: https://idatosabiertos.org/en/proyectos/english-empatia/.

31 For more information, please consult Red Flag's information page: www.redflags.eu.

32 For more information, please see Querido Diáro's website: https://queridodiario.ok.org.br/. (Original source material in Portuguese).

33 For more information, please view this instructional video on YouTube, posted by POLIS (affiliated with the London School of Economics): www.youtube.com/watch?v=xipAH7Cm2SA.

34 For an example of one of these civic tech initiatives, please view this webpage maintained by Democracia Digital: www.democraciadigital.pe/observatorio/.

35 Kerley et al., *Smart Cities and Democratic Vulnerabilities.*

36 "Iniciativa Tecla lança repositório de práticas pedagógicas e tecnologias no combate ao racismo e discriminação," Ação Educativa, 1 December 2022, https://acaoeducativa.org.br/iniciativa-tecla-lanca-repositorio-de-praticas-pedagogicas-e-tecnologias-no-combate-ao-racismo-e-discriminacao/. (Original source material in Portuguese).

37 For more information, please visit Fairwork's website: https://fair.work/en/fw/homepage/.

38 Eduardo Ferreyra, "Bridging the Gap between the Digital and Human Rights Communities," *Power 3.0,* 25 October 2022, www.power3point0.org/2022/10/25/bridging-the-gap-between-the-digital-and-human-rights-communities/.

39 For more information, please consult the "Global Index on Responsible AI" webpage, maintained by Data for Development: www.responsibleaiindex.org.

ABOUT THE EDITOR

Beth Kerley is a program officer with the research and conferences section of the National Endowment for Democracy's International Forum for Democratic Studies. She manages the Forum's emerging technologies portfolio, which covers the challenges and opportunities for democracy as technological advances in areas such as machine learning, the Internet of Things, and big-data analytics supply new tools of politics and governance. She was previously associate editor of the *Journal of Democracy*, and holds a PhD in History from Harvard University and a Bachelor of Science in Foreign Service from Georgetown University.

ACKNOWLEDGMENTS

Above all, the editor would like to thank the amazing participants at the Forum's May 2023 workshop, whether or not expressly named, for the contributions that ultimately resulted in this report. Credit for the creative insights and suggestions shared here belongs to them, although the report's framing reflects our editorial choices and should not be taken to indicate a consensus among the group. The editor is also grateful for the contributions of the International Forum's staff and leadership, including Christopher Walker, John K. Glenn, Kevin Sheives, John Engelken, Amaris Rancy, and Maya Recanati, all of whom played important roles in the editing and publication of this paper. The editor is also particularly grateful to Aubra Anthony, Eduardo Bertoni, and Dr. Renee Sieber for lending their expertise and knowledge to further sharpen the analysis presented in this report. Finally, the Forum wishes to thank Factor3 Digital for their efforts and invaluable support in producing graphical elements and designing this report for publication.

PHOTO CREDITS

Cover image: Photo by LuckyStep/Shutterstock

Page 2: Photo by pluie_r/Shutterstock

Page 5: Photo by Login/Shutterstock

Page 10: Photo by Stefan_Alfonso/Getty Images

Page 16: Photo by Ikon Images/Shutterstock

Page 23: Photo by Jason marz/Getty Images

FORUM | INTERNATIONAL FORUM FOR DEMOCRATIC STUDIES

The International Forum for Democratic Studies at the National Endowment for Democracy (NED) is a leading center for analysis and discussion of the theory and practice of democracy around the world. The Forum complements NED's core mission—assisting civil society groups abroad in their efforts to foster and strengthen democracy—by linking the academic community with activists from across the globe. Through its multifaceted activities, the Forum responds to challenges facing countries around the world by analyzing opportunities for democratic transition, reform, and consolidation. The Forum pursues its goals through several interrelated initiatives: publishing the *Journal of Democracy*, the world's leading publication on the theory and practice of democracy; hosting fellowship programs for international democracy activists, journalists, and scholars; coordinating a global network of think tanks; and undertaking a diverse range of analytical initiatives to explore critical themes relating to democratic development.

NED | NATIONAL ENDOWMENT FOR DEMOCRACY

SUPPORTING FREEDOM AROUND THE WORLD

The National Endowment for Democracy (NED) is a private, nonprofit foundation dedicated to the growth and strengthening of democratic institutions around the world. Each year, NED makes more than 1,700 grants to support the projects of nongovernmental groups abroad who are working for democratic goals in more than 90 countries. Since its founding in 1983, the Endowment has remained on the leading edge of democratic struggles everywhere, while evolving into a multifaceted institution that is a hub of activity, resources, and intellectual exchange for activists, practitioners, and scholars of democracy the world over.

1201 Pennsylvania Avenue, NW
Suite 1100
Washington, DC 20004
(202) 378-9700

@thinkdemocracy

ThinkDemocracy