Emerging Global Challenges to Democracy: Leveraging Technology for Democracy

New and emerging challenges to democracy have arisen in recent years that are driving political development in countries around the world. Amid global shifts in the information, financial, and technological landscapes, open societies face the erosion of familiar democratic guardrails, while autocrats have found ways to weaponize new digital capabilities and cross-border ties. Democracy's supporters must develop local responses to globally driven challenges—including those associated with sweeping technological change—that are moving with extraordinary speed. To begin addressing the systemic drivers of democratic decline, democrats need to cultivate new forms of collaboration, knowledge-sharing, and innovation.

The Challenge:

Digital authoritarianism is challenging democracy. Contrary to predictions made when new technologies first emerged as tools of protest in closed societies, digital advances have not simply translated into gains for freedom. Increasingly, cutting-edge tools like artificial intelligence (AI)-powered systems for analyzing speech or recognizing faces are becoming widely available and used to deepen state surveillance, to tighten control over the internet, and to shift global norms in ways that legitimize digital repression.

The People's Republic of China (PRC), in particular, is pushing the boundaries of digital totalitarianism at home while exporting advanced digital tools and infrastructure to every continent. As emerging technologies spread globally to young or struggling democracies, these patterns are producing new risks linked to the erosion of privacy, the opaque sale and operation of many digital tools, and the unbalanced relationships between local democratic institutions and foreign vendors—especially those based in authoritarian settings. They are intersecting with older risks stemming from democratic backsliding and executive overreach, legacies of inequality, and shortfalls in transparency and accountability. With global technology norms currently unsettled, few guardrails against these threats to democratic principles are in place.

At the same time, both existing and emerging technologies represent opportunities that the democracy support community cannot afford to neglect. AI tools, for instance, may be a boon for state surveillance, but they are also enabling grassroots groups to monitor corruption risks, track narratives online, and stay one step ahead of government censors. They offer new ways to facilitate civic discussion and government engagement with the governed. Civil society currently faces resource and capacity constraints that impede leveraging the potential of AI to scrutinize government conduct or foster civic participation. Open societies confront the challenge of constraining digital authoritarian actors and practices while also facilitating innovations that will make new digital tools work for democracy. How they address these risks and opportunities could decisively affect the trajectory of countries on the threshold between democracy and authoritarianism.

State of Play:

As advanced digital tools—from advanced surveillance systems to generative AI software that produces text or images—grow in power and availability, democracies, autocracies, and "swing states" alike are seeking to set the norms for technology use and development. Both the development of new systems and the proliferation of existing ones raise fundamental questions about the protection of privacy; information integrity; and the challenge of ensuring transparency, accountability, and equity as automation transforms the practice of governance.

Most recently, the release of Open AI's ChatGPT, with its convincing ability to mimic human speech or writing, has set off a flurry of discussion about the implications of generative AI models, including their potential to supercharge authoritarian influence campaigns. The COVID-19 pandemic has left a legacy of expanded digital surveillance around the globe, with concerns in a range of settings that health surveillance measures are being repurposed for political ends. AI-powered surveillance tools such as facial recognition cameras—integral to China's draconian system of control over Uyghurs and other ethnic minorities in the East Turkistan, and now being used by authorities in Russia to track and arrest antiwar protesters—have spread to at least 97 countries.

> *"Faced with a fast-moving transformation that has its roots in globalized technology markets, democracy's supporters across regions and sectors must collaborate in new ways to confront digital authoritarianism, guard against unintended impacts, and leverage technology for democracy."*

The PRC is striving energetically to set global standards for emerging technologies such as 5G networks and facial recognition tools, with coordinated state and private efforts under the auspices of the "China Standards 2035" initiative; democracies are weighing how they can push back while still reaping the benefits of a pluralistic, multistakeholder approach to standard-setting. Beyond these formal efforts, the global popularity of PRC systems such as Huawei's "safe cities" is putting Beijing in a position to influence the de facto digital norms taking shape on the ground.

Democratic governments and civil societies are also starting work to establish normative guardrails in the digital space. Nonetheless, enabling participatory, informed, and principled decision making about the place of emerging technologies in democratic societies will require scaling up knowledge and capacity more broadly.

Key Principles for Response:

Faced with a fast-moving transformation rooted in globalized technology markets, democracy's supporters must collaborate in new ways to confront digital authoritarianism, guard against unintended impacts, and leverage technology for democracy.

Cultivating Partnerships and Collaboration: To respond to a challenge that is transnational in nature and increasingly blurs any arbitrary line between the physical and digital realms, civil society organizations will need to build new partnerships and coalitions. They should work more closely, for instance, with like-minded journalists, media, and international organizations to shed light on abuses of technology and opaque agreements between companies and governments. Deeper engagement between the digital rights and traditional human rights communities will be needed. These collaborations can generate public pressure on national and local governments.

Developing New Norms: Civil society voices are vital to ensuring that new national and international frameworks for data protection, AI governance, and other emerging areas of regulatory scrutiny uphold democratic principles for all segments of society. Experts within civil society can join discussions at the local, regional, and national level to inform policy makers and citizens. Civil society can also play a critical role in raising public awareness about government-contracted projects and highlighting threats to civil liberties.

Addressing Crucial Knowledge and Capacity Gaps: Increasing the capacity of grassroots civil society groups to develop and leverage emerging tech tools in their own work is an important part of making digital advances work for democracy. Like other aspects of the digital governance challenge, however, this will require addressing knowledge and capacity gaps, combatting the mystification of technology, and cultivating a sharper understanding of what emerging tech tools can and cannot do. Democratizing artificial intelligence, for instance, will involve identifying new ways to connect civil society groups to AI expertise, such as partnerships with academic institutions, cultivation of in-house expertise, and knowledge-sharing from trailblazer institutions. Efforts of this kind can not only help civil society groups to better contend with the challenge from networked digital authoritarians, but also contribute to raising the profile of human rights and democracy concerns in the digital design ecosystem.

Additional Resources:

Global Spread of AI-powered Surveillance: A 2022 Forum report examines the global spread of AI-powered surveillance tools, especially to "swing states" on the border between autocracy and democracy, and the struggle to craft prodemocratic norms around these systems' design, export, and application. Accompanying essays share grassroots perspectives from Serbia and Argentina on the challenge of tracking imported surveillance systems.

The Challenge of Digital "Smart Cities": A recent report examines how "smart city" projects for municipal digitalization can interest with democratic vulnerabilities absent adequate transparency, oversight, and public participation. A case study from Mauritius (with accompanying podcast) outlines governance irregularities and unanswered questions around a Huawei "Safe City" project, while contributors from Brazil describe national initiatives for democratic smart city governance and ongoing challenges on the ground.

Countering Authoritarian Digital Influence: Members of the Carnegie Endowment's Digital Democracy network discussed with the International Forum how authoritarian actors are pushing new regulatory models and seizing on technological advances to advance novel strategies for digital repression.