

Artificial Intelligence and Democratic Norms

Meeting the Authoritarian Challenge

by Nicholas D. Wright



National Endowment
for Democracy
Supporting freedom around the world

forum
International Forum for Democratic Studies

ABOUT THE SHARP POWER AND DEMOCRATIC RESILIENCE SERIES

As globalization deepens integration between democracies and autocracies, the compromising effects of sharp power—which impairs free expression, neutralizes independent institutions, and distorts the political environment—have grown apparent across crucial sectors of open societies. The Sharp Power and Democratic Resilience series is an effort to systematically analyze the ways in which leading authoritarian regimes seek to manipulate the political landscape and censor independent expression within democratic settings, and to highlight potential civil society responses.

This initiative examines emerging issues in four crucial arenas relating to the integrity and vibrancy of democratic systems:

- Challenges to free expression and the integrity of the media and information space
- Threats to intellectual inquiry
- Contestation over the principles that govern technology
- Leverage of state-driven capital for political and often corrosive purposes

The present era of authoritarian resurgence is taking place during a protracted global democratic downturn that has degraded the confidence of democracies. The leading authoritarians are challenging democracy at the level of ideas, principles, and standards, but only one side seems to be seriously competing in the contest.

Global interdependence has presented complications distinct from those of the Cold War era, which did not afford authoritarian regimes so many opportunities for action within democracies. At home, Beijing, Moscow, and others have used twenty-first-century tools and tactics to reinvigorate censorship and manipulate the media and other independent institutions. Beyond their borders, they utilize educational and cultural initiatives, media outlets, think tanks, private sector initiatives, and other channels of engagement to influence the public sphere for their own purposes, refining their techniques along the way. Such actions increasingly shape intellectual inquiry and the integrity of the media space, as well as affect emerging technologies and the development of norms. Meanwhile, autocrats have utilized their largely hybrid state-capitalist systems to embed themselves in the commerce and economies of democracies in ways that were hardly conceivable in the past.

The new environment requires going beyond the necessary but insufficient tools of legislation, regulation, or other governmental solutions. Democracies possess a critical advantage that authoritarian systems do not—the creativity and solidarity of vibrant civil societies that can help safeguard institutions and reinforce democratic values. Thus, the papers in this series aim to contextualize the nature of sharp power, inventory key authoritarian efforts and domains, and illuminate ideas for non-governmental action that are essential to strengthening democratic resilience.

ABOUT THE AUTHOR

Dr. Nicholas D. Wright is an affiliated scholar at Georgetown University, an honorary senior research fellow at University College London (UCL), a consultant at Intelligent Biology, and fellow at New America. His work combines neuroscientific, behavioral, and technological insights to understand decision making in politics and international confrontations in ways practically applicable to policy. He leads international, interdisciplinary projects with collaborators in countries including China, the United States, Iran, and the United Kingdom. He was an associate in the Nuclear Policy Program at the Carnegie Endowment for International Peace. He has conducted work for the UK government and US Department of Defense. He was a clinical neurologist in Oxford and at the National Hospital for Neurology—and returned to frontline medicine during the COVID-19 pandemic. Dr. Wright is editor of the book *Artificial Intelligence, China, Russia, and the Global Order* (Air University Press, 2019) and has published articles in numerous academic, government, and general publications including *The Atlantic* and *Foreign Affairs*, in addition to appearing on CNN and the BBC. Dr. Wright received a medical degree from UCL, a BSc in Health Policy from Imperial College London, is a member of the Royal College of Physicians (UK), and holds an MSc in Neuroscience and a PhD in Neuroscience from UCL.

ACKNOWLEDGMENTS

The International Forum for Democratic Studies would like to recognize Lindsay Gorman and Rebecca MacKinnon for their valuable peer review, Wyatt Hoffman for his helpful comments, Tyler Royslance for his outstanding editorial support, and the contributions of Christopher Walker, Shanthy Kalathil, Jessica Ludwig, Cooper Hewell, Rachelle Faust, and others at the National Endowment for Democracy. The Forum also wishes to express its thanks to the Smith Richardson Foundation, which has provided critical financial support for this initiative.

The views expressed in this paper represent the opinions and analysis of the author and do not necessarily reflect those of the National Endowment for Democracy or its staff.

EXECUTIVE SUMMARY

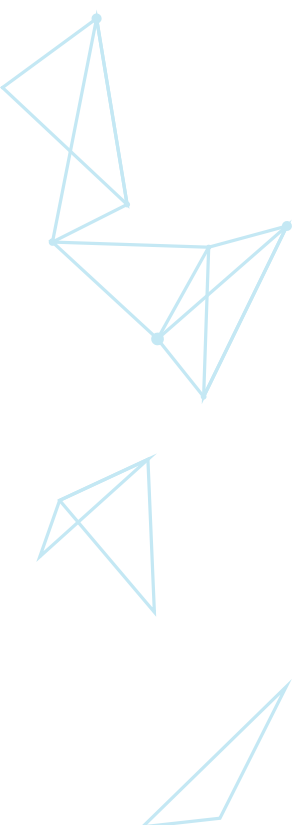
From industrial-age factory labor inspections to the fight against COVID-19, forms of surveillance and data monitoring have played a critical role in the last two centuries of economic and social progress. Now, as artificial intelligence (AI) and AI-related technologies potentially unlock the value of large-scale data collection, authoritarian regimes stand ready to manipulate the development of global surveillance to serve their own interests. Absent purposeful efforts to strengthen key democratic norms and accountability around emerging technologies, we risk spiraling into new authoritarian forms of surveillance-based governance.

As China and other authoritarian regimes construct digital authoritarian systems at home and propagate these models abroad, they are competing with democracies to shape global standards and infrastructure. How can liberal democracies harness the massive benefits of AI-related technologies without infringing on fundamental rights and risking a long-term shift toward authoritarianism?

- **Building and maintaining data silos.** Authoritarian regimes can turbocharge AI by training it on two types of data that liberal democracies should not similarly exploit or combine: “broad data” generated at volume on digital devices, and high quality “ground truth data,” such as tax returns and medical records. While conventional wisdom says that data must be integrated rather than isolated, siloing data limits authoritarian affordances and enhances security. Civil society must consider what silos are necessary to prevent misuse of data.
- **Affording new models of “digital sovereignty” for use by liberal democracies.** Authoritarian states advocate for digital sovereignty as a state-based model of control over the internet. There is a critical need to develop alternatives. Civil society can help think through new models that balance sovereignty with the protection of individual freedoms.
- **Support tech–civil society collaborations and develop resilience.** Civil society, in cooperation with government and big tech corporations where possible, can aim to correct market failures—like privileging advertising and marketing tools over individual privacy—by giving citizens the means to safeguard democratic integrity against malign information operations, while preserving essential openness of the information environment.
- **Resist sharp power in international fora.** Norm-setting and technical standardization of AI-related technologies happen at a global scale. Civil society should promote transparent, multistakeholder AI governance and develop AI standards that encourage democratic practices and individual privacy.

Civil society can play a crucial role to help democracies resist authoritarian influence in the surveillance context. Organizations focused on issues including privacy, human rights, free expression, technological standards, and public health can help identify, explain, and collaboratively address the complex challenges that arise from AI-related technologies. Democracies have adapted and thrived through past episodes of profound technological change. They must again evolve to continue delivering the many benefits of AI-related technologies while minimizing the affordances that could facilitate a shift toward authoritarianism. A robust civil society may be the greatest asset in the struggle to ensure that the current digital revolution results in more resilient liberal democracies.





In March 2020, almost everyone agreed that COVID-19 was changing the world. Countries everywhere struggled with deaths, lockdowns, economic devastation, or even the suspension of democratic protections and procedures in places where they were vulnerable. As with all such epidemics, public health requires effective surveillance within countries and at their borders. To have “life, liberty, and the pursuit of happiness,” one first needs life, which careful monitoring of infections helps to ensure.

Just a month prior, almost everyone agreed that artificial intelligence (AI) and other digital technologies were changing the world. China was constructing its digital authoritarian state at home and attempting to propagate its model abroad, competing with the United States and other democracies to shape global standards and infrastructure. This competition has raised profound questions for the wavering or backsliding democracies—like Hungary, Poland, or Kenya—that find themselves caught in the middle. If they must digitize, what is the best path forward?

Beijing’s answer is clear enough, but what models can liberal democracies offer the world that would allow a country to harness the massive benefits of AI-related technologies—for instance, in public health—while minimizing infringements on fundamental rights and the risk of a long-term shift toward authoritarianism?

Although poorly understood at the time, one of the most significant long-term effects of the 11 September 2001 terrorist attacks was expanded surveillance in the United States and other democracies. Similarly, one of COVID-19’s greatest long-term impacts may be a radical transformation of digital surveillance around the globe. This time, however, a failure to check overreach and abusive practices will be far more costly. Digital authoritarian competitors stand ready to exploit a lack of foresight in democracies and manipulate the development of global surveillance to serve their own interests. Indeed, contemporary authoritarian regimes have excelled at exerting influence in an increasingly interconnected world—not least through “sharp power,” which entails the use of intrusive means to impair free expression, compromise and neutralize independent institutions, and distort the political environment in targeted countries.¹

Governments are not the only competitors in this contest. Civil society around the world has an important role to play in helping democracies resist authoritarian pressure on the global surveillance environment. Organizations focused on diverse issues including privacy, human rights, free expression, technological standards, public health, and consumer protection can make crucial contributions in identifying, explaining, and collaboratively addressing the bewilderingly complex challenges that arise from AI-related technologies.

Two concepts may be helpful in identifying avenues for analysis and action by civil society.

- **Affordances:** Affordances are simply the possibilities for action that an actor perceives that their environment or tools present to them.² E-readers and tablets have different affordances, for instance, because they facilitate different actions. This is an important consideration when designing technology, since a system built for a particular purpose or set of purposes often enables other activities as well, and as strategists argue, capabilities create intentions. In the context of COVID-19, societies around the world are developing new public health surveillance systems that may create opportunities for other, more problematic forms of surveillance. Meaningful public input on proper limits for these systems is only possible in democratic environments and depends heavily on consultation with and action by nongovernmental organizations. Civil society must help guide the development of new digital capabilities to manage any affordances that would encourage a future shift toward authoritarianism.

- **Upsides of surveillance:** To enable the rich industrialized world's social and economic progress over the past two centuries, forms of surveillance and monitoring were entirely necessary. In fact, the story of modern human development is in part the story of surveillance. In nineteenth-century Britain, for instance, enforcement of legislation aimed at protecting factory workers, combating infectious diseases, or curbing pollution and the adulteration of food required new or vastly expanded inspectorates.³ The collection and analysis of data and statistics skyrocketed in government, the private sector, and academia. Yet throughout this period, Britain's robust parliamentary system became steadily more democratic and inclusive. Such historical experiences demonstrate that surveillance can confer enormous benefits, and that it is possible to reach these outcomes while protecting basic liberties and democratic governance.

The central question, then, is how to establish democratically accountable rules and norms that provide as much of the upside of AI-supported surveillance as possible, without creating technological affordances that could facilitate authoritarian concentrations of power.

This report focuses on surveillance issues in the more fragile democracies and their implications for civil society against a global backdrop of intensifying great-power competition. Part one describes AI-related technologies and how data integration can facilitate shifts to digital authoritarianism. Part two describes how digital sovereignty—defined here as the digital face of the broader principle of sovereignty—can enable basic state functions, such as democratically accountable public health surveillance and interventions. Although the term has been widely used in the past by authoritarian regimes to advocate for a state-based model of control over the internet, this paper will argue for presenting more fragile democracies with new models of democratic digital sovereignty. Part three considers how AI-related technologies afford opportunities for authoritarian states to exert sharp power—for instance, by boosting the dissemination of authoritarian narratives and sowing discord through disinformation campaigns, as seen with COVID-19—and the need for fragile democracies to develop resilience, in part through the work of civil society. Part four describes the competition for influence in international fora, which play crucial roles in shaping the potential digital futures—whether more authoritarian or more liberal and democratic—of all states grappling with these challenges.

AI-RELATED TECHNOLOGIES: HOW DATA INTEGRATION ENABLES DIGITAL AUTHORITARIANISM

AI-related technologies comprise the cutting edge of the broader digital technologies. The term “AI” here refers to a constellation of AI-related technologies that provide powerful, wide-ranging, and new capabilities.⁴ Together, they enable a new industrial revolution, taking the vast reams of data now produced by the computers and internet of the preceding revolution and turning it into useful data. None of these technologies is entirely new, but recent big improvements (particularly from deep learning around 2012) mean together they have revolutionary applications. Four are crucial—AI more tightly defined, big data, machine learning, and digital things.⁵ (See the AI and Related Technologies text box on page 3.)

Digital authoritarian competitors stand ready to exploit a lack of foresight in democracies and manipulate the development of global surveillance to serve their own interests.

AI AND RELATED TECHNOLOGIES

AI (more tightly defined)⁶: While the definition of AI is hotly debated and can be subdivided in various ways, generally speaking it refers to the automated analysis of data to model some aspect of the world, so that inferences from such models can be used to anticipate other possible events. Importantly, AI programs do not simply analyze data in the way they were originally programmed. Instead, they learn from data in order to respond intelligently to new data and adapt their outputs accordingly. AI is ultimately about “giving computers behaviors which would be thought intelligent in human beings.”⁷

Machine learning: Many computational methods for AI come from a field called machine learning—“the set of techniques and tools that allow computers to ‘think’ by creating mathematical algorithms based on accumulated data.”⁸ Deep learning is one method for machine learning that has recently led to major advances in AI.

Big data: These are high-volume—and often high-velocity and high-variety—information assets that demand cost-effective, innovative forms of information processing to enable enhanced insight and decision making.

Digital things: Data-collecting objects ranging from smartphones and digital assistant devices to toasters, military drones, and robots in factories will increasingly be able to perceive (for example, through facial or speech recognition), decide, and act.

When combined, these technologies amount to more than the sum of their parts. Big data as an asset can be difficult to exploit; AI is a key to unlocking its value, and machine learning is one technical part of that key.

AI-related advances have featured two main strengths and two main limitations.

AI is currently good at *perception*, meaning the processing and analysis of images, speech, or patterns in big data, and at *bounded decisions*, or tasks that are limited enough to be very well described by vast amounts of (often labeled) data, such as logistics in a warehouse. The continued rollout of technologies in the areas in which AI is already strong, which notably include surveillance, will likely dominate the next five to ten years of AI development and are consequently the focus of this report.

However, rolling out AI in the real world beyond these areas, let alone at scale, has proven difficult in many fields—including medicine—because of current AI technology’s two main limitations. One is a poor ability to assess *context*, so humans are often required to make even common-sense judgments. Another is the need for *vast amounts of labeled data*, which means that the laborious creation of huge datasets is often a precondition.

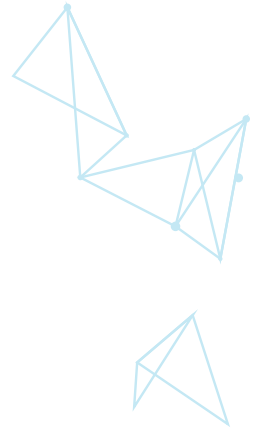
In other words, AI-related technologies currently enable increased surveillance, which can be partially automated and thus more efficient and cost-effective. However, because of AI’s current limitations, incorporating these technologies into social governance requires extensive human involvement to help deal with context, and current efforts will likely be dominated by developing big datasets. These factors are clearly illustrated by conditions in China.

AI AND DIGITAL AUTHORITARIANISM IN CHINA

In a digital authoritarian regime, digital technologies enable key aspects of the government’s repressive activities and efforts at social control. Beijing is already far along in developing such a system.

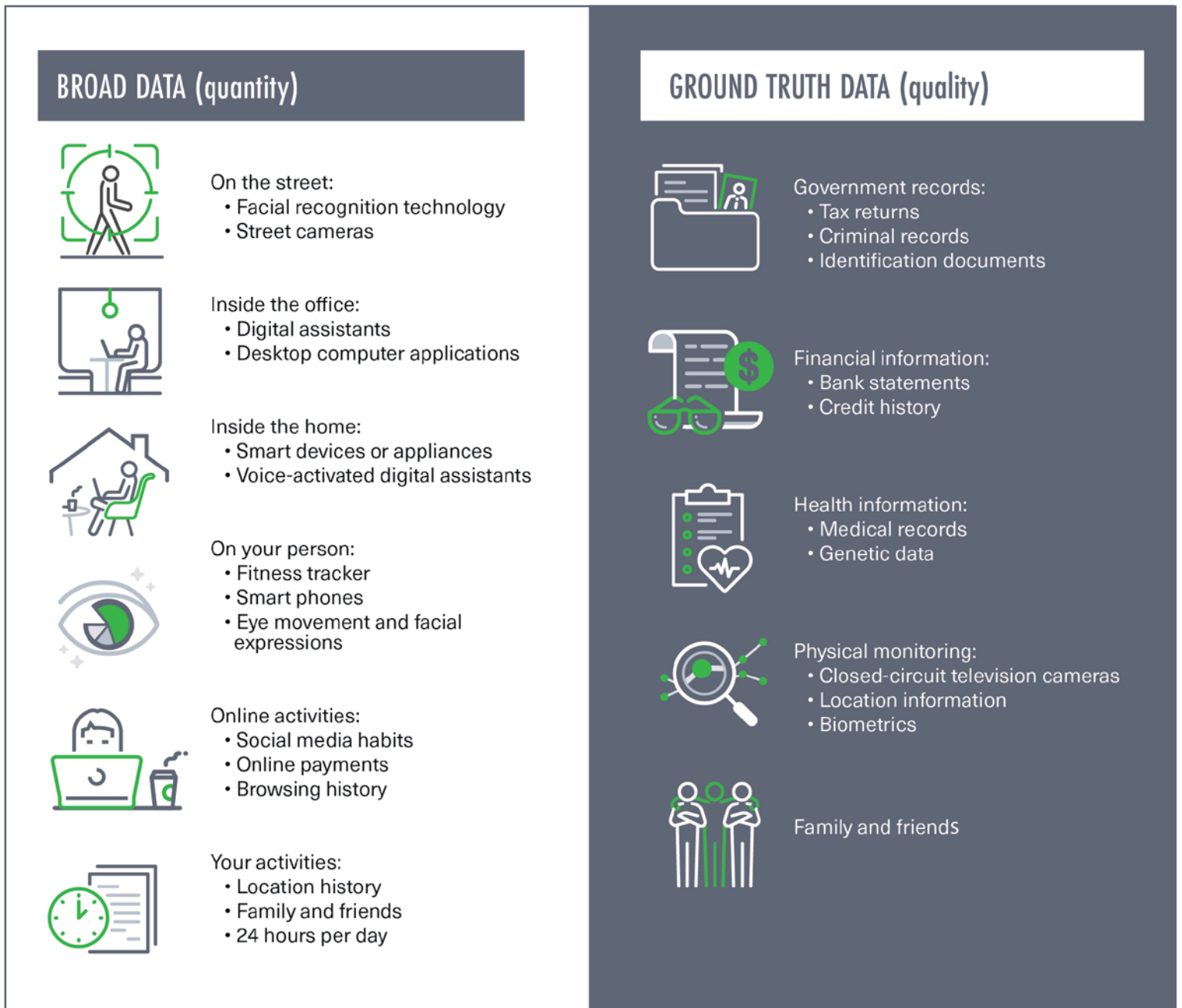
AI promises to minimize the costs and enhance the effectiveness of censorship and other official constraints on citizen behavior. Crucially, it offers a degree of selectivity that can preserve the free flow of information for economically creative and productive endeavors while simultaneously curbing political dissent. China’s internet filtration system, known as the Great Firewall, was an early demonstration of selective censorship, allowing Chinese users to access some but not all of the global internet.⁹ Moreover, AI-related technologies could enable predictive control of possible dissidents by extrapolating from an individual’s existing data.

China and other authoritarian regimes can turbocharge their AI by training it on two types of data that liberal democracies cannot and should not similarly exploit or combine. One type is the incredible breadth and volume of data generated by individuals on all the mobile



devices or digital platforms they may carry and interact with in their daily lives, referred to here as "broad data". The second type is "ground truth" data from tax returns, medical records, criminal records, police records, bank statements, genetic profiles, physical monitoring via enhanced security camera networks, and even family and friends. AI is as good as the data it trains on. The quantity and quality of data available to the Chinese regime on all individuals in society will, sadly, be excellent for training AI.

FIGURE: INTEGRATING TWO TYPES OF DATA FORMS A POWERFUL TRAINING SET FOR AI.¹⁰





This integration of different types of data is critical. Often, only governments hold the incredibly valuable “ground truth” data that act like labels for the broader information that might be collected from smart devices; if they do not hold these official records themselves, they typically regulate who can access them. The Chinese government’s surveillance and incarceration of the Uighur minority in Xinjiang Autonomous Region, through the “Integrated Joint Operations Platform” and other mechanisms, notably brings together diverse forms of data.¹¹ Leaked documents from inside the reeducation camp network in Xinjiang have described the importance of “one person, one file.”¹² More broadly, the various social credit systems being rolled out across China have sought, with varying degrees of success, to integrate data that existed separately.¹³ Many local social credit experiments explicitly look to fold together government and private-sector data.¹⁴

International assistance programs may be encouraging data integration in developing democracies without sufficient consideration of its ramifications. The World Bank, for instance, promotes digitizing government processes and interactions with citizens,¹⁵ and global measures of public-sector digitization show that it has increased in every region since the relevant indicators were first examined.

The private sector also provides digital services that billions of people want, and firms around the world are exhorted to undergo “digital transformation” or risk becoming the next corporate dinosaur to face extinction.¹⁶

Thus, the challenge for democracies and democratic civil society is to build digitized systems that enable economic and social development but do not afford a shift to authoritarianism.

While technical and regulatory solutions may help, only one response can deny the full-fledged digital surveillance state what it truly needs—high-quality and high-quantity integrated data to train its AI systems.

IDEAS FOR CIVIL SOCIETY: THE BENEFITS OF BUILDING AND MAINTAINING DATA SILOS

According to many in the public and private sectors, conventional wisdom says to simply break down “silos,” in which one department’s data is isolated from the rest of the organization—much like grain in farm silos. That conventional wisdom is wrong.

In the field of international development, breaking down silos in favor of integration is staple advice for the public sector. It appears, for instance, in World Bank reports with titles like *Digital Dividends* (2016), *Big Data in Action for Government* (2017), and *Data-Driven Development* (2018).¹⁷

Private-sector advice concurs. The *Harvard Business Review* describes the “demon that ... often makes initiatives impossible: data silos.” It continues, “expect 80% of the work in becoming data-driven to be integrating your data.”¹⁸ Prominent technology entrepreneur Thomas Siebel’s recent bestselling book *Digital Transformation* declares, “a unified data stack is a prerequisite.”¹⁹

Given the threat posed by digital authoritarianism, this conventional wisdom is dangerous. In the political realm, by analogy, power in a democracy is deliberately siloed among different branches of government and other independent institutions. This can make for slower and messier decision making, but it also brings profound benefits, because a single unified power center provides much greater affordances for tyranny. So too with data.

Some data-sharing can clearly yield efficiencies, but just as clearly, breaking down all silos is neither necessary nor beneficial. It is not obvious why innovation or services would be stifled by denying the tax service unfettered access to individuals' medical records, genetic data, or interactions with local government. Data can instead be shared between silos on a case-by-case basis with appropriate permissions—this is the difference between authoritarian mass surveillance and the limited surveillance necessary to combat crime or terrorism and perform other legitimate government functions. China's social credit system aims to do away with silos, in order to better achieve authoritarian control.²⁰

Siloing data also enhances security in the face of external threats. The disastrous Chinese hack that stole intimate data on about 22 million government employees, including those with security clearances, from the U.S. Office of Personnel Management illustrates the inherent risks of building a giant repository of valuable information.²¹ If the records had been stored separately, the damage from any hack would have been much less severe. Similarly, when the *Titanic* hit an iceberg in 1912, its bulkheads were not tall enough to contain the water in the breached compartments, and the entire ship consequently sank.²²

Civil society's role should be to think carefully about where authoritarian affordances will arise in AI-related technology and what sorts of silos are necessary to prevent them. With respect to COVID-19, public health data must be collected. Contact tracers, for instance, need to document the recent movements and interactions of infected people in order to understand and control the contagion—a central tool in public health since the 1850s. But this data must be rigorously protected, held separately from other government and private-sector data, and eliminated once it is no longer needed, despite the temptation to keep it. Civil society experts in technology, law, policy, and advocacy should all participate in determining how these sorts of distinctions *can* be made, as well as what governments and technology companies *should* do to implement them.

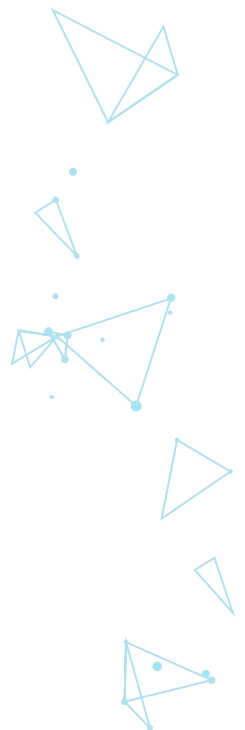
Digital public health surveillance requires democratic accountability and robust legal frameworks to protect both individual freedom and public health, and these in turn are implicated in rapidly advancing discussions on digital sovereignty.

DEMOCRATIC DIGITAL SOVEREIGNTY AND THE PROTECTION OF BASIC STATE FUNCTIONS

Vulnerable and emerging democracies should not be presented with a false dichotomy between either a borderless internet where anything goes or closed authoritarian systems of digital surveillance, censorship, and oppression. Forcing states to choose from those two extremes only helps the case being made by authoritarians. We need to afford fragile democracies plausible alternatives.

While all countries are now interdependent in various ways, the sovereignty of states is still profoundly important. Countries like Germany, France, and the United Kingdom are all working to ensure that they can exert sovereign control over aspects of the internet and digital technologies that they fear could threaten their political systems and societies.²³ This imperative has the unhappy consequence of appearing to validate the long-standing calls of authoritarian states like China and Russia for digital sovereignty.²⁴ But all countries must develop ideas about digital sovereignty. Democracies must confront the problem and develop their own ideas about digital sovereignty rather than clinging to an unrealistic vision from the early years of the internet.

Civil society's role should be to think carefully about where authoritarian affordances will arise in AI-related technology and what sorts of silos are necessary to prevent them.



Until humanity does away with states, states will continue to exist and rest on sovereignty. This does not deny the importance of, for instance, individuals' rights or states' interdependence. Our globalizing world is interdependent *and* states matter profoundly. "Digital sovereignty" as a term should be recaptured for use by liberal democracies by redefining it. Instead of the way that authoritarian states have previously used digital sovereignty—to advocate for absolute control by states over the internet—it should be understood as the digital face of the broader principle of sovereignty as supreme power within a state. This would afford democracies space to articulate more democratic visions for accountable forms of governance in the digital realm.

The following are just a few examples of the state functions that must be extended to the digital realm, particularly in light of the COVID-19 crisis:

- **Ensuring democratic accountability:** People around the world have handed enormous volumes of personal data to powerful technology companies based in foreign countries. Only sovereign states can hold such companies accountable to democratic institutions, like competitively elected legislatures and independent courts, for any abuses by or on their platforms. Democratic governments should be able to impose controls on the spread of truly harmful content like child-abuse imagery, and they must be empowered to enforce legal protections for sensitive medical and public health data. In other words, state officials are there to safeguard the interests of the people they represent.
- **Defending democratic integrity:** Democratic states have an obligation to defend their societies against authoritarian sharp power campaigns, and this requires making and enforcing relevant laws as well as developing cybersecurity capabilities that are fit to purpose and subject to independent oversight. While private-sector allies are vital, democratically accountable leaders need to have the means to respond to authoritarian influence efforts aimed at sowing division and warping domestic politics. The dangers such campaigns can pose are demonstrated by the disinformation and conspiracy theories emanating from China and Russia surrounding COVID-19.²⁵
- **Collecting taxes and responding to economic shocks:** If the AI-related digital economy becomes as large as anticipated, and if that economy cannot be taxed because of international tax avoidance by major technology companies,²⁶ then states will be unable to fund vital services. They will eventually have to exert sovereignty by levying taxes from the relevant firms and activities. Moreover, since the outbreak of COVID-19, states have responded to the threat of economic collapse by providing emergency funding to businesses and individuals on a scale that no private-sector entity could match.

Civil society must help governments constructively think through the challenges of digital sovereignty and help answer a key question: *how can we afford governments models of democratic digital sovereignty?*

Civil society should continue moving toward the recognition that borders matter for data storage, analysis, and flows—and policy researchers should break each area down to develop more granular accounts of how countries can vet and interact with external digital regimes.

IDEAS FOR CIVIL SOCIETY: AFFORD NEW MODELS OF DEMOCRATIC DIGITAL SOVEREIGNTY

Various models of democratic digital sovereignty will likely emerge in the coming years. This discussion need not reinvent the wheel, as it can essentially transfer debates about human rights to the digital sphere.²⁷ Democratic digital sovereignty must balance two factors: sovereignty and the protection of individual freedoms.

- **Control of information storage, analysis, and flows:** The United States currently stores some 92 percent of the Western world's data.²⁸ These democratic states would obviously not allow 92 percent of their cloud data to be stored in China or Russia, which suggests that the location of data storage is a matter of sovereign interest. In fact, France and Germany have launched a European cloud project to avoid dependence on either the United States or China.²⁹ Many other countries face similar challenges as Chinese firms move into the African cloud market,³⁰ and the services of Chinese technology giants like Alibaba already have advantages in regions like Southeast Asia.³¹ In addition to storage, data are increasingly analyzed in the cloud,³² and unfettered flows of information from China or Russia are a live issue given those regimes' efforts at election interference. Much useful civil society work has begun to examine these issues, for example at the Internet and Jurisdiction Policy Network.³³

Civil society should continue moving toward the recognition that borders matter for data storage, analysis, and flows—and policy researchers should break each area down to develop more granular accounts of how countries can vet and interact with external digital regimes. For instance, a state might only allow cloud analysis of its citizens' more personal data in countries that meet specific standards. Civil society advocates could then push to apply these models.

- **Protecting individuals from their own state:** For sovereign control over data to be truly democratic, there must be protections for individual freedoms and human rights, including from abuses by the state in question. However, moving sole responsibility for and control over personal data to individuals is no solution on its own,³⁴ and it would not address unwanted side effects like the spread of misinformation or lack of transparency.³⁵ Instead, the best approach will probably involve some variant of data protection law, whether of the more patchwork U.S. or uniform European Union type,³⁶ and surveillance reform.

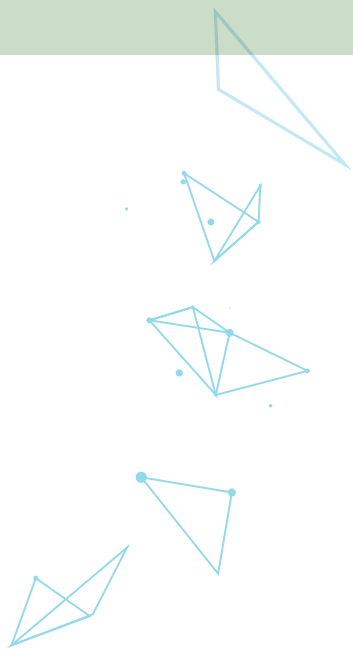
Civil society should argue for laws and regulations that enhance individual privacy and security and prevent routine mass surveillance. This would include, for instance, affording individuals with options to see their data in understandable formats, to easily delete it, and to not have it shared as a simple default.

There is a critical need to develop plausible models of non-authoritarian digital sovereignty that will protect individuals' rights and resist authoritarian influence, as increasing global competition with authoritarian powers will require democracies to find new ways to cooperate (and compete) digitally across borders. The next two sections consider this competition, and specifically how to counter authoritarian sharp power campaigns involving AI-related technologies, both within states and at the international level.

AI AND DUAL-USE MARKETING TOOLS

Microtargeting is a form of online targeted advertising that can employ AI to analyze personal data and identify specific audiences or interests.³⁷ Platforms like Facebook produce the data that make commercial microtargeting possible,³⁸ and that microtargeting apparatus in turn affords political exploitation, as in the Cambridge Analytica scandal.³⁹

Social bots are algorithmic software programs designed to interact with or send information to humans. Bots capable of amplifying commercial messages can also have political uses.⁴⁰ Such bots published perhaps a fifth of all tweets about the 2016 U.S. presidential election and a third of all tweets about Brexit. They may have spread propaganda in 50 countries.⁴¹ Most bots are not yet powered by sophisticated AI, but those enhancements are becoming available and will further automate campaigns.⁴² Conversational “chatbots” or AI personas represent another major field for research and development.⁴³



SHARP POWER AND AI WITHIN GLOBAL SWING STATES

Global competition has intensified over the past decade, with great powers like the United States, China, and Russia competing for influence within states that they might tilt in their favor, such as Indonesia, Hungary, India, or across sub-Saharan Africa. The AI-related technologies afford opportunities for authoritarian states to exert sharp power within these global swing states, amongst which are many fragile democracies or would-be authoritarian regimes that have yet to entrench themselves. Beyond sowing discord via disinformation campaigns, as seen with COVID-19,⁴⁴ AI can help penetrate the open and accessible cultural, academic, media, and publishing sectors within democratic countries. This threat arises from the ways in which the digital marketing business evolved in the U.S.-dominated tech ecosystem, as well as from the technical character of AI itself.

The greatest single factor enabling the authoritarian AI offensive is a profound market failure. The tech industry has made colossal efforts to develop advertising and marketing tools, which is understandable given that global ad spending on social media alone amounted to some US \$84 billion in 2019.⁴⁵ But there is no equivalent market incentive to build tools that defend users from improper influence or manipulation.

Indeed, protecting users costs businesses money. As the huge costs of even basic defensive measures emerged, for instance, Facebook took a big hit. The *Financial Times* described how “investors were particularly spooked in July 2018 by warnings from the company itself about the huge financial costs of tackling problems such as disinformation, data protection and other online abuses.”⁴⁶ This largely explains why Facebook concentrated on cheaper AI-heavy responses to the problem,⁴⁷ even though, as explained below, an effective defense requires many expensive human workers as well. Perhaps a robust democracy like the United States can get away with weaker protections, or perhaps not, but it is a certainty that fragile democracies remain extremely vulnerable. Facebook anticipates most user growth in the Asia-Pacific region, yet it fails globally to transfer content-moderation manuals to foreign markets—let alone providing required local adaptation—and struggles with translation across its dozens of supported languages.⁴⁸

AI’s technical character helps explain why effective defenses against authoritarian information campaigns are costly. AI’s strength at visual or auditory perception enables the creation of “deepfakes”—synthetic but highly convincing media materials. However, because AI lacks contextual knowledge and creativity, information campaigns require human-machine teams to mass-produce effective messaging. Facebook banned some uses of deepfakes in 2020,⁴⁹ but human-AI teams of attackers exploit the context-related weaknesses of AI defenders in many ways. They constantly blur lines by using subtle gradations of fakeness, placement of true content in fake contexts, subtle cropping

of images and video framing, and “satirical” or “humorous” deepfakes that are not banned. An adequate response to these techniques requires expensive human staffers in addition to AI-based detection.

AI affordances for authoritarian information activities are already being exploited quite broadly. A recent survey identified 53 foreign influence efforts targeting 24 countries from 2013 through 2018.⁵⁰ Authoritarian governments are willing to spend heavily when influencing foreign populations.⁵¹

The pervasive employment of AI will shape many other aspects of life, potentially to authoritarians’ liking. Facial recognition systems can be deployed in workplaces, at turnstiles in sporting arenas, or at subway systems’ entry gates. IBM promoted “smart cities” years ago, but China is now forging ahead and building integrated urban surveillance networks at an incredible pace.⁵² There is potential demand for such technology in the developing world, particularly for India’s vast urbanizing population or the extra billion people expected to be born in Africa in the coming decades. If leading democracies fail to offer these societies an alternative to the Chinese version of smart cities and other new AI-related technology, the authoritarian model will succeed by default.

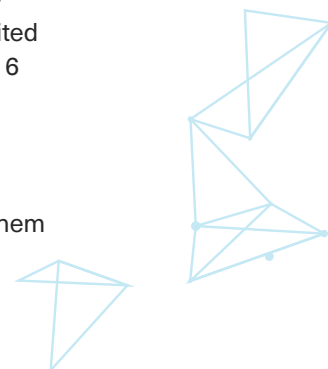
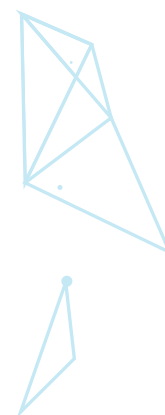
IDEAS FOR CIVIL SOCIETY: TECH—CIVIL SOCIETY COLLABORATIONS AFFORD INDIVIDUALS AND STATES THE MEANS TO DEFEND THEMSELVES

Civil society, in cooperation with government and big tech corporations where possible, can aim to correct market failures by giving citizens the means to safeguard democratic integrity against malign information operations, while preserving the basic openness of the information environment.

- **Civil society and digital technical experts should increase efforts to co-create solutions.** Above all, civil society should find ways to work with technical experts to develop solutions that can be applied in a variety of settings around the world. These solutions must be cost effective and preferably “open source,”⁵³ and they must allow local partners in various countries to draw on their own ground-truth insights, as well as a global network of expertise and other resources. Given the scarcity of such expertise, it is important to maintain a global perspective and ensure that the need to mitigate threats in fragile democracies is not overshadowed by prominent political concerns in rich countries like the United States, such as algorithmic discrimination or lack of diversity in big tech.⁵⁴

“Choice Shield” is one example of an early-stage project that emerged from interactions among academics from the cognitive and communication sciences, civil society, and technologists.⁵⁵ It aims to afford people the ability to choose what they see on social media—without censorship—using an app or browser extension. Users can decide how many manipulated images they want to see, and select which organizations will rate those images as manipulated. The code and tools will be open source. Conceptual prototypes piloted in two 2019 studies showed considerable appetite among users for control over what they saw on Facebook. Tools that give users more tailored control already exist in a more limited version,⁵⁶ and revealingly there was some legal pushback from Facebook before the 2016 U.S. election changed the political climate.⁵⁷

- **Protecting elections requires building technical capabilities ahead of time and sustaining them within fragile democracies.** When it comes to funding, global civil society must take a long-term approach, building technical capabilities and sustaining them over time rather than generating ephemeral projects shortly before national elections in fragile democracies.



- **Civil society groups should push—globally and in each country—for social media platforms to adequately fund and implement appropriate, carefully tailored, and well-informed content moderation in all countries where they operate, and not just during elections.** Activists and users in fragile democracies should not have to address their concerns to powerless local representatives or a distant corporate headquarters in the United States.
- **The integrity of the information ecosystem must be defended.** Civil society will have to devote attention to the broader information environment. Combating AI-enabled influence operations requires a healthy media landscape with diverse and independent news outlets—including public service broadcasting where possible—and a well-crafted and well-enforced framework of domestic laws.

Similar ideas apply to areas like smart cities—co-creation, cost effective and open source methods, and global foundations with local understanding. That global scale is key for AI.

SHARP POWER AND AI IN INTERNATIONAL FORA

Much about AI-related technologies happens at global scale. The United States and China, with their respective corporate tech titans, compete for influence in international fora. They play a crucial role in shaping the potential digital futures of the world’s roughly 5 billion unique mobile phone users, 4.5 billion internet users, and 3.8 billion active social media users.⁵⁸

Global norms are one area of competition, with important multilateral work on AI ethics taking place at fora like the Organization for Economic Co-operation and Development (OECD) and eminent international commissions that—when led by democracies—stress safeguards against election interference and for human rights.⁵⁹

Technical standardization, however, represents an equally if not more significant area of competition. Standardized specifications enable the interoperability of products and technologies.⁶⁰ They are crucial because of what they afford: depending on its design, the AI being built into the fabric of people’s lives could either facilitate or obstruct the formation of integrated authoritarian surveillance states.

It matters profoundly, for instance, whether digital things—toasters, cars, lights, office furniture, medical equipment—have privacy baked into their design and defaults, or if they form an open and integrated book for comprehensive surveillance. Many experts argue that authoritarian governments tried to embed the latter model into standards for the “internet of things” at the United Nations’ International Telecommunication Union (ITU) through a “Digital Object Architecture” scheme that would have assigned each digital object a unique, persistent, government-registered identifier.⁶¹ If that happened, the pervasive technology would naturally afford authoritarianism, even if a fragile democracy’s domestic safeguards staved it off in practice. Similar debates surround facial recognition, video monitoring, and city and vehicle surveillance.⁶²

Standards are voluntary, and authoritarian states cannot force them on powerful democracies like the United States. Indeed, Europe and North America can draw on standard-setting bodies—such as the Institute of Electrical and Electronics Engineers (IEEE) and the 3rd Generation Partnership Project (3GPP)—that are dominated by their domestic industry players. But international fora like the ITU, the International Organization for Standardization (ISO), or the International Electrotechnical Commission (IEC) are pivotal for AI’s effects on fragile democracies or swing states for four reasons:

- These bodies' standards are often adopted by member states that lack the resources to develop standards themselves, particularly developing African, Middle Eastern, and Asian states that have accepted infrastructure projects and surveillance technology sponsored by China's Belt and Road Initiative (BRI).⁶³
- Standards that allow the measurement and improvement of AI products' quality, effectiveness, and safety may increase social acceptance in new markets,⁶⁴ broadening the technologies' potential impact.
- Standards can favor one country's products and cement commercial advantages. A standard put forward by China's ZTE and China Mobile and accepted in June 2019 governs the "requirements and functional architecture of a smart street light service," including an option to "add video monitoring capabilities when deploying smart street lights." The requirements not only raise surveillance concerns, but also reportedly "reflect the design of ZTE's Smart Street 2.0 street light, including back-end architecture and functionality," providing a big edge to the company.⁶⁵
- Standards afford greater or lesser individual protections. They could enable or limit the use of streetlight surveillance to identify and track people in public, or the exploitation of digital things with inbuilt government identifiers to amass comprehensive information about people's personal lives.

China also influences international tech standardization by changing facts on the ground. Multiple "memorandums of understanding" with BRI partner countries incorporate standardization clauses, and China has translated more than 500 domestic standards into English.⁶⁶ The country's vast internal market lends considerable influence to these rules. The importance of standard setting to the regime is underscored by the attention it has apparently received from General Secretary Xi Jinping, who reportedly declared that "standards determine quality," and that one can achieve "high quality only with high standards."⁶⁷

But Chinese influence on standards, while growing, should not be overstated, and pushing back too hard poses risks. China far from dominates key standard-setting bodies like the ISO or IEC, and its new technical expertise deserves a legitimate role in establishing global standards. For instance, although China increased its participation in ISO technical committee and working group secretariats between 2011 and 2018, China's share was still under 10 percent in 2018. Its share continues to be dwarfed by the European Union, United Kingdom, United States, and Japan who together hold almost all the rest.⁶⁸ Moreover, splitting international standards would only escalate global competition. China is rumored to be considering an "Asian Standardization Organization"—akin to the Asian Infrastructure Investment Bank, which attempts to rival the Bretton Woods economic institutions created by democratic powers—that would be available first to Asian BRI partner countries and then more widely.⁶⁹

The question for civil society is how best to resist authoritarian influence in international fora.

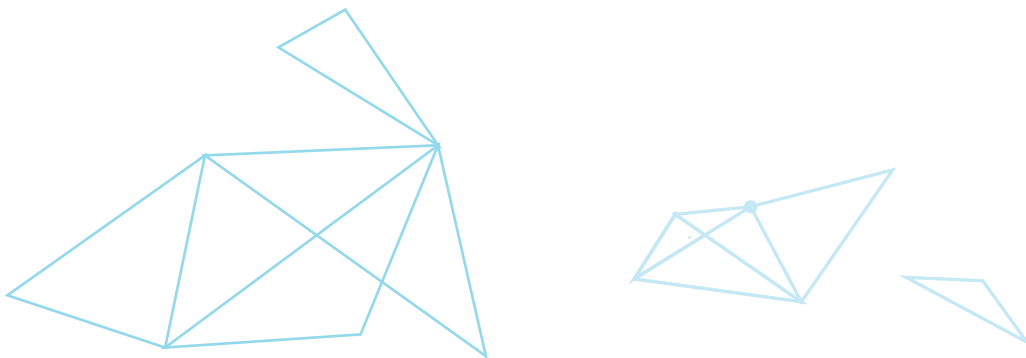


Standards are voluntary, and authoritarian states cannot force them on powerful democracies ... But international fora like the International Telecommunication Union (ITU), the International Organization for Standardization (ISO), or the International Electrotechnical Commission (IEC) are pivotal for AI's effects on fragile democracies or swing states.

IDEAS FOR CIVIL SOCIETY: RESIST SHARP POWER IN INTERNATIONAL FORA

To engage constructively and effectively in international fora, four clear steps must be taken by civil society.

- **First, to achieve global aims—which are needed given AI's global scale—civil society requires new funding and collaboration with tech expertise.** Given scarce global AI expertise,⁷⁰ this will have to include links between technical experts in well-resourced democracies and local organizations focused on human rights or consumer advocacy.
- **Second, civil society should aim for ambiguous, overlapping global AI governance without exacerbating Sino-U.S. competition.** Effective governance should involve multistakeholder groups (including governments, private sector, academics, and civil society), while simultaneously limiting the broader risks that could result from splitting up multilateral organizations like the ITU, ISO, and IEC. Civil society should help develop ideas of non-authoritarian digital sovereignty that protect individual rights. Those more granular approaches to information storage, analysis, and flow will facilitate new multistakeholder ways to bolster cooperation between democracies and compete with authoritarian influence.
- **Third, civil society should use international fora to help develop and promote AI standards that afford democratic practices and individual privacy.** For instance, the strategic encouragement of data silos militates against a centralized and integrated “internet of things” that might be exploited by state authorities or other malign actors. Democratic digital sovereignty related to AI standards can build in privacy or even human rights by design.⁷¹ Civil society should also anticipate pushback from some Western companies. Privacy may be against some current business models (for example, Facebook)⁷² but more compatible with others (such as Microsoft or Apple, each of whose market capitalization of approximately \$1.4 trillion dwarfs Facebook’s valuation of around \$610 billion).
- **Finally, civil society should specifically contribute to transparency and oversight of global AI governance at international and regional fora.** The ITU notably lacks transparency about how decisions are reached, and civil society representatives rarely attend standard-setting meetings. Independent civil society monitoring and analysis can help countries with limited technical expertise better understand the intended and unintended consequences of potential standards and norms under discussion at these fora.



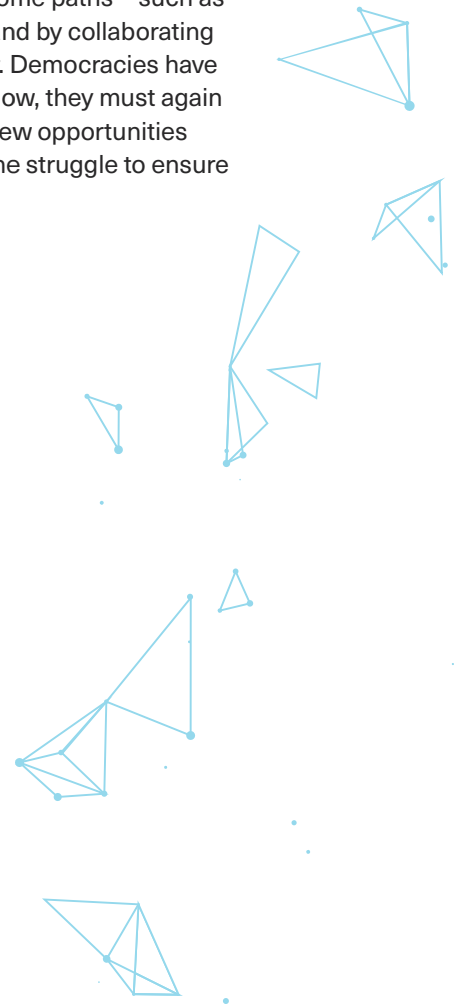
CONCLUSION

If China offers you a free lunch then perhaps, as the saying goes, you are the lunch. But if hundreds of millions of Chinese people seem to be eating well, few others will reject an offer of apparently free food—especially when there is no obvious alternative. Similarly, authoritarian standards for AI-related technologies may appear acceptable, without obvious alternatives. Civil society can help afford alternatives that are better for democracy.

For many years now, smartphones and other common devices have conducted constant surveillance to provide users with desirable services. Economic growth has come to depend on digitization and the collection and processing of big data. In 2020, democracies and authoritarian regimes alike are employing intrusive health-related surveillance to combat COVID-19, and in some cases they appear to be achieving success.⁷³

As daunting and inexorable as they may seem, AI-related technologies are still young, and it remains possible to continue delivering their many benefits while minimizing the affordances that could facilitate shifts toward authoritarianism.

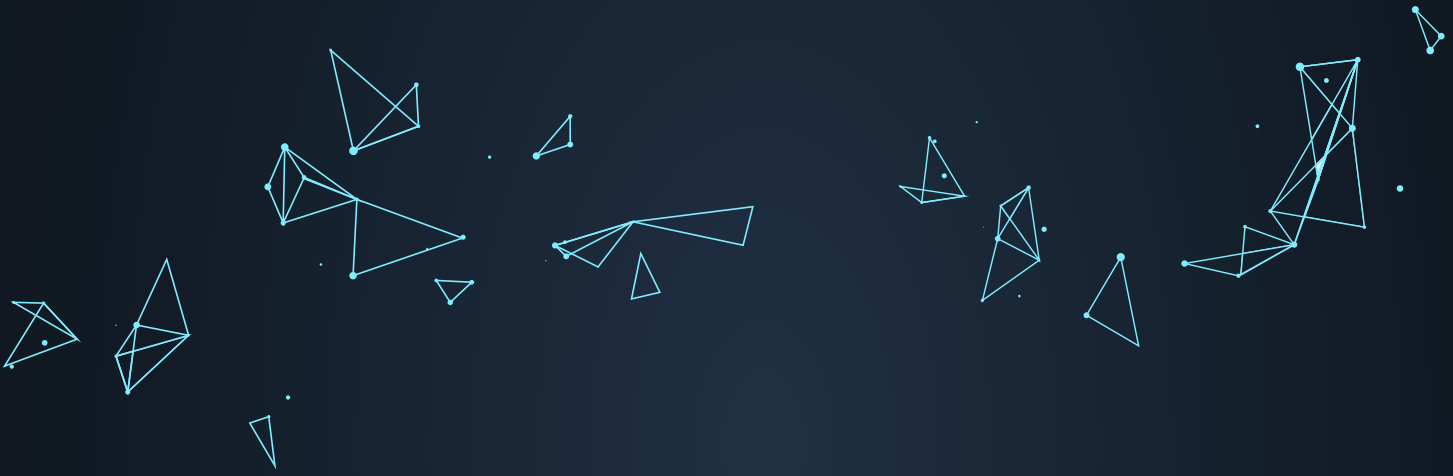
Civil society can contribute to this goal by anticipating the dangers afforded by some paths—such as the heedless elimination of data silos that could help protect individual rights—and by collaborating with technologists to develop better models for fragile democracies in particular. Democracies have adapted and thrived through past episodes of profound technological change. Now, they must again adapt, not least to develop models of democratic digital sovereignty and afford new opportunities rooted in democratic norms. A robust civil society may be the greatest asset in the struggle to ensure that the current digital revolution results in more resilient liberal democracies.



ENDNOTES

- 1 Christopher Walker, Shanthi Kalathil, and Jessica Ludwig, "The Cutting Edge of Sharp Power," *Journal of Democracy* 31, no. 1 (January 2020): 124–37.
- 2 For a recent review in cognitive science see Maxwell J. D. Ramstead, Samuel P. L. Veissire, and Laurence J. Kirmayer, "Cultural Affordances: Scaffolding Local Worlds Through Shared Intentionality and Regimes of Attention," *Frontiers in Psychology* 7 (2016).
- 3 Such examples are discussed in David Cannadine, *Victorious Century: The United Kingdom, 1800–1906* (Penguin UK, 2017).
- 4 A broad characterization is used here, because the term AI has come to refer to many significant things that are not captured by narrower definitions.
- 5 For further details see Nicholas D. Wright, ed., *Artificial Intelligence, China, Russia, and the Global Order* (Maxwell Air Force Base, Alabama: Air University Press, 2019). The definitions draw also on UK Information Commissioner's Office (ICO), "Big Data, Artificial Intelligence, Machine Learning and Data Protection," 2017, <https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf>.
- 6 This tighter definition of AI itself is also highly debated, and is further subdivided in various ways. For instance, one might contrast "general AI" that can apply its intelligence to many tasks, against an AI such as Siri that is programmed to essentially perform a single task ("narrow AI"). This also broadly corresponds to "strong AI" versus "weak AI."
- 7 ICO, "Big Data, Artificial Intelligence, Machine Learning and Data Protection."
- 8 Deb Landau, "Artificial Intelligence and Machine Learning: How Computers Learn," IQ, 17 August 2016, <https://iq.intel.com/artificial-intelligence-and-machine-learning>.
- 9 Gary King, Jennifer Pan, and Margaret E. Roberts, "How Censorship in China Allows Government Criticism but Silences Collective Expression," *American Political Science Review* 107, no. 2 (May 2013): 326–43.
- 10 Wright, *Artificial Intelligence, China, Russia, and the Global Order*.
- 11 "China: Big Data Fuels Crackdown in Minority Region," Human Rights Watch, 26 February 2018, www.hrw.org/news/2018/02/26/china-big-data-fuels-crackdown-minority-region. "China's Algorithms of Repression: Reverse Engineering a Xinjiang Police Mass Surveillance App," Human Rights Watch, 1 May 2019, www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass-surveillance.
- 12 Bethany Allen-Ebrahimi, "Exposed: China's Operating Manuals for Mass Internment and Arrest by Algorithm," International Consortium of Investigative Journalists, 24 November 2019, www.icij.org/investigations/china-cables/exposed-chinas-operating-manuals-for-mass-internment-and-arrest-by-algorithm. The ICIJ translation of the Chinese Government document read: "When students enter and leave the training center, their information must be promptly entered into the public security 'integrated' platform. In accordance with the requirements of 'one person, one file,' the student education and training files shall be established, and the students' records in performance, rewards and punishments, and grade improvements, etc. in the areas of ideological education, study and training, and compliance and discipline, etc. shall be collected in a timely and accurate manner."
- 13 Rogier Creemers, "China's Social Credit System: An Evolving Practice of Control," SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, 9 May 2018), <https://papers.ssrn.com/abstract=3175792>.
- 14 Wright, *Artificial Intelligence, China, Russia, and the Global Order*.
- 15 "E-government refers to government agencies' use of information technologies ... that have the ability to transform relations with citizens, businesses, and other arms of government. These technologies can serve a variety of different ends: better delivery of government services to citizens, improved interactions with business and industry, citizen empowerment through access to information, or more efficient government management." Roberto Panzardi, Carlos Calcopietro, and Enrique Fanta Ivanovic, "New Economy Sector Study: Electronic Government and Governance: Lessons for Argentina," World Bank, 2002, <http://documents1.worldbank.org/curated/en/527061468769894044/pdf/266390WPOE1GovIgentina1Final1Report.pdf>.
- 16 Thomas M. Siebel, *Digital Transformation: Survive and Thrive in an Era of Mass Extinction* (New York: Rosetta Books, 2019). Chapter 2 describes numerous digital transformation indices.
- 17 "Big Data in Action for Government: Big Data Innovation in Public Services, Policy, and Engagement," World Bank, 3 April 2017, <http://documents.worldbank.org/curated/en/176511491287380986/Big-data-in-action-for-government-big-data-innovation-in-public-services-policy-and-engagement>. *World Development Report 2016: Digital Dividends* (Washington, DC: World Bank Publications, 2016). *Information and Communications for Development 2018: Data-Driven Development* (Washington, DC: World Bank Publications, 2018).
- 18 Edd Wilder-James, "Breaking Down Data Silos," *Harvard Business Review*, 5 December 2016, <https://hbr.org/2016/12/breaking-down-data-silos>.
- 19 Siebel, *Digital Transformation: Survive and Thrive*.
- 20 Creemers, "China's Social Credit System."
- 21 David E. Sanger, *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age* (New York: Penguin Random House, 2019). David Perera, "Lawsuit Seeks Relief from Cyberspying - CIA and OPM: Rethinking the Silo," Politico, 14 July 2015, www.politico.com/tipsheets/morning-cybersecurity/2015/07/lawsuit-seeks-relief-from-cyberspying-cia-and-opm-rethinking-the-silo-212543.
- 22 "Sinking of the Titanic," National Geographic Society, 26 March 2012, www.nationalgeographic.org/media/sinking-of-the-titanic.
- 23 Kenneth Propp, "Waving the Flag of Digital Sovereignty," Atlantic Council (blog), 11 December 2019, www.atlanticcouncil.org/blogs/new-atlanticist/waving-the-flag-of-digital-sovereignty. Britain seeks a digital tax and controlling childrens' access to the internet without explicitly using the language of "sovereignty."
- 24 Andrei Soldatov and Irina Borogan, *The Red Web: The Struggle Between Russia's Digital Dictators and the New Online Revolutionaries* (New York: PublicAffairs, 2015), 233–38. Elizabeth C. Economy, *The Third Revolution: Xi Jinping and the New Chinese State* (Oxford: Oxford University Press, 2018), chapter 3.
- 25 Julian E. Barnes, Matthew Rosenberg, and Edward Wong, "As Virus Spreads, China and Russia See Openings for Disinformation," *New York Times*, 28 March 2020, www.nytimes.com/2020/03/28/us/politics/china-russia-coronavirus-disinformation.html.
- 26 Richard Waters, "Google to End Use of 'Double Irish' as Tax Loophole Set to Close," *Financial Times*, 1 January 2020, www.ft.com/content/991f11ae-2c51-11ea-bc77-65e4aa615551.
- 27 Eileen Donahoe and Megan MacDuffee Metzger, "Artificial Intelligence and Human Rights," *Journal of Democracy* 30, no. 2 (April 2019): 115–26.
- 28 Propp, "Waving the Flag of Digital Sovereignty."
- 29 Stefan Nicola and Helene Fouquet, "Amazon Brushes Off European Challenge to Its Cloud Business," Bloomberg, 29 October 2019, www.bloomberg.com/news/articles/2019-10-29/france-joins-german-cloud-effort-to-challenge-amazon-and-alibaba.
- 30 Toby Shapshak, "South Africa Is Now a Major Hub for Big Tech's Cloud Datacenters," Quartz Africa, 20 March 2019, <https://qz.com/africa/1576890/amazon-microsoft-huawei-building-south-africa-data-hubs>.
- 31 Yifan Yu, "Amazon Prepares to Battle with Alibaba in Asia's Cloud," *Nikkei Asian Review*, 4 May 2019, <https://asia.nikkei.com/Business/Companies/Amazon-prepares-to-battle-with-Alibaba-in-Asia-s-cloud>. Abigail Opiah, "Chinese Cloud Firms Now Account for 40% of the APAC Cloud Market," Data Economy, 24 May 2019, <https://data-economy.com/chinese-cloud-firms-now-account-for-40-the-of-apac-cloud-market>.
- 32 Siebel, *Digital Transformation*.
- 33 See www.internetjurisdiction.net.
- 34 E.g. Tim Berners-Lee—led <https://solid.mit.edu>.
- 35 For the side effects see Kieron O'Hara and Wendy Hall, "Four Internets: The Geopolitics of Digital Governance," CIGI Paper No. 206, Centre for International Governance Innovation, December 2018.
- 36 Stephen P. Mulligan, Wilson C. Freeman, and Chris D. Linebaugh, "Data Protection Law: An Overview," Congressional Research Service, R45631, 25 March 2019.
- 37 Information Commissioner's Office, "Microtargeting," 8 May 2019, <https://ico.org.uk/your-data-matters/be-data-aware/social-media-privacy-settings/microtargeting>. Nitasha Tiku, "Welcome to the Next Phase of the Facebook Backlash," *Wired*, 21 May 2017, www.wired.com/2017/05/welcome-next-phase-facebook-backlash.
- 38 John Naughton, "'The Goal Is to Automate Us': Welcome to the Age of Surveillance Capitalism," *The Guardian*, 20 January 2019, www.theguardian.com/technology/2019/jan/20/shoshana-zuboff-age-of-surveillance-capitalism-google-facebook.
- 39 See *The Guardian* series, "The Cambridge Analytica Files," www.theguardian.com/news/series/cambridge-analytica-files.
- 40 Nicholas Confessore et al., "The Follower Factory," *New York Times*, 27 January 2018, www.nytimes.com/interactive/2018/01/27/technology/social-media-bots.html.
- 41 Bruce Schneier, "Bots Are Destroying Political Discourse As We Know It," *The Atlantic*, 7 January 2020, www.theatlantic.com/technology/archive/2020/01/future-politics-bots-drowning-out-humans/604489.
- 42 Samuel Woolley, "We're Fighting Fake News AI Bots by Using More AI. That's a Mistake," MIT Technology Review, 8 January 2020, www.technologyreview.com/s/614810/were-fighting-fake-news-ai-bots-by-using-more-ai-thats-a-mistake. Bernard Marr, "How Artificial Intelligence Is Making Chatbots Better For Businesses," *Forbes*, 18 May 2020, www.forbes.com/sites/bernardmarr/2018/05/18/how-artificial-intelligence-is-making-chatbots-better-for-businesses.

- 43 Andreas Vogel and Nicholas D. Wright, "Alexa Is Both Friend and Sales Robot. That's a Problem," *Slate*, 10 May 2019, <https://slate.com/technology/2019/05/alexa-amazon-voice-assistant-conflict-interest-regulation.html>.
- 44 Barnes, Rosenberg, and Wong, "As Virus Spreads, China and Russia See Openings for Disinformation."
- 45 John McCarthy, "Social Media Ad Budgets Continue to Grow at 'Expense of Print', up 20% in 2019," *The Drum*, 7 October 2019, www.thedrum.com/news/2019/10/07/social-media-ad-budgets-continue-grow-expense-print-up-20-2019.
- 46 Tim Bradshaw, "Facebook Shares Hit Record High, Surpassing 2018 Peak," *Financial Times*, 10 January 2020, www.ft.com/content/5fda80c8-33a3-11ea-9703-eea0cae3f0de.
- 47 Madhumita Murgia and Hannah Murphy, "Can Facebook Really Rely on Artificial Intelligence to Spot Abuse?" *Financial Times*, 7 November 2019, www.ft.com/content/69869f3a-018a-11ea-b7bc-f3fa4e77dd47.
- 48 "Facebook's Flood of Languages Leave It Struggling to Monitor Content," Reuters, 23 April 2019, www.reuters.com/article/us-facebook-languages-insight-idUSKCN1RZ0DW.
- 49 Sam Shead, "Facebook to Ban 'Deepfakes,'" BBC News, 7 January 2020, www.bbc.com/news/technology-51018758.
- 50 Diego A. Martin and Jacob N. Shapiro, "Trends in Online Foreign Influence Efforts," Princeton University, 2019.
- 51 "Gaining Face - China Is Using Facebook to Build a Huge Audience around the World," *The Economist*, 20 April 2019, www.economist.com/graphic-detail/2019/04/20/china-is-using-facebook-to-build-a-huge-audience-around-the-world.
- 52 Kai-Fu Lee, *AI Superpowers: China, Silicon Valley, and the New World Order* (Houghton Mifflin Harcourt, 2018).
- 53 Mike Volpi, "How Open-Source Software Took over the World," TechCrunch, 12 January 2019, <http://social.techcrunch.com/2019/01/12/how-open-source-software-took-over-the-world>. "The Rise of Open-Source Computing," *The Economist*, 3 October 2019, www.economist.com/leaders/2019/10/03/the-rise-of-open-source-computing.
- 54 Elizabeth Gibney, "The Battle for Ethical AI at the World's Biggest Machine-Learning Conference," *Nature* 577 (24 January 2020): 609.
- 55 The author's collaborators are: Karen Dill-Shackelford (Fielding University), Aurie Babarinsa (Carnegie Mellon University, formerly at Twitch) Jevin West (University of Washington), Don Grant (Resolutions Teen Center), and Richard Petty (Ohio State University). Contact the author at nick@intelligentbiology.co.uk for data or further details.
- 56 <https://socialfixer.com/index.html> and more recently www.media.mit.edu/projects/gobo/overview.
- 57 Violet Blue, "Popular plugin Social Fixer surrenders to Facebook legal menacing," ZDNet, 6 October 2013, www.zdnet.com/article/popular-plugin-social-fixer-surrenders-to-facebook-legal-menacing.
- 58 "Digital in 2020," We Are Social, <https://wearesocial.com/digital-2020>.
- 59 One example is the Global Commission on the Stability of Cyberspace, "Advancing Cyberstability: Final Report," November 2019, <https://cyberstability.org/report>. The report's second of its eight proposed norms is: "State and non-state actors must not pursue, support or allow cyber operations intended to disrupt the technical infrastructure essential to elections, referenda or plebiscites" (p. 21). Of the report's four principles, one is "Respect for Human Rights: Efforts to ensure the stability of cyberspace must respect human rights and the rule of law" (p.18). The OECD published principles at <https://www.oecd.org/going-digital/ai/principles>.
- 60 Bjorn Fagersten and Tim Ruhling, *China's Standard Power and Its Geopolitical Implications for Europe* (Utrikespolitiska institutet: UI Brief, March 2019), www.ui.se/butiken/uis-publikationer/ui-brief/2019/chinas-standard-power-and-its-geopolitical-implications-for-europe.
- 61 Dominique Lazanki, "The Problem With the United Nations Setting Tech Standards for Your Internet Devices," Council on Foreign Relations, 22 September 2016, www.cfr.org/blog/problem-united-nations-setting-tech-standards-your-internet-devices. Exeter University, "Digital Object Architecture and IoT Standardisation," www.internetpolicystreams.com/news/item/362-digital-object-architecture-and-iot-standardisation. John Chen et al., "China's Internet of Things: Report for the U.S.- China Economic and Security Review Commission" (Vienna, Virginia: SOSI, October 2018), www.uscc.gov/research/chinas-internet-things.
- 62 Madhumita Murgia, Yuan Yang, and Anna Gross, "Chinese Tech Groups Shaping UN Facial Recognition Standards," *Financial Times*, 1 December 2019, www.ft.com/content/c3555a3c-0d3e-11ea-b2d6-9b4d1957a67.
- 63 Ibid.
- 64 Martijn Rasser et al., *The American AI Century: A Blueprint for Action* (Center for New American Security, 17 December 2019). Jeffrey Ding, Paul Triolo, and Samm Sacks, "Chinese Interests Take a Big Seat at the AI Governance Table," *New America*, 20 June 2018, www.newamerica.org/cybersecurity-initiative/digichina/blog/chinese-interests-take-big-seat-ai-governance-table.
- 65 Murgia, Yang, and Gross, "Chinese Tech Groups Shaping UN Facial Recognition Standards."
- 66 Fagersten and Ruhling, *China's Standard Power and Its Geopolitical Implications for Europe*.
- 67 Chen et al., "China's Internet of Things: Report for the U.S.- China Economic and Security Review Commission," 61.
- 68 See Figures 1 and 3 in Fagersten and Ruhling, *China's Standard Power and Its Geopolitical Implications for Europe*, pp. 4 and 10.
- 69 Ibid.
- 70 "2019 Global AI Talent Report," Element AI, 2 April 2019, www.elementai.com/news/2019/2019-global-ai-talent-report.
- 71 Donahoe and MacDuffee Metzger, "Artificial Intelligence and Human Rights."
- 72 Amnesty International, "Surveillance Giants: How the Business Model of Facebook and Google Threatens Human Rights," Amnesty International, 21 November 2019, www.amnesty.org/download/Documents/POL3014042019ENGLISH.PDF.
- 73 Nicholas Wright, "Coronavirus and the Future of Surveillance," *Foreign Affairs*, 6 April 2020, www.foreignaffairs.com/articles/2020-04-06/coronavirus-and-future-surveillance.



**National Endowment
for Democracy**

Supporting freedom around the world



ABOUT THE NATIONAL ENDOWMENT FOR DEMOCRACY

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 non-governmental 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.

ABOUT THE FORUM

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.

