ARGUMENT
An expert's point of view on a current event.

AI's Alarming Trend Toward Illiberalism

Left ungoverned, the technology opens pathways to undermine democracy.

OCTOBER 31, 2024

*By **Ami Fields-Meyer**, and **Janet Haven***

As the United States nears its consequential November election, concerns about the impacts of artificial intelligence on the country's electoral integrity are front and center. Voters are receiving deceptive phone calls mimicking candidates' voices, and campaigns are using AI images in their ads. Many fear that highly targeted messaging could lead to suppressed voter turnout or false information about polling stations. These are legitimate concerns that public officials are working overtime to confront.

But free and fair elections, the building blocks of democratic representation, are only one dimension of democracy. Today, policymakers must also recognize an equally fundamental threat that advanced technologies pose to a free and open society: the suppression of civil rights and individual opportunity at the hands of opaque and unaccountable AI systems. Ungoverned, AI undermines democratic practice, norms, and the rule of law—fundamental commitments that underpin a robust a liberal democracy—and opens pathways toward a new type of illiberalism. To reverse this drift, we must reverse the currents powering it.

Liberal societies are characterized by openness, transparency, and individual agency. But the design and deployment of powerful AI systems are the precise inverse.

In the United States, as in any country, those who control the airwaves, steer financial institutions, and command the military have long had a wide berth to make decisions that shape society. In the new century, another set of actors joins that list: the increasingly concentrated group of corporate players who control data, algorithms, and the processing infrastructure to make and use highly capable AI systems. But without the kind of robust oversight the government prescribes over other parts of the economy and the military, the systems these players produce lack transparency and public accountability.

The U.S. foreign-policy establishment has long voiced legitimate concerns about the use of technology by authoritarian regimes, such as China's widespread surveillance, tracking, and control of its population through deep collusion between the state and corporations. Civil society, academics, and journalists have recognized the threat of those same tools being deployed to similar ends in the United States. At the same time, many of today's AI systems are undermining the liberal character of American society: They run over civil rights and liberties and cause harm for which people cannot easily seek redress. They violate privacy, spread falsehoods, and obscure economic crimes such as price-fixing, fraud, and deception. And they are increasingly used—without an architecture of accountability—in institutions central to American life: the workplace, policing, the legal system, public services, schools, and hospitals.

All of this makes for a less democratic American society. In cities across the United States, people of color have been arrested and jailed after being misidentified by facial recognition tools. We've seen AI used in loan refinancing charge more to applicants who went to historically Black colleges. An AI program aimed at preventing suicide among veterans prioritizes white men and overlooks survivors of sexual violence, who are much more likely to be women. Hidden behind computer code, illegal and unfair treatment long banned under federal law is becoming harder to detect and to contest.

To global observers, the trendlines of AI in American society will look familiar; the worst harms of these systems mirror the tenets of what has been called "illiberal democracy." Under that vision—championed most famously by Hungarian Prime Minister Viktor Orban, a darling of the U.S. right—a society "maintains the outward appearances of a democracy ... but in fact seeks to undermine all the institutions and norms that give democracy meaning," scholar Susan Rubin Suleiman wrote in 2021. This doesn't have to look like canceling elections or dismantling a sitting legislative body; instead, the vision takes the form of a more subtle assault—foreclosing the ability of individuals and minority groups to assert their rights.

As powerful new AI products are born and come of age amid a growing political alliance between far-right ideologues and some of the most powerful leaders in the technology industry, these foundational threats to free society could accelerate. Elon Musk, amplifying alarmist narratives on migrants and dehumanizing language about women and LGBT people, has said he would serve in a potential second Trump administration. Elsewhere in Silicon Valley, a growing cadre of venture capitalists are boldly betting the house on Trump in the belief that their portfolios—brimming with crypto and AI bets—may be better off under a president who is unfazed by harms to the most vulnerable and who challenges the exercise of fundamental rights.

Simply studying these tools and their effects on society can prove difficult: Scientific research into these systems is dominated by profit-motivated private actors, the only people who have access to the largest and most powerful models. The systems in question are primarily closed-source and proprietary, meaning that external researcher access—a basic starting point for transparency—is blocked. Employees at AI companies have been forced to sign sweeping nondisclosure agreements, including those about product safety, or risk losing equity. All the while, executives suggest that understanding precisely how these systems make decisions, including in ways that affect people's lives, is something of luxury, a dilemma to be addressed sometime in the future.

The real problem, of course, is that AI is being deployed now, without public accountability. No citizenry has elected these companies or their leaders. Yet executives helming today's big AI firms have sought to assure the public that we should trust them. In February, at least 20 firms signed a pledge to flag AI-generated videos and take down content meant to mislead voters. Soon after, OpenAI and its largest investor, Microsoft, launched a $2 million Societal Resilience Fund focused on educating voters about AI. The companies point to this work as core to their missions, which imagine a world where AI "benefits all of humanity" or "helps people and society flourish."

Tech companies have repeatedly promised to govern themselves for the public good—efforts that may begin with good intentions but fall apart under the pressure of a business case. Congress has had no shortage of opportunities over the last 15 years to step in to govern data-centric technologies in the public's interest. But each time Washington has cracked open the door to meaningful technology governance, it has quickly slammed it shut. Federal policymakers have explored reactive and well-meaning but flawed efforts to assert governance in specific domains—for example, during moments of attention to teen mental health or election interference. But these efforts have faded as public attention moved elsewhere. Exposed in this story of false starts and political theatrics is the federal government's default posture on technology: to react to crises but fail to address the root causes.

Even following well-reported revelations, such as the Cambridge Analytica scandal, no legislation has emerged to rein in the technology sector's failure to build products that prioritize Americans' security, safety, and rights—not to mention the integrity of U.S. democracy. The same story has unfolded in the doomed push to achieve data privacy laws, efforts that have stalled out in committee ad infinitum, leaving Americans without the basic protections for their personal information that are enjoyed by people living in 137 other countries.

The Biden-Harris administration decided to push harder, through initiatives we worked both directly and indirectly on. Even before ChatGPT vaulted AI to the center of the national discourse in November 2022, President Joe Biden's White House released an AI Bill of Rights proposing five key assurances all Americans should be able to hold in an AI-powered world: that AI technologies are safe, fair, and protective of their privacy; that they are made aware when systems are being used to make decisions about them; and that they can opt out. The framework was a proactive, democratic vision for the use of advanced technology in American society.

The vision has proved durable. When generative AI hit the consumer market, driving both anxiety and excitement, Biden didn't start from scratch but from a set of clear and affirmative first principles. Pulling from the 2022 document, his 2023 executive order on AI mandated a coordinated federal response to AI, using a "rights and safety" framework. New rules from the powerful Office of Management and Budget turned those principles into binding policy, requiring federal agencies to test AI systems for their impact on Americans' rights and safety before they could be used. At the same time, federal enforcement agencies used their existing powers to enforce protections and combat violations in the digital environment. The Federal Trade Commission stepped up its enforcement of digital-era violations of well-established antitrust laws, putting AI companies on notice for potentially unfair and deceptive practices that harm consumers. Vice President Kamala Harris presided over the launch of a new AI Safety Institute, calling for a body that addressed a "full spectrum" of risks, including both longer-term speculative risks and current documented harms.

This was a consequential paradigm shift from America's steady state of passive technology nongovernance—proof-positive that a more proactive approach was possible. Yet these steps face a range of structural limitations. One is capacity: Agencies across the federal government carrying out the work of AI governance will need staff with sociotechnical expertise to weigh the complex trade-offs of AI's harms and opportunities.

Another challenge is the limited reach of executive action. Donald Trump has promised to repeal the AI executive order and gut the civil service tasked with its implementation. If his first term is any indication, a Republican administration would reinstate the deregulatory status quo. Such is the spirit of plans reportedly drawn up by Larry Kudlow, Trump's former National Economic Council director, to create "industry-led" task forces, placing responsibility for assessing AI tools' safety into the hands of the powerful industry players who design and sell them.

And Biden's measures, for the most part, guide only the government's own use of AI systems. This is a valuable and necessary step, as the behavior of agencies bears on the daily lives of

Americans, particularly the most vulnerable. But the effects of executive actions on the private sector are circumscribed, related to pockets of executive authority such as government contracting, civil rights enforcement, or antitrust action. A president's pen alone cannot create a robust or dynamic accountability infrastructure for the technology industry. Nor can we rely on agencies to hold the line; recent Supreme Court decisions—*Loper Bright*, *Corner Post*, and others—have weakened their authority to use their mandated powers to adapt to new developments.

This, of course, is the more fundamental shortcoming of Biden's progress on AI and technology governance: It does not carry the force of legislation. Without an accompanying push in Congress to counter such proposed rollbacks with new law, the United States will continue to embrace a largely ungoverned, innovation-at-all-costs technology landscape, with disparate state laws as the primary bulwark—and will continue to see the drift of emerging technologies away from the norms of robust democratic practice.

Yet meaningful governance efforts may be dead on arrival in a Congress that continues to embrace the flawed argument that without carte blanche for companies to "move fast and break things," the United States would be doomed to lose to China, on both economic and military fronts. Such an approach cedes the AI competition to China's terms, playing on the field of Chinese human rights violations and widespread surveillance instead of the field of American values and democratic practice. It also surrenders the U.S. security edge, enabling systems that could break or fail at any moment because they were rushed to market in the name of great-power competition.

Pursuing meaningful AI governance is a choice. So is the decision, over decades, to leave powerful data-centric technologies ungoverned—a decision to allow an assault on the rights, freedoms, and opportunities of many in American society. There is another path.

Washington has the opportunity to build a new, enduring paradigm in which the governance of data-centric predictive technologies, as well as the industry that creates them, is a core component of a robust U.S. democracy.

We must waste no time reaffirming that the protections afforded by previous generations of laws also apply to emerging technology. For the executive branch, this will require a landmark effort to ensure protections are robustly enforced in the digital sphere, expanding enforcement capacity in federal agencies with civil rights offices and enforcement mandates and keeping up the antitrust drumbeat that has put anti-competitive actors on notice.

The most consequential responsibility for AI governance, though, rests with Congress. Across the country, states are moving to pass laws on AI, many of which will contradict one another and form an overlapping legal tangle. Federal lawmakers should act in the tradition of the 1964 Civil Rights Act, issuing blanket protections for all Americans. At a minimum, this should include a new liability regime and guarantee protection from algorithmic discrimination; mandate pre- and post-deployment testing, transparency, and explainability of AI systems; and a requirement for developers of AI systems to uphold a duty of care, with the responsibility to ensure that systems are safe and effective.

These AI systems are powered by data, so such a bill should be accompanied by comprehensive data privacy protections, including a robust embrace of data minimization, barring companies from using personal information collected for one purpose in order to achieve an unrelated end.

While only a start, these steps to protect democratic practice in the age of AI would herald the end of America's permissive approach to the technology sector's harms and mark the beginning of a new democratic paradigm. They should be followed forcefully by a separate but complementary project: ensuring that individuals and communities participate in deciding how AI is used in their lives—and how it is not. Most critically, more workers—once called America's "arsenal of democracy"—must organize and wield their collective power to bargain over whether, when, and how technologies are used in the workplace.

Such protections must also extend beyond the workplace into other areas of daily life where technology is used to shape important decisions. At a moment of weakening democratic norms, we need a new, concerted campaign to ease the path for anyone to challenge unfair decisions made about them by ungoverned AI systems or opt out of AI systems' use altogether. This must include a private right of action for ordinary people who can show that AI has been used to break the law or violate their rights. We must also open additional pathways to individual and collective contestation, including robust, well-resourced networks of legal aid centers trained in representing low-income clients experiencing algorithmic harms.

We can bring many more people into the process of deciding what kinds of problems powerful AI systems are used to solve, from the way we allocate capital to the way we conduct AI research and development. Closing this gap requires allowing people across society to use AI for issues that matter to them and their communities. The federal government's program to scale up access to public research, computing power, and data infrastructure is still only a pilot, and Congress has proposed to fund it at only $2.6 billion in its first six years. To grasp that number's insufficiency, one needed only to listen to Google's spring earnings call, where investors heard that the tech giant planned to spend about $12 billion on AI development *per quarter*. Next, the U.S. government should invest in the human and tech infrastructures of "public AI," to provide both a sandbox for applied innovation in the public interest and a countervailing force to the concentration of economic and agenda-setting power in the AI industry.

These are some of the measures the United States can undertake to govern these new technologies. Even in an administration that broadly supports these goals, however, none of this will be possible or politically viable without a change in the overall balance of power. A broad-based, well-funded, and well-organized political movement on technology policy issues is needed to dramatically expand the coalition of people interested and invested in technology governance in the United States.

Ushering in these reforms begins with telling different stories to help people recognize their stake in these issues and understand that AI tools directly impact their access to quality housing, education, health care, and economic opportunity. This awareness must ultimately translate to pressure on lawmakers, a tool those standing in the way of a democratic vision for AI use to great effect. Musk is reportedly bankrolling a pro-Trump super PAC to the tune of tens of millions per month. Andreessen Horowitz, the venture firm led by anti-regulation founders, increased its lobbying budget between the first and second quarter of this year by 135 percent. Not only are the big corporate tech players spending millions of dollars on lobbying per quarter, but each is also running a political operation, spending big money to elect political candidates who will look after their interests.

The academic, research, and civil society actors whose work has helped change the tech policy landscape have succeeded in building strong policy and research strategies. Now is the time to venture further into the political battlefield and prepare the next generation of researchers, policy experts, and advocates to take up the baton. This will require new tools, such as base-building efforts with groups across the country that can help tie technology governance to popular public issues, and generational investments in political action committees and lobbying. This shift in strategy will require new, significant money; philanthropic funders who have traditionally backed research and nonprofit advocacy will need to also embrace an explicitly political toolkit.

The public interest technology movement urgently needs a political architecture that can at last impose a political cost on lawmakers who allow the illiberal shift of technology companies to proceed unabated. In the age of AI, the viability of efforts to protect democratic representation, practice, and norms may well hinge on the force with which non-industry players choose to fund and build political power—and leverage it.

A choice confronts the United States as we face down AI's threats to democratic practice, representation, and norms. We can default to passivity, or we can use these instruments to shape a free society for the modern era. The decision is ours to make.

Ami Fields-Meyer *is a senior fellow at the Harvard Kennedy School and former senior policy advisor to Vice President Kamala Harris.*
Janet Haven *is the executive director of Data & Society and a member of the National AI Advisory Committee. The opinions expressed in this article do not represent the opinions of the National AI Advisory Committee or any other U.S government body.*