DIALOGUE SNAPSHOT

Technology & Democracy

April 2024

the Hollings Center
for international dialogue

Technology & Democracy

Digital transformation in societies – the increasing use of internet and technological solutions to everyday problems as well as governance issues - presents opportunities for increased access to and participation in civic life. The effects of new technologies have entered the political and social sphere. Democratic institutions continue to grapple with these effects. And, the risk of abuse by authoritarian regimes continues to grow. With numerous elections to take place globally in 2023 and 2024, the topic of the effect of technology and digital platforms on democratic institutions has returned to the forefront. Now, with the rapid deployment of big data, artificial intelligence, and social media growth, an analysis of the new landscape is critical. To address the questions, challenges, and potential of the intersection of technology and democracy, the Hollings Center for International Dialogue convened a group of experts to evaluate that landscape. The dialogue took place in Washington, D.C. in May 2023.

The exploration into the intersection of technology and democratic governance commenced with a focus on the promises and challenges associated with digital transformation. Participants engaged in a discussion on the potential of technology to enhance democratic participation and local governance. While acknowledging the benefits of technology in decision-making and civic interaction, concerns emerged regarding the growing disillusionment with the actual impact of these endeavors. The dialogue highlighted the global race for digitalization and lessons learned from diverse regions. However, the dual nature of technology emerged as a central theme, emphasizing the need for a nuanced understanding and comprehensive strategies to navigate the complex terrain.

The dialogue then shifted its focus to the pressing issue of digital threats to democracy. Participants collectively discussed how both autocratic regimes and democracies are leveraging digital technologies for control and suppression. The threats were categorized into three key areas: Blocking Content, Surveillance, and Digital Perception/ Misinformation. The indispensable role of civil society in addressing these challenges became evident, with participants emphasizing their role for raising awareness, providing evidence-based research, advocacy, support services, and transparency. Despite the challenges posed by the influence of major actors in the tech field, participants

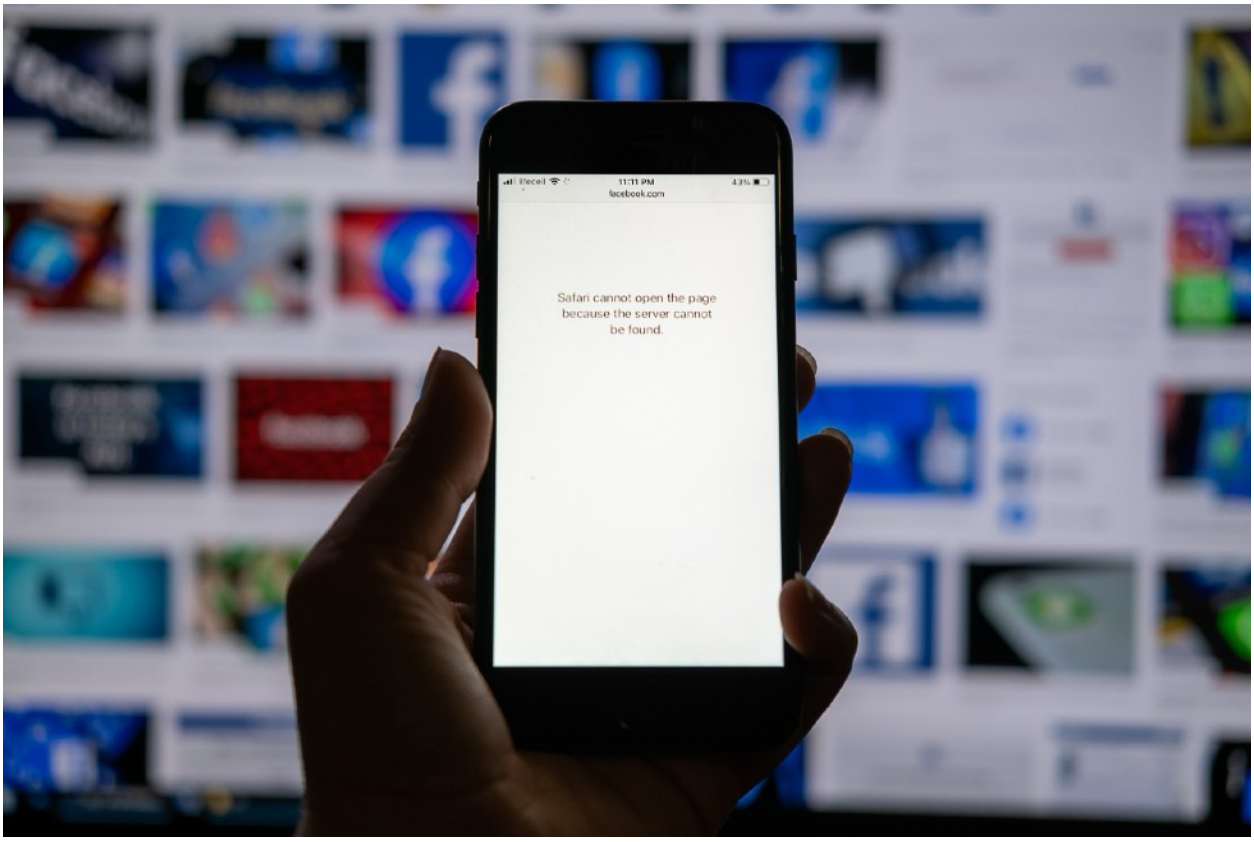
underscored the collective effort required to safeguard democratic values in the face of evolving digital threats.

Technology's Promise and Reality

The dialogue commenced with a discussion on the potential of digital transformation to enhance democratic participation and local governance. While global attention in recent years has focused predominantly on the peril of the integration of technology with democracy, some participants argued the importance of remembering the benefits technology in governance and civic interaction. Around the world, governments and municipalities are turning to digital technologies to improve in decision-making and address civic issues.

Participants collectively recognized the global race for digitalization, with a participant from Mauritius highlighting recent deployment of technology in support of digital governance. Initiatives such as the Open Government Partnership (OGP) were brought up, aimed at empowering citizens and combating corruption. Dialogue participants conveyed additional examples of lessons learned from this technological race with positive impact. Participants highlighted the Ukrainian Foreign Ministry's innovative solutions like e-declarations and anti-corruption schemes. They discussed technology as a means to bypass authoritarian control of information ecosystems, drawing examples from the Arab Spring. Taiwan's embrace of digital democracy and the successful transition of independent websites into official platforms were collectively noted. Lessons from Tunisia emphasized the need for effective local implementation and addressing complex issues like access to information.

However, each time an example was cited by a participant, it came with a caveat. Participants noted that there was growing disillusionment regarding the real impact of such endeavors, leading to questions about governments' genuine commitment to continue them. One participant from Africa noted, "The key question is how willing are governments to go all the way?" Some legitimately positive deployments of technology never emerged from pilot stages, despite initial success. Throughout the dialogue, participants noted the growing digital divide, limiting access to civic technology options more and more to social elites. Participants expressed concerns about the influence of major actors like mega-corporations and governments in the tech field, leading to complex issues like net neutrality. The conversation delved into the rise of algorithmic



Efforts by some governments to block social media access to suppress opposition and dissent was highlighted by dialogue participants. Source: Irina Imago, Shutterstock.

decision-making, technophobia versus technophilia, and the looming artificial intelligence (AI) divide, which could exacerbate existing inequalities.

Thus, technology's dual nature became a central theme throughout the dialogue. As one participant from Turkiye noted, “Every technology brings its own accidents.” The participants collectively acknowledged that while technology offers tremendous potential, it can also be a source of significant harm and disruption. Better understanding of this duality is needed, with one participant calling for better education and study around human-machine interaction.

Digital Threats to Democracy

For all of the promise that technology could have in the support of democratic ideals, much discussion in the dialogue focused on how technology can threaten established democratic norms. Participants explored the pressing issue of digital threats to democracy. They collectively discussed how both autocratic regimes and democracies are

harnessing digital technologies to maintain power and control. There has been heavy investment by governments in spyware, malware, and AI which have collectively become tools of control and suppression.

Participants categorized digital threats into three key areas:

- **Blocking Content**: This includes censorship, internet shutdowns, and the criminalization of free speech and activism through cyber laws. Regimes can further utilize fragmentation of the internet to control content. An example cited included China's efforts to reshape internet governance globally. However, the blocking of content is not just limited to anti-democratic regimes. Participants expressed concerns about the influence of major actors like mega-corporations in the tech field, leading to complex issues like net neutrality.

- **Surveillance**: Regimes employ mass surveillance and AI for broad monitoring, along with targeted surveillance using spyware. The surveillance industry, both overt and covert, has thrived in recent years, being utilized by governments, corporations, and individuals alike. The export of smart city surveillance models from China and a thriving spyware industry contribute to profiling and targeted information attacks.

- **Digital Perception/Misinformation**: Manipulating public opinion through false narratives, doctored images, and deep fake videos adds to the existing information crisis. As one participant said, "The most engaging content is usually the most horrific content." These technologies are becoming more readily available to the general public, increasing the likelihood of the manipulation of politics and injustice.

The discussion in this segment shifted its focus towards the indispensable role of civil society in addressing digital threats. Participants collectively delineated a range of strategies that civil society organizations (CSOs) employ as part of their crucial functions. These strategies encompassed, firstly, the pivotal role of CSOs in raising awareness by educating the public about the implications of digital threats, contributing to the mitigation of false narratives. Secondly, participants emphasized the importance of evidence-based research conducted by CSOs and journalists, serving as a cornerstone for providing tangible proof of digital abuses and exposing the actions of both governments and tech companies. Furthermore, the dialogue underscored CSOs' engagement in targeted advocacy efforts, exerting pressure to instigate behavioral changes in tech

companies and government policies. Additionally, CSOs were recognized for offering essential support services, including fact-checking, aimed at combating disinformation and providing assistance to victims. Lastly, the conversation emphasized the proactive role of CSOs in pushing for transparency, urging tech companies, governments, and international agencies to adopt a more open stance regarding their actions. This collective approach highlights the diverse and interconnected strategies employed by civil society in combating digital threats.

Addressing the Digital Threats

The latter half of the dialogue offered an opportunity for participants to not only deeply evaluate the threats posed to democracy by new digital realities, but also offer suggestions of how to combat these pervasive threats. This discussion also explored human stories, diversity, operationalizing legislation, intra-institutional analysis, building new norms, and the importance of collaboration to protect democratic values in the digital age. Participants collectively emphasized the urgency of addressing digital security, especially for marginalized groups. Furthermore, they collectively stressed the need for transparency and cooperation among governments, tech companies, and civil society. Participants also worked to address digital media's transformative power in closed autocratic states.

Many participants expressed their full awareness that addressing digital threats will require careful balancing and deliberation. Challenges noted by participants included balancing online harm and freedom of expression, the absence of consensus on online safety standards, and the lack of comprehensive privacy laws. Recognition that authoritarian governments are now utilizing this technology has heightened the need to address these challenges. While many of these challenges remain unmitigated and unresolved, technology companies continue to push new products to market without full understanding of their impacts, as the industry incentivizes profit and celebrates “disruption.” Meanwhile, participants fully realized that in many respects, those seeking a more responsible deployment of technology will be working from behind as the speed of technological development far outpaces social response. This is complicated further by limited funding and increased government scrutiny.

Throughout the dialogue, participants highlighted numerous avenues to direct efforts in addressing these challenges. Participants emphasized strategies by civil society

organizations such as raising awareness, evidence-based research, targeted advocacy, support services, and pushing for transparency. Diversity and inclusion were collectively emphasized along with a call for effective legislation operationalization, intra-institutional analysis, building new norms, and overcoming challenges collectively. Collaboration among civil society, governments, and tech companies also emerged as essential to protect democratic values in the digital age.

Combating Disinformation

Specific sessions of the dialogue were dedicated to some of the larger challenges in the integration of technology and democracy. One such challenge was disinformation. Participants noted how disinformation has increased in pervasiveness, led to the rapid spread of false information on social media platforms, and augmented the difficulty of fact-checking in real-time. This environment leaves individuals with a lack of credible information sources in tightly controlled regions. Moreover, the language barrier in regions with numerous dialects poses a significant problem. The participants specifically noted the following:

- **Understanding Disinformation:** The participants recognized that disinformation encompasses a wide range of content, including outright lies, the politicized use of facts, and manipulated narratives. They emphasized the importance of avoiding a Euro-centric perspective on disinformation and instead understanding the political agendas of diverse audiences.

- **Regional Variations:** Acknowledging that regions are not homogenous; the conversation emphasized the need to consider the distinct challenges faced by different regions. Language barriers emerged as a significant obstacle to understand context and its impacts in regions such as sub-Saharan Africa and the Middle East. The participants noted that politicians often exploit identity politics and group-based grievances, contributing to the spread of disinformation.

- **Role of Civil Society:** Civil society plays a crucial role in addressing disinformation, with fact-checking initiatives gaining prominence, often fueled by external funding. Additionally, organizations are focused on capacity building and creating alliances among stakeholders to tackle disinformation collectively.

The promise and peril of social media platforms were discussed throughout the dialogue. While in some examples, social media provided an open space for debate and protest, others highlighted the spread of disinformation and government cooption. Some also raised concerns about the influence these large social media companies wield. Source: easy camera, Shutterstock.

- **Need for Transparency and Accountability:** The participants stressed the importance of transparency, both in the operations of social media platforms and in the methodologies used to verify information. They also called for greater accountability, especially among tech companies, to address the trust deficit that enables disinformation to thrive.

- **Shift from Objectivity to Credibility:** The field of journalism is under intense pressure. As one said, "We have gone from journalists who thought their jobs were to be watchdogs to becoming participants and activists." The discussion highlighted a paradigm shift in media and information consumption. While objectivity was once a primary goal in media, today's users seek transparency and credibility from information sources. To build trust, media outlets must open up their processes and establish partnerships within the new information ecosystem.

- **Local Initiatives:** Emphasis was placed on the effectiveness of local-level initiatives, including libraries and community organizations, in promoting media literacy. Participants pointed out that these organizations often have deep-rooted credibility within their communities, making them valuable resources for combating disinformation.

Navigating the Terrain of Big Data, AI, and Data Privacy

In a different session, the participants delved into the intricate world of big data, AI, and data privacy. The multifaceted discussion uncovered critical issues that spanned the realms of technology, ethics, and societal impact:

- **Big Data's Complex Tapestry:** The discussion collectively acknowledged that the vastness and intricacy of big data surpassed traditional management and monitoring techniques. Participants recognized that the sheer volume, velocity, and variety of data in the big data ecosystem presented challenges in terms of processing, analysis, and interpretation.

- **Concerns Amidst Profit-Driven Algorithms:** A joint concern emerged regarding the potential misuse of big data for profit-driven machine learning algorithms. The profit motive, when driving the development and application of algorithms, was seen as a source of ethical apprehension. The participants explored the implications of algorithms prioritizing financial gain over ethical considerations.

- **AI Technologies and Bias:** AI technologies, with a spotlight on ChatGPT, were scrutinized. Participants expressed concerns about biases embedded in AI systems and grappled with the challenge of oversight during their developmental stages. The discussion underscored the importance of addressing biases to ensure fairness, equity, and responsible AI deployment.

- **Unraveling the Web of Hyper-Targeted Information:** The conversation unfolded into the realm of hyper-targeted information derived from big data. Participants examined the implications of personalized content delivery, emphasizing the need for ethical data use. The dialogue grappled with the balance between personalization for user experience and the potential risks associated with algorithms reinforcing biases or creating information bubbles.

- **The Political Dimension of Open-Source Databases:** A pivotal point of discussion was the introduction of open-source databases, collectively recognizing the political dimension embedded in their adoption. Participants explored the potential shift from proprietary models to open alternatives, viewing it as a political choice with implications for accessibility, affordability, and data control.

- **Biases and the Dark Side of Deepfakes:** The participants explored the darker aspects of AI, focusing on biases within AI systems and the alarming risks posed by deepfakes. Special attention was given to the egregious issue of non-consensual pornography, where AI technology could be exploited to create manipulated and harmful content. The participants collectively emphasized the need for vigilant safeguards against such malicious uses.

- **Job Displacement and Economic Repercussions:** The debate extended to the socio-economic domain, discussing the potential displacement of jobs due to AI. Participants collectively considered the broader economic repercussions of technological advancements, weighing the benefits of efficiency against the potential challenges of workforce displacement.

- **Data Control, Privacy, and the Human Element:** An emphasis was placed on user control over data and the transparency needed in data collection processes. Participants underscored the importance of preserving individuals' privacy rights in the age of data-driven technologies. The discussion collectively recognized the human dimension in data privacy, emphasizing the need to empower users with control over their personal information.

- **Real-World Harms and Ethical Imperatives:** The dialogue acknowledged the sobering reality of AI's potential to inflict harm on humanity. Participants called for a conscientious approach to address real-world harms arising from technological advancements. The ethical imperatives of responsible AI development, deployment, and usage were underscored as crucial considerations.

- **Striking a Balance:** Control and Transparency: The central theme revolved around the collective recognition of the imperative to strike a balance between control and transparency in AI development. Participants advocated for measures that ensure

responsible practices, ethical considerations, and transparency, emphasizing that a harmonious equilibrium is pivotal to address the challenges posed by big data and AI.

- **International Cooperation and Collaborative Solutions:** The dialogue jointly recognized that the challenges presented by big data and AI are global in nature. Participants emphasized the need for international cooperation, collaborative solutions, and shared frameworks to address the ethical, social, and technological dimensions of these challenges. The collective disposition echoed a call for a united effort to navigate the complex terrain of emerging technologies responsibly.

Unveiling the Landscape of Digital Decentralization

In the final session of the dialogue, participants discussed the rise of decentralization of the internet, often coined in the industry as "web3." The most commonly known of these decentralization technologies is blockchain, an encrypted peer-to-peer network that serves as the background for cryptocurrencies like Bitcoin. Like AI and social media, the coming impact of decentralization on democracy poses both great possibilities and potential abuses. The dialogue session focused on its impact on society, including politics, economics, and social rights. Participants acknowledged the following:

- **Ethical Concerns Decentralized Mass Surveillance:** An ethical undercurrent throughout the session scrutinized the exponential growth of decentralized mass surveillance systems. Questions arose about the implications of such systems on privacy, individual freedoms, and the ethical considerations surrounding surveillance in a decentralized paradigm. This scrutiny marked a shared commitment to ethical reflections on the evolving landscape.

- **Balancing Decentralization and Harm Prevention:** The dialogue pondered on how to harness the positive potential of decentralization while safeguarding against the perils associated with the spread of harmful content. While a group solution was not reached beyond generalizations, participants did acknowledge that more discussion about this balance is needed.

- **Decentralization Requires Navigating Beyond Data:** The participants highlighted decentralization as extending its influence far beyond the realm of data management. It was an acknowledgment that decentralization, in its true essence, transcends

technological domains, requiring a commitment to responsible practices to navigate the evolving contours of this paradigm shift.

- **Diverse Approaches to Web3 Deployment:** The discussion collectively wove a tapestry of diverse approaches to decentralization, showcasing the intricacies of Blue Sky (a text-based messaging app), Macedon (workflow optimization), and NORSTER (a decentralized Twitter alternative). Each approach offered unique solutions and incentives. The collective engagement allowed participants to unravel the merits, challenges, and potential societal impacts of these distinct paths, fostering a comprehensive understanding. On a positive note, participants noted that these technologies could prevent surveillance by authoritarian regimes. Conversely, they acknowledged the potential security risks of such applications in the hands of nefarious or violent actors.

- **Safeguarding Inclusivity and Safety:** Participants expressed concern that decentralized applications and platforms may lead, like other technology businesses, to monopolization. Given that risk, participants emphasized the paramount importance of inclusivity and safety, envisioning platforms that not only embrace diversity but also stand as bastions of accessibility and guardians of the principles of openness and freedom of expression.

- **Understanding Community Inequity:** The dialogue recognized that not all communities stand on equal footing when faced with the advent of decentralized technologies. The use of these technologies still requires the basics, such as internet access. Said one, “The major suppliers of the internet are states. They are holding the pipeline. How is decentralization going to help us?” Access can remain a challenge in underdeveloped regions or lower income households. This shared realization underscored the need for tailored solutions, sensitive to the unique needs and challenges of diverse communities.

Cover Photo: BestBackgrounds, Shutterstock

The Hollings Center for International Dialogue is a non-profit, non-governmental organization dedicated to fostering dialogue between the United States and countries with predominantly Muslim populations around the world. In pursuit of its mission, the Hollings Center convenes dialogue conferences that generate new thinking on important international issues and deepen channels of communication across opinion leaders and experts. The Hollings Center is headquartered in Washington, D.C. and maintains a representative office in Istanbul, Türkiye.

To learn more about the Hollings Center's mission, history and funding:
http://www.hollingscenter.org/about/mission-and-approach
info@hollingscenter.org