THE GLOBAL STRUGGLE OVER AI SURVEILLANCE

// **STEVEN FELDSTEIN,** SENIOR FELLOW, CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE

THE RISE OF AI SURVEILLANCE

Through several key advances that enable approaches such as facial recognition, social media monitoring, and smart policing techniques, AI technology is extending the power of states to monitor citizens. While entrenched autocracies are making eager use of these new capacities, more open political systems are also incorporating AI surveillance tools, raising troubling questions about the impact on due process, free expression, and active citizenship.

In the context of global democratic backsliding, unregulated AI surveillance threatens to widen gaps in the rule of law and tilt the playing field toward illiberal governments in settings where checks and balances are already weakened. Civil society campaigns are drawing attention to these dangers, and established democracies are moving toward defining clearer ground rules for AI surveillance use. To bring principles into practice, however, more robust leadership from democracies, active collaboration among stakeholders, and sustained engagement with the broader public are needed.

AI systems augment government surveillance powers in several ways. First, AI facilitates the automation of operations previously carried out by humans, for instance by using algorithms to match images with footage. Second, AI technology can classify information and predict patterns autonomously,

enabling automated systems to flag perceived anomalies and attempt to anticipate future events.[1] Third, advanced AI sifts through an unprecedented volume of data. These elements benefit law enforcement agencies, but they also **create threats of privacy violations and investigative overreach**, not to mention **discriminatory bias** (for example, when facial recognition tools misidentify members of particular racial or ethnic groups at higher rates). The weight of both intentional abuse and flawed design often falls heaviest on marginalized communities.

Surveillance risks extend across regime types

In authoritarian settings, these new capabilities have obvious potential to deepen repression. Most notably, researchers have investigated the **combined use of biometric surveillance and social media monitoring to feed into an integrated system of physical and digital control in China's Xinjiang province**.[2] While this comprehensive application of AI tools to repress an entire region still represents an extreme case, the potential for surveillance breakthroughs to subvert expectations of privacy, facilitate political persecution or group discrimination, and erode the freedoms of expression and association is not unique to autocracies.[3]

The potential for surveillance breakthroughs to subvert or erode rights and freedoms is not unique to autocracies.

Advocates in liberal democracies have justifiable concerns about authorities leveraging new technologies in antidemocratic ways. In fact, the use of electronic surveillance to monitor and harass civil rights activists, protesters, and Native American organizations led to passage of the United States' 1978 Foreign Intelligence Surveillance Act, which set parameters for authorizing certain electronic surveillance activities.[4] Today, against the backdrop of expanding and controversial uses of AI surveillance tools, as well as democratic backsliding trends in some settings, liberal governments are struggling to find an acceptable balance between maintaining public order and protecting civil liberties.

In **France**, the mayor of Marseille has initiated the **"Big Data of Public Tranquility Project,"** which will incorporate predictive policing technology (involving the mass collection and analysis of data in order to anticipate, deter, and respond to future criminal activity) as well as thousands of video cameras purchased from PRC tech giant ZTE.[5] Recent reports have shown that public agencies in the **United States** are making wide use of **facial recognition technology (FRT), including software developed through social-media scraping by the private vendor Clearview AI**.[6]

U.S. police departments have also leaned heavily on social media surveillance and facial recognition algorithms to identify suspects in the January 6, 2021 Capitol Hill insurrection.[7] In **Israel**, the military is implementing a program that **integrates FRT with smart phone and video surveillance devices to monitor Palestinians**.[8] In many cases, new surveillance infrastructure is spreading under the radar, with these systems drawing public notice and debate only after they have already been deployed.

In weak democracies and hybrid regimes, the risks that advanced surveillance technologies pose are acute. Where democratic backsliding has already weakened rule of law protections, as in Poland, Hungary, India, or the Philippines, these tools offer **new possibilities for tracking and intimidating dissenters, monitoring political opponents, and preempting challenges to government power**.[9]

Public documentation shows how these regimes are embracing high-tech surveillance. In **India**, authorities are using FRT to track down protesters.[10] In **Serbia**, officials contracted with Huawei to establish a surveillance network that will soon "cover every significant street and passageway" of Belgrade (see essay by Danilo Krivokapić on pp. 23–25).[11] **Pakistan's government**, meanwhile, purchased an $18.5 million system from the Canadian firm Sandvine to surveil online traffic and monitor communications.[12]

To what extent will the growing availability of AI surveillance tools in swing states (hybrid regimes or weak democracies, defined for purposes of this paper using V-Dem electoral democracy scores) speed democratic backsliding, fuel repressive practices, or undermine the rule of law? The answer to this question is likely to be shaped by the interplay of a globalized surveillance market, with China as a major player; domestic political conditions in the countries where surveillance tools are deployed; and ongoing efforts by national governments, civil society groups, and the wider global community to craft new norms around AI.

Police in Kuala Lumpur, Malaysia operate a drone. Around the world, law enforcement officials make use of novel surveillance technologies to keep tabs on the public.

THE GLOBAL AI SURVEILLANCE MARKET

AI surveillance technology is becoming increasingly ubiquitous, particularly as its cost comes down and relevant components become more affordable. As Stanford's 2021 AI Index notes: **"The technologies necessary for large-scale surveillance are rapidly maturing, with techniques for image classification, face recognition, video analysis, and voice identification all seeing significant progress."**[13]

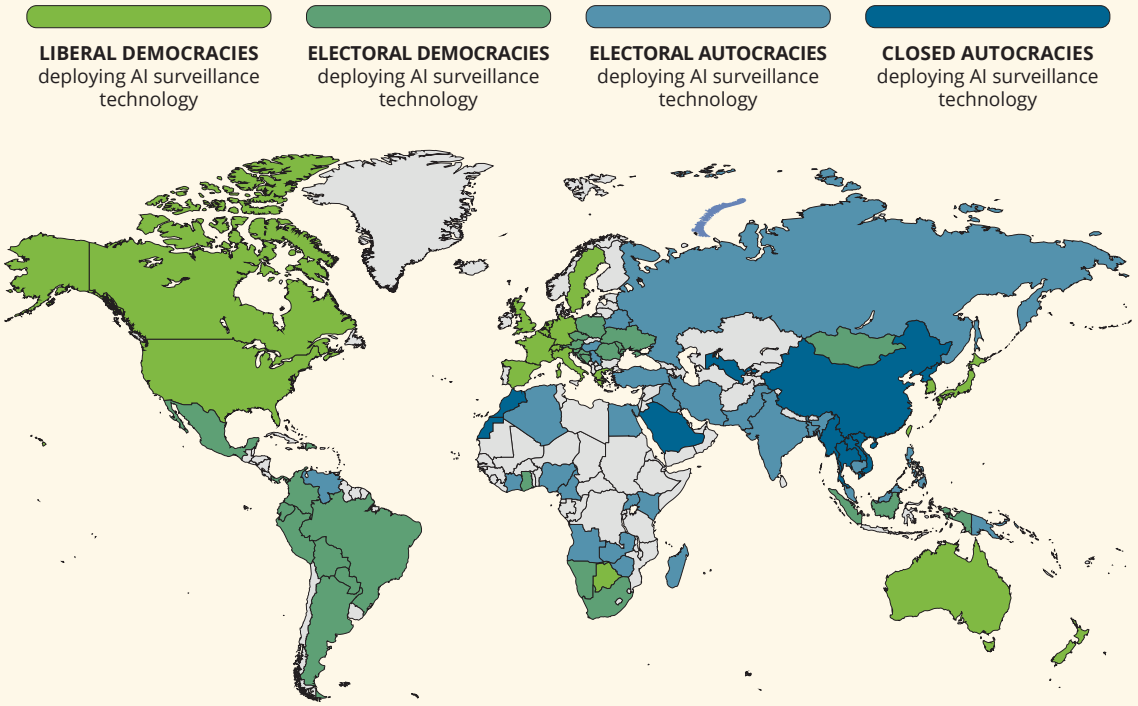
In 2019, I released an index that used open-source content analysis to measure the global prevalence of four types of AI-powered surveillance systems.[14] These are: FRT (biometric technology that analyzes human faces for identification purposes), smart or safe cities (urban networks comprising thousands of sensors that transmit real-time data to facilitate city management), smart policing techniques (data-driven methods for police response, investigations, crime prediction, and even sentencing decisions), and social media monitoring (algorithms that automatically monitor millions of online communications). The index was updated in 2022.[15] As the Figure below shows, slightly more democratic governments than authoritarian regimes have known AI surveillance capabilities: **52 of the 97 countries with these tools are classified by V-Dem as liberal or electoral democracies.**[16]

52 of 97

Slightly more democratic governments than authoritarian regimes have known AI surveillance capabilities.

FIGURE

Global Presence of AI-Powered Surveillance Technologies



Classifications according to Michael Coppedge et al., "V-Dem Codebook v12," Varieties of Democracy [V-Dem] Project, 2022, pp. 287–88, using data for 2021.

PRC companies are popular suppliers of AI surveillance tools for governments

Chinese companies remain at the forefront when it comes to providing advanced artificial intelligence/machine learning (AI/ML) tools that enable governments to carry out mass surveillance. These firms are seeking out new markets vigorously, and state subsidies often support their efforts. Governments around the world have eagerly adopted the low-cost imports enabled by these policies: Surveillance cameras manufactured by Hikvision and Dahua now account for "nearly 40 percent" of the global market.[17] **Chinese surveillance technology is used in over eighty countries spanning every region of the world.**[18]

40%

Surveillance cameras manufactured by Hikvision and Dahua now account for "nearly 40 percent" of the global market.

PRC surveillance exports build on the continuing development of these technologies at home. Despite international outrage over surveillance practices in Xinjiang, firms such as Huawei and Dahua have been working with the Chinese government to pilot new systems that include **emotion recognition software** (applications that purport to infer an individual's emotional state) and **ethnic identification techniques** (programs that use information from facial scans to infer conclusions about race) **targeting China's Uyghur minority population.**[19] Article 19 researchers indicate that the PRC has a "burgeoning market for emotion recognition technologies" with little oversight or public consultation.[20]

Beijing is also building up its "data fusion" capabilities (merging disparate datasets to enhance the analytical power of digital tools).[21] Its researchers are investing heavily in improving computer vision and visual surveillance outcomes (with a particular focus on techniques related to person re-identification, crowd monitoring, and facial spoofing detection, or techniques to determine if a person is masquerading as someone else).[22] **PRC authorities are also honing their ability to conduct mass surveillance against foreign targets** by using sophisticated data analytic software to mine external social media and internet platforms.[23]

Companies in OECD countries actively contribute to the marketplace

Yet companies based in OECD countries are also selling predictive policing software, facial recognition algorithms, and social media surveillance applications widely, including to authoritarian clients. **Most governments, especially those with ample resources, purposely avoid relying on one country or supplier to fulfill their surveillance objectives.** In Saudi Arabia, for example, **Huawei** has been contracted to build safe cities, **Google and Microsoft** oversee the country's cloud-computing servers, **U.K. arms manufacturer BAE** has supplied mass surveillance systems, including internet interception technology, **Japan's NEC** provides facial recognition cameras, and **Amazon and Alibaba** are weighing partnering on a major smart city project.[24]

PRC-based Hikvision is one of the world's largest suppliers of video surveillance technology, and their products are increasingly ubiquitous.

European and U.S. vendors have even exported AI surveillance tools to the PRC, where some of these systems were found to have gone to an entity in Xinjiang.[25] Moreover, use of AI surveillance technology continues to grow in liberal democracies themselves.[26]

The COVID-19 pandemic has been a boon for surveillance vendors globally, with governments and private institutions alike deploying tools such as contact-tracing apps, public health prediction algorithms, and temperature sensors. At the pandemic's onset, civil society groups expressed alarm over privacy risks linked to government use of these systems.[27] In fact, many states failed to implement them fully or were disappointed by the outcomes.[28] Nonetheless, there is **a real risk that invasive measures and erosions of data privacy will persist beyond the pandemic**. In some countries, there are growing indications that tools such as China's health code app, which rates users' likelihood of exposure to determine their access to public places, will remain in use and may underpin new forms of political repression.[29] Demand for temperature scanners also gave companies linked to human rights abuses in the PRC, such as Dahua, a chance to expand their sales abroad.[30]

The COVID-19 pandemic has been a boon for surveillance vendors globally.

THE VULNERABILITIES OF SWING STATES

Although commentary has focused heavily on either China's full-fledged techno-authoritarian model or surveillance debates in liberal-democratic settings, **AI surveillance practices in hybrid regimes and weak democracies may seriously impact both the political evolution of these countries and the trajectory of global tech norms.**[31] These swing states represent partly open political settings where key liberal-democratic guardrails are weakened or absent in ways that could heighten the appeal of authoritarian digital models. Surveillance deployments present increased risk to civil liberties and the rule of law, but space for civil society to challenge these deployments remains.

Swing states: partly open political settings that combine democratic traits with autocratic attributes.

For purposes of this paper, swing states are identified using a combination of V-Dem electoral democracy scores and qualitative indicators selected by the author, yielding a total of 67 countries in this group (a full list can be found in Appendix 1).[32] While all states in this category combine democratic traits with autocratic attributes, they vary in the robustness of their rule of law frameworks and the mechanisms they have available to check surveillance abuses. Most suffer from some mix of serious democratic weaknesses, such as concentrated power in the executive branch, lack of judicial independence, limitations on media, repression of civil society, and infringements on political freedoms.

Swing states increasingly use AI surveillance tools

Of the 67 swing states, 44 already possess AI surveillance capabilities. In the coming years, this number will only grow higher. In many cases, there is still little information available on how AI tools are being or will be used in these settings. As I have shown in prior research, however, there is a **strong relationship between curtailments of political liberties and subsequent government abuse of surveillance technologies.**[33] Thus, the risk that surveillance abuses will feed on and, in turn, exacerbate broader governance problems is a serious one.

44 OF 67

swing states already possess AI surveillance capabilities.

How are swing states deciding their approaches to the use of AI surveillance? The PRC retains a major presence in most of these countries, and its companies figure prominently in the acquisition and deployment of relevant technologies. Among the 67 swing states, 55 are members of Beijing's Belt and Road Initiative. Still, **it is important not to overlook domestic factors, such as political norms, security threats, and regime incentives, that shape governments' choices** (not to mention the impact of non-Chinese exports of AI technology).[34]

55 OF 67

swing states are members of Beijing's Belt and Road Initiative

For example, security concerns, whether external or internal, are an important driver of surveillance investments. It is logical that countries such as India, Pakistan, Iraq, and Kenya—which variously face challenges from terrorism, internal insurgencies, and large refugee inflows—would choose to invest in sophisticated surveillance systems. Peer influence is also a factor. As Akın Ünver writes, the PRC's provision of lower cost surveillance technologies to certain countries may prompt rival states to "turn to the same suppliers. . . in order to swiftly acquire competing capabilities and resolve their security dilemma."[35]

The track record of AI surveillance

In a subset of the swing states—including India, Nigeria, and Singapore—there is already evidence of surveillance practices that raise concerns around privacy, fairness, or the rule of law.[36] In India, for instance, police forces deploy FRT routinely to implement "broad sweep-and-search actions that often target poor neighborhoods heavily populated by Muslims and migrants from north India."[37]

As digitalization sweeps the country, surveillance has been incorporated into India's governance, leading to the creation of what Sangeeta Mahapatra describes as "an early-warning system against security threats and a behavior-moderating system of social management and control."[38] Elsewhere, significant patterns of abuse either have not emerged or have yet to be documented. Concerning trajectories are less likely in those countries where robust legal frameworks protect **privacy rights** and provide **avenues for citizens to seek accountability.**

To call attention to the deployment of Huawei surveillance cameras in Belgrade, SHARE Foundation placed stickers reading "under surveillance" and QR codes leading to their website on the camera poles.

Despite the global popularity of AI surveillance tools, **evidence suggests that these technologies have yet to deliver on expectations in many countries**. The reasons behind these apparent shortcomings vary but may include issues of capacity, available expertise, and a lack of the interoperability required to make these high-tech tools work properly.

In Lahore, Pakistan, for example, the government installed 8,000 cameras in 2016 as part of a Safe City project; however, total crime in Punjab either rose or remained flat in the next several years.[39] A smart city project in Kenya has barely gotten off the ground in thirteen years amid legal snags and logistical hurdles.[40] Interlocutors in the Philippines described the government's investment in Chinese surveillance technology as **largely "security theater"** intended to intimidate but lacking a real impact on public safety.[41] As scholar Sheena Greitens writes, "At present, rigorous empirical evidence on the effect of Chinese surveillance technology platforms outside China is thin to nonexistent."[42] It behooves researchers and policymakers to probe further the real world impact of these technologies.

ESTABLISHING RULES OF THE ROAD

Currently, swing states and advanced democracies alike operate in an environment where broader global norms around AI surveillance are still being defined. **Multilateral fora have made progress in establishing agreement on high-level AI ethical principles, but it remains unclear how governments or companies will instill these concepts in the actual development and deployment of AI systems.** Some experts have also voiced concerns that framing the guardrails against abuse in terms of "AI ethics," rather than established international human rights norms, offers a loophole for states and corporations to pay lip service to concerns about AI harms without facing any enforceable obligations.[43]

Most AI governance initiatives remain at a high level of abstraction, lacking details about actual implementation.

Government and multilateral policy efforts to address AI governance

Multilaterally, regionally, and nationally, there are efforts afoot to begin addressing AI governance questions. Most of these initiatives remain at a high level of abstraction, lacking details about actual implementation. Recently, European regional institutions have been actively engaging in this domain. In early 2021, the **European Commission introduced the Artificial Intelligence Act**, a proposed framework to address systemic AI risks and promote innovation, which is under discussion at the European Parliament as of this writing in May 2022.[44] While some stakeholders are pressuring lawmakers to prohibit whole categories of technology, such as biometric surveillance tools, restrictions such as court authorization requirements or limits on data retention are likelier outcomes. The **Council of Europe** is carrying out a parallel effort to promulgate global standards on AI.[45]

Within the UN system, the **Office of the High Commissioner for Human Rights (OHCHR) has recommended a "moratorium" on the sale and use of "AI systems that pose a serious risk to human rights,"** pending new safeguards.[46] The Human Rights Council has called for a follow-up report, which will likely influence the development of AI policy in a range of fora.[47] Moreover, **UNESCO** produced draft AI ethics recommendations in mid-2021 that include surprisingly robust human rights language.[48]

Overall, **national governments' treatment of AI and human rights issues remains undeveloped**, although there has been local legislative activity (for instance, Portland, Oregon's complete prohibition of FRTs).[49] Under President Biden, the United States has rolled out several new initiatives. For example, the White House has launched an effort to develop an AI "bill of rights" that would set new rules for how biometric and automated technologies will be used.[50]

In addition, the United States has implemented **trade restrictions on AI technology**. These restrictions include requiring licenses for the export of sensitive technologies and limiting investment in and transactions with specific PRC-based companies, due in part to documented human rights abuses in Xinjiang linked to AI surveillance technology.[51]

When it comes to the global proliferation of **national and regional AI strategies,** Global Partners Digital found that **few of these documents engage extensively with the human rights impacts of AI technology**, and that most lacked "depth and specificity on how human rights should be protected."[52] These omissions stand in contrast to the detail with which the same strategy documents addressed issues such as economic competitiveness or fostering innovation. The most widely cited human rights issues were rights to privacy, followed by rights to equality and non-discrimination. A smaller subset of states referenced the right to an effective remedy and rights to freedom of expression and access to information.[53]

Civil society's role in shaping AI surveillance policy

CSOs have a critical role to play in shaping AI surveillance policy. **With authorities often inclined to make decisions on these issues in the dark, there is a risk of disregard for human rights principles and social concerns.** Public involvement at all stages is crucial to ensuring that democratic principles and processes guide the development and deployment of new technologies.

First, **CSOs are needed to build public awareness about government-contracted projects with civil liberties implications.** Obtaining information from governments is not easy. Eduardo Ferreyra, from Argentina's Asociación por los Derechos Civiles, notes that governments avoid publishing contractual information about newly procured surveillance technologies, and that freedom of information requests face delays or are ignored. Still, activists and journalists have used creative strategies to overcome these obstacles and provide vital information to the public. (For more, see essay on pp. 20-22.)

In the #ConMiCaraNo ("Not with My Face") campaign, Asociación por los Derechos Civiles warns about the risks of FRT. The large text reads "It's not protection, it's control."

In democracies, citizens have more opportunities to **question how public funds are being spent, scrutinize the government's rationale for proceeding with particular programs, and inquire how agencies intend to collect, store, and deploy user data.** In the Philippines, for instance, combined pressure from civil society and concerned parliamentarians led to major delays in funding a "Safe Philippines" surveillance project contracted with Huawei.[54] Danilo Krivokapić from Serbia's SHARE Foundation relates how his organization mobilized the community around plans to establish a city-wide surveillance system using Huawei technology in Belgrade (see pp. 23–25). Even in some more closed settings where there is less formal room for CSOs to maneuver, groups have found ways to muster public outrage and push for authorities to scale back or cancel concerning projects. In Uganda, for example, activists have raised the alarm regarding the potential uses of a digital vehicle tracking project contracted from a Russian firm, nominally to fight crime.[55]

Even when governments complete surveillance projects successfully, CSOs can play a vital role in **"watching the watchers," monitoring for signs of abuse.** Activists can also pressure the companies administering these systems to adhere to established business and human rights principles (the public backlash against the Canada-based internet firm Sandvine's transactions in Belarus is a good example).[56] Finally, although many existing international fora and government decision making processes are set up in a way that makes civil society input difficult, such participation is critical to shaping democratic norms. From the multilateral down to the local level, citizens can **submit briefs, attend public hearings, petition lawmakers, and mobilize fellow citizens to push for greater surveillance accountability and constraints on the use of novel systems**.

Private sector responsibilities

The onus for ensuring compliance with human rights standards and norms should not reside solely on governments or CSOs. There are **steps businesses should take voluntarily to mitigate harms and protect privacy**. Unfortunately, many companies, such as facial recognition firm Clearview AI, or data brokers such as LexisNexis, Nielsen, or Acxiom (all of which "openly and explicitly" sell data on millions of individuals for use by law enforcement surveillance software), are relying on gaps in law to validate their business practices. Paradoxically, in the United States, some of the biggest clients of these firms are law enforcement agencies.[57] As tech policy researcher Justin Sherman writes: "There are virtually no controls on the data brokerage industry . . . and on the practice of data brokerage itself."[58]

One solution is for legislatures to pass privacy laws regulating how data brokerages and private surveillance firms can operate, for instance, by establishing what data they are able to collect, and how affected individuals can seek accountability. But **enterprises also have an independent "responsibility to respect human rights."**[59] As laid out in the UN Guiding Principles on Business and Human Rights, companies are obligated to assess whether their conduct may be in violation of relevant human rights norms and to address adverse impacts with which they may be involved.[60]

Particularly when it comes to the surveillance industry, where the risk is heightened, **a useful approach proposed by Privacy International is for companies and governments that enter into public-private partnerships to incorporate specific agreements** reflecting principles of transparency, rules-respecting procurement, accountability, oversight, legality, necessity and proportionality, and redress.[61] This practice could mitigate concerns that commonly arise from such partnerships: Lines of accountability are often blurred, and companies—even when their technologies are being used by state agencies—can hide behind intellectual property and trade secrecy provisions to undercut transparency about their operations.

RISING TO THE CHALLENGE

For democratic societies, the right set of safeguards to rein in surveillance abuses remains elusive. Yet as AI surveillance technology becomes increasingly ubiquitous, it is vital to break the policy and regulatory logjam. Governments can start by being more transparent about how they are using AI technology. Improving transparency can be as straightforward as mandating **periodic AI risk assessment reports for government agencies** that deploy this technology in order to ensure appropriate privacy safeguards for data collection or to flag discriminatory impacts linked to underlying datasets. This practice could be supplemented by ex ante human rights impact assessments for specific intended uses (such as a planned law enforcement deployment of AI-powered drones to monitor crowds during protests).

As AI surveillance technology becomes increasingly ubiquitous, it is vital to break the policy and regulatory logjam.

Democratic governments should begin moving beyond promulgating high-level AI ethical principles and toward **establishing concrete benchmarks and regulations for responsible AI use that reflect international human rights law and standards**. These regulations should include protections for citizens against rights violations linked to tracking and mass surveillance, as well as limits on government uses of large-scale commercial datasets managed by data brokers.

In February 2020, the European Commission held a press conference on artificial intelligence. European institutions have been increasingly active in seeking to define AI norms.

Establishing oversight bodies, such as national task forces to evaluate privacy and human rights implications of AI technologies, is a good way to ensure an ongoing assessment of surveillance impacts as well as to involve civil society and outside actors in the review process.[62] **Governments should work hand-in-hand with civil society actors as equal stakeholders.** Outside experts, academics, and researchers should be brought into the rulemaking process rather than asked to comment at the end stage about the suitability of impending projects or policies.[63]

A multistakeholder body purpose-built to address survillance is needed

One substantive gap is the lack of a normative multistakeholder body mandated to address surveillance concerns, including AI-enabled uses. While there are a growing number of institutions examining AI governance issues, such as the OECD's AI Policy Observatory or Stanford University's Institute for Human-Centered AI, they are not focused on surveillance concerns specifically. Other human rights and digital rights institutions, such as UN OHCHR or the Freedom Online Coalition, have convened fora that touch upon AI surveillance, but their focus tends to be ad hoc.

One substantive gap is the lack of a normative multistakeholder body mandated to address surveillance concerns, including AI-enabled uses.

An enduring multistakeholder body mandated to tackle a wide array of surveillance issues is needed. Such an entity would engage in areas from developing **norms of responsible use**, to sponsoring **research on emerging uses** of new technology and devising **legal frameworks** that balance public interests and individual harms. This body could link to existing multistakeholder entities, such as the Internet Governance Forum or Global Partnership on AI, but would incorporate a dedicated surveillance mandate.

Among the organization's goals would be to address emerging approaches to preempt harmful applications (such as the development of emotion recognition and ethnic identification software), advance responsible use by private companies and governments, promote knowledge sharing, proactively foster concrete policy change, and raise public awareness of surveillance concerns.

The organization should emphasize **fostering new coalitions**—for instance, bringing together digital rights activists and software engineers to head off problems at the product design stage, rather than address them only after products have already hit the market. To some extent, organizations such as the Global Network Initiative, which brings together private sector stakeholders and digital rights advocates to discuss issues of concern related to freedom of expression and privacy, offer a partial model. However, the new grouping would focus explicitly on surveillance concerns and would incorporate an applied aspect to its work, going beyond policy engagement to discuss actual product design features.

While it is important to solicit participation from private, government, and civil society stakeholders, multistakeholderism should not amount to dilution. **Governments and companies that participate in this effort should possess demonstrably strong records on surveillance use and practices.** (Thus, governments like those of Egypt or Pakistan, or companies like NSO Group or Clearview AI, would be de facto barred from participating). The worst-case scenario would be for this organization to suffer from the same pathologies as the International Telecommunication Union (ITU) or UN Human Rights Council, where autocracies with appalling human rights records routinely are elected as members or hold leadership positions.[64]

The challenge for democracies

Democracies must move more vigorously on thinking through how democratic principles apply to AI governance, following through at home, and defining global norms in this area. Beijing is moving rapidly to write rules for AI systems. According to the Carnegie Endowment's Matt Sheehan, the new AI governance approaches that are emerging in the PRC touch on everything from rules for online algorithms to AI ethics principles. He also writes that the potential regulatory impact extends far beyond China's borders: "China will be running some of the world's largest regulatory experiments on topics that European regulators have long debated. Whether Chinese companies are able to meet these new demands could inform analogous debates in Europe."[65] **These efforts will give Beijing substantial sway when it comes to shaping global rules around AI surveillance technology, which could in turn diminish the role of human rights norms** in these frameworks. But the PRC is not alone; European regulators have also been busy. The EU's AI Act and the Council of Europe's Committee on AI offer potential avenues for democracies to counterbalance Beijing's regulatory push.

Beijing is moving rapidly to write rules for AI systems.

Facilitating greater public involvement in decision making about AI systems is crucial. Mariano-Florentino Cuéllar and Aziz Z. Huq propose searching for strategies that will help a wider array of citizens to "better understand the moral and political choices embedded not just in code but in the design choices of AI systems."[66] These authors argue that it is vital to empower as many users as possible "to influence and even change the policies and values embedded in those systems, whether adopted in the public or the private sphere."[67]
It is less important that individuals understand how specific AI systems work. Rather, it is essential that citizens can evaluate the impact of these systems. (Technologist David Weinberger explains this distinction as prioritizing "optimization over explanation.")[68] In this regard, civil society can help guide individual understanding, empowerment, and engagement regarding the societal impact of AI.

To address the challenge of AI surveillance, democracies need to undertake several major tasks simultaneously. First, they must **define regulatory norms** to guide responsible AI use, whether through national AI strategies and legislation or through regional efforts. To ensure that this norm-setting occurs democratically and reflects the concerns of affected groups, **citizens must have more opportunities to be involved** in the deliberation process. Finally, **democratic governments need to form coalitions** of like-minded states to advance shared digital values. Through this combination of strategies, democracies can prepare themselves to promulgate standards globally that will embed AI in human rights and rule of law safeguards, keep abuses in check, and counter authoritarian ambitions to set the rules of the game.

APPENDIX 1

TABLE

Swing States and AI Surveillance

Country	Region*	V-Dem Electoral Democracy Index	V-Dem Regime Type	Digital Repression Index**	AI Surveillance Capabilities?	Member of the Belt & Road Initiative?
Jamaica	WH	0.81	Electoral Democracy	-0.95	✓	✓
Czech Republic	EUR	0.81	Electoral Democracy	-1.10	✓	✓
Romania	EUR	0.78	Electoral Democracy	-0.94	✓	✓
Peru	WH	0.76	Electoral Democracy	-1.03	✓	✓
Croatia	EUR	0.75	Electoral Democracy	-0.94	✓	✓
Panama	WH	0.75	Electoral Democracy	-0.89	✓	✓
Armenia	EUR	0.74	Electoral Democracy	-0.57	✓	✓
Israel	MENA	0.74	Liberal Democracy	-0.15	✓	
Moldova	EUR	0.74	Electoral Democracy	-0.69	✓	✓
South Africa	AFR	0.72	Electoral Democracy	-0.59	✓	✓
Senegal	AFR	0.71	Electoral Democracy	-0.06		✓
Slovenia	EUR	0.70	Electoral Democracy	-0.95	✓	✓
Dominican Republic	WH	0.68	Electoral Democracy	-1.25	✓	
Ghana	AFR	0.66	Electoral Democracy	-0.35	✓	✓
Brazil	WH	0.66	Electoral Democracy	0.06	✓	
Bulgaria	EUR	0.66	Electoral Democracy	-0.85		✓
Georgia	EUR	0.65	Electoral Democracy	-0.54	✓	✓
Colombia	WH	0.65	Electoral Democracy	1.09	✓	
Ecuador	WH	0.64	Electoral Democracy	0.47	✓	✓
Namibia	AFR	0.63	Electoral Democracy	-0.39	✓	✓
Mexico	WH	0.63	Electoral Democracy	-0.44	✓	
Mongolia	EAP	0.63	Electoral Democracy	-0.87	✓	✓
Liberia	AFR	0.62	Electoral Democracy	0.18		✓
Lesotho	AFR	0.62	Electoral Democracy	0.06		✓
Malawi	AFR	0.62	Electoral Democracy	-0.08		

Continued

Country	Region*	V-Dem Electoral Democracy Index	V-Dem Regime Type	Digital Repression Index**	AI Surveillance Capabilities?	Member of the Belt & Road Initiative?
Kosovo	EUR	0.60	Electoral Democracy	-0.38		
Botswana	AFR	0.59	Liberal Democracy	-0.67	✓	
Nepal	SCA	0.59	Electoral Democracy	0.58		✓
North Macedonia	EUR	0.59	Electoral Democracy	-0.35		✓
Indonesia	EAP	0.59	Electoral Democracy	0.03	✓	✓
Poland	EUR	0.59	Electoral Democracy	-0.63	✓	✓
Sri Lanka	SCA	0.57	Electoral Democracy	0.50	✓	✓
Paraguay	WH	0.57	Electoral Democracy	-0.73	✓	
Tunisia	MENA	0.56	Electoral Autocracy	-0.44	✓	✓
Sierra Leone	AFR	0.55	Electoral Democracy	0.09		✓
Bosnia and Herzegovina	EUR	0.53	Electoral Democracy	-0.50	✓	✓
Niger	AFR	0.52	Electoral Democracy	0.49		✓
Ukraine	EUR	0.52	Electoral Democracy	0.32	✓	✓
Guatemala	WH	0.50	Electoral Democracy	-0.48		
The Gambia	AFR	0.50	Electoral Autocracy	-0.15		✓
Montenegro	EUR	0.50	Electoral Autocracy	-0.35		✓
Nigeria	AFR	0.49	Electoral Autocracy	0.11	✓	✓
Madagascar	AFR	0.48	Electoral Autocracy	0.16	✓	✓
Albania	EUR	0.48	Electoral Autocracy	-0.19		✓
Kenya	AFR	0.47	Electoral Autocracy	0.00	✓	✓
El Salvador	WH	0.47	Electoral Autocracy	-0.27		✓
Hungary	EUR	0.46	Electoral Autocracy	-0.45	✓	✓
Lebanon	MENA	0.46	Electoral Autocracy	0.98	✓	✓
India	SCA	0.44	Electoral Autocracy	0.97	✓	
Ivory Coast	AFR	0.43	Electoral Autocracy	0.20	✓	✓
Philippines	EAP	0.43	Electoral Autocracy	0.64	✓	✓
Papua New Guinea	EAP	0.42	Electoral Autocracy	-0.30	✓	✓
Benin	AFR	0.42	Electoral Autocracy	-0.02		✓
Kyrgyzstan	SCA	0.42	Electoral Autocracy	0.02	✓	✓
Malaysia	EAP	0.41	Electoral Autocracy	0.03	✓	✓

Continued

Country	Region*	V-Dem Electoral Democracy Index	V-Dem Regime Type	Digital Repression Index**	AI Surveillance Capabilities?	Member of the Belt & Road Initiative?
Singapore	EAP	0.40	Electoral Autocracy	0.31	✓	✓
Honduras	WH	0.39	Electoral Autocracy	-0.16		
Mauritania	AFR	0.39	Electoral Autocracy	0.33		✓
Gabon	AFR	0.38	Electoral Autocracy	0.76		✓
Iraq	MENA	0.37	Electoral Autocracy	0.78	✓	✓
Togo	AFR	0.37	Electoral Autocracy	0.54		✓
Pakistan	SCA	0.36	Electoral Autocracy	0.65	✓	✓
Tanzania	AFR	0.36	Electoral Autocracy	0.38		✓
Democratic Republic of the Congo	AFR	0.36	Electoral Autocracy	0.28		✓
Mozambique	AFR	0.36	Electoral Autocracy	-0.13		✓
Angola	AFR	0.35	Electoral Autocracy	0.02	✓	✓
Serbia	EUR	0.34	Electoral Autocracy	0.11	✓	✓

*Regional abbreviations: WH = Western Hemisphere; EUR = Europe and Eurasia; AFR = Sub Saharan Africa; MENA = Middle East and North Africa; SCA = South and Central Asia; and EAP = East Asia and Pacific

**On the digital repression index please consult Steven Feldstein, *The Rise of Digital Repression: How Technology is Reshaping Power, Politics, and Resistance* (New York: Oxford University Press, 2021); and Steven Feldstein, "Digital Repression Index (updated 2021 data)," Mendeley Data, V3, 2022, doi: 10.17632/5dnfmtgbfs.3

ENDNOTES

The Global Struggle over AI Surveillance

1 Steven Feldstein, *The Rise of Digital Repression: How Technology is Reshaping Power, Politics, and Resistance*, (New York: Oxford University Press, 2021), 218.

2 For more information, please consult: Maya Wang, *China's Algorithms of Repression*, Human Rights Watch, 1 May 2019, www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass.

3 On human rights risks from AI see Article 19, *Privacy and Free Expression in the Age of Artificial Intelligence,* April 2018, www.article19.org/wp-content/uploads/2018/04/Privacy-and-Freedom-of-Expression-In-the-Age-of-Artificial-Intelligence-1.pdf.

4 For more information, please see: LeRoy Ashby and Rod Gramer, *Fighting the Odds: The Life of Senator Frank Church,* (Pullman, Washington: Washington State University Press, 1994), 478.

5 Morgan Meaker, "Marseille's Fight against AI Surveillance," Coda Story, 26 March 2020, https://www.codastory.com/authoritarian-tech/ai-surveillance-france-crime/; and Auriane Dirou, "The French Global Security Law: Security or Liberties?," *Just Security,* 15 April 2021, https://justsecurity.org/75754/the-french-global-security-law-security-or-liberties/.

6 "Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks," Government Accountability Office, 29 June 2021, www.gao.gov/products/gao-21-518; and Ryan Mac et al., "Surveillance Nation," *BuzzFeed News*, 6 April 2021, www.buzzfeednews.com/article/ryanmac/clearview-ai-local-police-facial-recognition.

7 James Vincent, "FBI Used Facial Recognition to Identify a Capitol Rioter from His Girlfriend's Instagram Posts," Verge, 21 April 2021, www.theverge.com/2021/4/21/22395323/fbi-facial-recognition-us-capital-riots-tracked-down-suspect.

8 Elizabeth Dworkin, "Israel escalates surveillance of Palestinians with facial recognition program in West Bank," *Washington Post,* 8 November 2021, www.washingtonpost.com/world/middle_east/israel-palestinians-surveillance-facial-recognition/2021/11/05/3787bf42-26b2-11ec-8739-5cb6aba30a30_story.html.

9 Vanessa A. Boese et al., "Autocratization Changing Nature? Democracy Report 2022," Varieties of Democracy Institute (V-Dem), 2022, https://v-dem.net/media/publications/dr_2022.pdf.

10 Prabhjote Gill, "India Is Ramping Up the Use of Facial Recognition to Track Down Individuals Without Any Laws to Keep Track of How This Technology Is Being Used," *Business Insider India,* 10 February 2021, www.businessinsider.in/tech/news/what-is-facial-recognition-technology-and-how-india-is-using-it-to-track-down-protestors-and-individuals/articleshow/80782606.cms.

11 Bojan Stojkovski, "Big Brother Comes to Belgrade," *Foreign Policy*, 18 June 2019, https://foreignpolicy.com/2019/06/18/big-brother-comes-to-belgrade-huawei-china-facial-recognition-vucic/.

12 Umer Ali and Ramsha Jahangir, "Pakistan Moves to Install Nationwide 'Web Monitoring System,'" Coda Story, 24 October 2019, www.codastory.com/authoritarian-tech/surveillance/pakistan-nationwide-web-monitoring/.

13 Daniel Zhang et al., "The AI Index 2021 Annual Report," AI Index Steering Committee, Human-Centered AI Institute, Stanford University, March 2022, https://aiindex.stanford.edu/wp-content/uploads/2021/11/2021-AI-Index-Report_Master.pdf.

14 Steven Feldstein, *The Global Expansion of AI Surveillance,* Carnegie Endowment for International Peace, 17 September 2019, https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847.

15 Steven Feldstein, "AI & Big Data Global Surveillance Index (2022 updated)," Mendeley Data, V3, 2022, https://data.mendeley.com/datasets/gjhf5y4xjp/3.

16 Political system classification uses V-Dem's "regimes of the world" measure. For more information, please consult: Lührmann et al., "V-Dem Codebook v11.1," Varieties of Democracy (V-Dem) Project, 2021, www.v-dem.net/static/website/img/refs/codebookv111.pdf.

17 *Mapping China's Digital Silk Road,* Center for Strategic and International Studies, Reconnecting Asia Project, 19 October 2021, https://reconasia.csis.org/mapping-chinas-digital-silk-road/.

18 Sheena Chestnut Greitens, "China's Surveillance State at Home & Abroad: Challenges for U.S. Policy," Working Paper for the Penn Project on the Future of U.S.-China Relations, 2020, https://cpb-us-w2.wpmucdn.com/web.sas.upenn.edu/dist/b/732/files/2020/10/Sheena-Greitens_Chinas-Surveillance-State-at-Home-Abroad_Final.pdf.

19 Jane Wakefield, "AI Emotion-Detection Software Tested on Uyghurs," *BBC News*, 26 May 2021, www.bbc.com/news/technology-57101248; "Dahua Provides 'Uyghur Warnings' to China Police," IPVM, 9 February 2021, https://ipvm.com/reports/dahua-uyghur-warning; and Drew Harwell and Eva Dou, "Huawei Tested AI Software That Could Recognize Uighur Minorities and Alert Police, Report Says," *Washington Post*, 8 December 2020, www.washingtonpost.com/technology/2020/12/08/huawei-tested-ai-software-that-could-recognize-uighur-minorities-alert-police-report-says/.

20 "Emotional Entanglement: China's Emotion Recognition Market and Its Implications for Human Rights," Article 19, January 2021, www.article19.org/wp-content/uploads/2021/01/ER-Tech-China-Report.pdf.

21 Dahlia Peterson, *How China Harnesses Data Fusion To Make Sense Of Surveillance Data*, Brookings Institution, 23 September 2021, www.brookings.edu/techstream/how-china-harnesses-data-fusion-to-make-sense-of-surveillance-data/.

22 According to analysis from Georgetown's Center for Security and Emerging Technology, PRC institutions are responsible "for more than one third of publications in both computer vision and visual surveillance research." For more information, please see: Ashwin Acharya, Max Langenkamp, and James Dunham, "Trends in AI Research for the Visual Surveillance of Populations," Center for Security and Emerging Technology, January 2022, https://doi.org/10.51593/20200097.

23 Cate Cadell, "China Harvests Masses of Data on Western Targets, Documents Show," *Washington Post*, 31 December 2021, www.washingtonpost.com/national-security/china-harvests-masses-of-data-on-western-targets-documents-show/2021/12/31/3981ce9c-538e-11ec-8927-c396fa861a71_story.html.

24 Feldstein, *The Rise of Digital Repression*, 241.

25 *Out of Control: Failing EU Laws for Digital Surveillance Export,* Amnesty International, 21 September 2020, www.amnesty.org/en/documents/eur01/2556/2020/en; and Mara Hvistendahl, "How Oracle Sells Repression in China," Intercept, 18 February 2021, https://theintercept.com/2021/02/18/oracle-china-police-surveillance/.

26 For more information, please see: Steven Feldstein and David Wong, "New Technologies, New Problems—Troubling Surveillance Trends in America," *Just Security,* 6 August 2020, www.justsecurity.org/71837/new-technologies-new-problems-troubling-surveillance-trends-in-america/.

27 For example, please see: Paresh Dave, "Companies Bet on AI Cameras to Track Social Distancing, Limit Liability," *Reuters,* 27 April 2020, www.reuters.com/article/us-health-coronavirus-surveillance-tech-idUSKCN22914R; Antonia do Carmo Barriga et al., "The COVID-19 Pandemic: Yet Another Catalyst for Governmental Mass Surveillance?" *Social Sciences & Humanities Open* 2, (2020), www.sciencedirect.com/science/article/pii/S2590291120300851; and Melissa Heikkla, "Politico AI: Decodes: Color-blind Policy—France Debates Facial Recognition—MEPs AI Law Wishlist," *Politico*, 17 March 2021, www.politico.eu/newsletter/ai-decoded/politico-ai-decoded-color-blind-policy-france-debates-facial-recognition-meps-ai-law-wishlist/.

28 Wim Naudé, "Artificial Intelligence vs COVID-19: Limitations, Constraints and Pitfalls," *AI & SOCIETY* 35 (1 September 2020): 761–65, https://doi.org/10.1007/s00146-020-00978-0; and see also "The Role of AI Technology in Pandemic Response and Preparedness: Recommended Investments and Initiatives," National Security Commission on Artificial Intelligence, 25 June 2020, www.nscai.gov/wp-content/uploads/2021/01/NSCAI_White-Paper_The-Role-of-AI-Technology-in-Pandemic-Response-and-Preparedness.pdf.

29 Chris Buckley, Vivian Wang, and Keith Bradsher, "Living by the Code: In China, Covid-Era Controls May Outlast the Virus," *New York Times,* 30 January 2022, www.nytimes.com/2022/01/30/world/asia/covid-restrictions-china-lockdown.html.

30 Darren Bylar, "The Covid Tech That Is Intimately Tied to China's Surveillance State," *MIT Tech Review,* 11 October 2021, www.technologyreview.com/2021/10/11/1036582/darren-byler-xinjiang-china-uyghur-surveillance.

31 For more information, please see: Robert Morgus, Jocelyn Woolbright, and Justin Sherman, *The Digital Deciders*, New America, 23 October 2018, www.newamerica.org/cybersecurity-initiative/reports/digital-deciders/.

32 The paper used the following methodology to identify swing states: filtered V-Dem's electoral democracy index to include all countries scoring between Serbia (0.342) and Jamaica (0.81). The list was then narrowed by removing small island states and states with populations under 2 million. Countries with clear authoritarian characteristics and/or states recently beset by turmoil and instability were also excluded (Afghanistan, Burkina Faso, Central African Republic, Guinea-Bissau, Haiti, Mali, Myanmar, Somaliland). This method left 67 countries on the swing states list.

33 Feldstein, *The Rise of Digital Repression.*

34 Researchers such as Sheena Chestnut Greitens, Iginio Gagliardone, Matthew S. Erie, and Thomas Streinz observe that a combination of "push and pull factors" better explains why certain regimes obtain PRC surveillance technologies and how they will be used. For more information, please consult: Sheena Chestnut Greitens, *Dealing with Demand for China's Global Surveillance Exports,* Brookings Institution, April 2020, www.brookings.edu/research/dealing-with-demand-for-chinas-global-surveillance-exports/; Iginio Gagliardone, *China, Africa, and the Future of the Internet,* (London: Zed Books, 2019); and Matthew S. Erie and Thomas Streinz, "The Beijing Effect: China's' Digital Silk Road's Transnational Data Governance." *New York University Journal of International Law and Politics* (JILP) 54 (Fall 2021): 1-91, www.nyujilp.org/wp-content/uploads/2022/02/NYUJILP_Vol54.1_Erie_Streinz_1-91.pdf.

35 Akın Ünver, "Motivations for the Adoption and Use of Authoritarian AI Technology," *Issues on the Frontlines of Technology and Politics,* ed. Steven Feldstein (Washington, D.C.: Carnegie Endowment for International Peace, 19 October 2021), 16, https://carnegieendowment.org/2021/10/19/motivations-for-adoption-and-use-of-authoritarian-ai-technology-pub-85510; and please see: Akın Ünver and Arhan S. Ertan, "Politics of Artificial Intelligence Adoption: Unpacking the Regime Type Debate," *Democratic Frontiers: Algorithms and Society,* ed. Michael Filimowicz (New York: Routledge, 2022).

36 *Nigeria: Freedom on the Net 2021 Country Report*, Freedom House, last modified 20 September 2021, https://freedomhouse.org/country/nigeria/freedom-net/2021; and *Singapore: Freedom on the Net 2021 Country Report,* Freedom House, last modified 20 September 2021, https://freedomhouse.org/country/singapore/freedom-net/2021.

37 Gautam Bhatia, "India's Growing Surveillance State," *Foreign Affairs,* 19 February 2020, www.foreignaffairs.com/articles/india/2020-02-19/indias-growing-surveillance-state.

38 Sangeeta Mahapatra, *Digital Surveillance and the Threat to Civil Liberties in India,* German Institute for Global and Area Studies, 2021, www.giga-hamburg.de/en/publications/giga-focus/digital-surveillance-and-the-threat-to-civil-liberties-in-india.

39 Sheridan Prasso, "Huawei's Claims That It Makes Cities Safer Mostly Look Like Hype," *Bloomberg,* 12 November 2019, www.bloomberg.com/news/articles/2019-11-12/huawei-s-surveillance-network-claims-face-scrutiny?sref=QmOxnLFz.

40 Carey Baraka, "The Failed Promise of Kenya's Smart City," *Rest of World,* 1 June 2021, https://restofworld.org/2021/the-failed-promise-of-kenyas-smart-city/.

41 Feldstein, *The Rise of Digital Repression,* 165.

42 Sheena Chestnut Greitens, *Dealing with Demand for China's Global Surveillance Exports.*

43 Ben Wagner, "Ethics As an Escape from Regulation: From "Ethics-Washing" to Ethics-Shopping?" *Being Profiled: Cogitas Ergo Sum,* eds. Emre Bayamlıoğlu, Irina Baraliuc, Liisa Janssens, and Mireille Hildebrandt, (Amsterdam: Amsterdam University Press, 2018), please see here for online access: www.cohubicol.com/assets/uploads/being-profiled-16-wagner.pdf; and Eileen Donahoe and Megan MacDuffee Metzger, "Artificial Intelligence and Human Rights," *Journal of Democracy* (April 2019): 115–26, www.journalofdemocracy.org/articles/artificial-intelligence-and-human-rights/.

44 *"Artificial Intelligence Act," European Parliament, 2021,* https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2021/0106(COD)&l=en.

45 "CAHAI—Ad hoc Committee on Artificial Intelligence," Council of Europe, 2021, www.coe.int/en/web/artificial-intelligence/cahai.

46 "Artificial Intelligence risks to privacy demand urgent action—Bachelet," United Nations Human Rights Office of the High Commissioner, 15 September 2021, www.ohchr.org/en/2021/09/artificial-intelligence-risks-privacy-demand-urgent-action-bachelet.

47 "Resolution on the Right to Privacy in the Digital Age," (A/HRC/48/L.9/REV.1), United Nations Human Rights Council, 48th session, 13 September-8 October 2021, https://documents-dds-ny.un.org/doc/UNDOC/LTD/G21/274/69/PDF/G2127469.pdf?OpenElement.

48 "Draft Text of the Recommendation on the Ethics of Artificial Intelligence," United Nations Educational, Scientific and Cultural Organization, 25 June 2021, https://unesdoc.unesco.org/ark:/48223/pf0000377897.

49 Rachel Metz, "Portland Passes Broadest Facial Recognition Ban in the US," CNN, 10 September 2020, https://edition.cnn.com/2020/09/09/tech/portland-facial-recognition-ban/index.html.

50 "ICYMI: WIRED (Opinion): Americans Need a Bill of Rights for an AI-Powered World," White House, 22 October 2021, www.whitehouse.gov/ostp/news-updates/2021/10/22/icymi-wired-opinion-americans-need-a-bill-of-rights-for-an-ai-powered-world/.

51 "Treasury Identifies Eight Chinese Tech Firms as Part of The Chinese Military-Industrial Complex," U.S. Department of Treasury, 16 December 2021, https://home.treasury.gov/news/press-releases/jy0538; and James Vincent, "US announces AI software export restrictions," Verge, 5 January 2020, www.theverge.com/2020/1/5/21050508/us-export-ban-ai-software-china-geospatial-analysis.

52 Charles Bradley and Richard Wingfield, "National Artificial Intelligence Strategies and Human Rights: A Review," 2nd ed., Global Partners Digital and Stanford's Global Digital Policy Incubator, April 2021, www.gp-digital.org/wp-content/uploads/2021/05/NAS-and-human-rights_2nd_ed.pdf.

53 In a similar analysis of 34 country AI plans undertaken by Fatima et al., they found that "most plans did not contain any information on the actual implementation strategies or tracking mechanisms, and this highlights the largely aspirational nature of the plans." Plans largely focused on how governments should leverage AI to modernize the public sector and how industry can benefit from AI to enhance their competitiveness. For more information, please consult: Samar Fatima, Kevin C. Desouza, and Gregory S. Dawson, "National Strategic Artificial Intelligence Plans: A Multi-Dimensional Analysis," *Economic Analysis and Policy* 67 (2020): 178-194, www.sciencedirect.com/science/article/abs/pii/S0313592620304021.

54 Niharika Mandhana, "Huawei's Video Surveillance Business Hits Snag in Philippines," *Wall Street Journal,* 20 February 2019, www.wsj.com/articles/huaweis-video-surveillance-business-hits-snag-in-philippines-11550683135.

55 Elias Biryabarema, "Ugandan Opposition, Activists Denounce Digital Car Tracker Plan," *Reuters,* 19 July 2021, www.reuters.com/world/africa/ugandan-opposition-activists-denounce-digital-car-tracker-plan-2021-07-29/.

56 Ryan Gallagher, "Francisco-Backed Sandvine Nixes Belarus Deal," *Bloomberg,* 15 September 2020, www.bloomberg.com/news/articles/2020-09-15/sandvine-says-it-will-no-longer-sell-its-products-in-belarus.

57 Justin Sherman, "Data Brokers and Sensitive Data on U.S. Individuals," Duke University Sanford Cyber Policy Program, 2021, 9, https://sites.sanford.duke.edu/techpolicy/wp-content/uploads/sites/17/2021/08/Data-Brokers-and-Sensitive-Data-on-US-Individuals-Sherman-2021.pdf.

58 Sherman, "Data Brokers and Sensitive Data," 12.

59 "Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework," United Nations Human Rights Office of the High Commissioner (UN OHCHR), (HR/PUB/11/04), 2011, www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf.

60 "Guiding Principles," UN OHCHR.

61 "Safeguards for Public-Private Surveillance Partnerships," Privacy International, December 2021, https://privacyinternational.org/our-demands/safeguards-public-private-surveillance-partnerships.

62 "Final Report," National Security Commission on Artificial Intelligence, 2021, www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf.

63 The White House initiative to create a "bill of rights for an automated society," for instance, is soliciting a broad range of external feedback, including through the setting up of two public listening sessions and six public events to discuss risks, benefits, and core principles related to the responsible regulation of AI technology. For more information, please see: "Join the Effort to Create A Bill of Rights for an Automated Society," White House, 10 November 2021, www.whitehouse.gov/ostp/news-updates/2021/11/10/join-the-effort-to-create-a-bill-of-rights-for-an-automated-society/.

64 Mary Hui, "China's election to the UN Human Rights Council revealed its shaky global status," Quartz, 14 October 2020, https://qz.com/1917295/china-elected-to-un-rights-council-but-with-lowest-support-ever/.

65 Matt Sheehan, *China's New AI Governance Initiatives Shouldn't Be Ignored,* Carnegie Endowment for International Peace, 4 January 2022, https://carnegieendowment.org/2022/01/04/china-s-new-ai-governance-initiatives-shouldn-t-be-ignored-pub-86127.

66 Mariano-Florentino Cuéllar and Aziz Z. Huq, *The Democratic Regulation of Artificial Intelligence,* The Knight First Amendment Institute, 31 January 2022, https://knightcolumbia.org/content/the-democratic-regulation-of-artificial-intelligence.

67 Cuéllar and Huq, *Democratic Regulation.*

68 Weinberger writes: "use our existing policy-making processes—regulators, legislators, judicial systems, irate citizens, squabbling politicians—to decide what we want these systems optimized for. Measure the results. Fix the systems when they don't hit their marks. Celebrate and improve them when they do." For more information, please see: David Weinberger, "Optimization over Explanation: Maximizing the Benefits of Machine Learning Without Sacrificing Its Intelligence," *Medium,* 28 January 2018, https://medium.com/berkman-klein-center/optimization-over-explanation-41ecb135763d.

Overcoming Obstacles to Surveillance Research: Lessons for Civil Society

69 For more information, please visit https://adc.org.ar/en/home.

70 This essay draws on research published in the December 2021 ADC report *Surveillance Technology in Argentina,* authored by Alejo Kiguel, Eduardo Ferreyra, and Leandro Ucciferri (available at https://adc.org.ar/wp-content/uploads/2022/03/ADC-Surveillance-Technology-in-Argentina.pdf) and in Gaspar Pisanu et al., Surveillance Tech in Latin America: Made Abroad, Deployed at Home, Access Now, 10 August 2021, www.accessnow.org/cms/assets/uploads/2021/08/Surveillance-Tech-Latam-Report.pdf.

71 Pisanu et al., *Surveillance Tech in Latin America,* 7.

72 The archived page is available at "Case Study: Integrated Urban Safety Solutions, Tigre City," NEC, 2016, https://web.archive.org/web/20170321095617/http:/www.nec.com/en/case/tigre/pdf/brochure.pdf (accessed 21 March 2017).

73 Dave Gershgorn, "The U.S. Fears Live Facial Recognition. In Buenos Aires, It's a Fact of Life," *OneZero,* 4 March 2020, https://onezero.medium.com/the-u-s-fears-live-facial-recognition-in-buenos-aires-its-a-fact-of-life-52019eff454d.

74 "Argentina: Child Suspects' Private Data Published Online," Human Rights Watch, 9 October 2020, www.hrw.org/news/2020/10/09/argentina-child-suspects-private-data-published-online.

Starting the Debate on Facial Recognition: A Case Study from Belgrade

75 Danijela Vukosavljević, "The Privacy of Citizens Will Not Be Endangered," *Politika,* 7 October 2019, https://www-politika-rs.translate.goog/sr/clanak/439334/Privatnost-gradana-nece-biti-ugrozena?_x_tr_sl=sr&_x_tr_tl=en&_x_tr_hl=en&_x_tr_pto=sc; and "What and When Will 1,000 New Cameras Be Filmed on City Streets," RTS, 9 February 2019, https://www-rts-rs.translate.goog/page/stories/sr/story/125/drustvo/3415215/sta-ce-i-koga-snimati-1000-novih-kamera-po-gradskim-ulicama.html?_x_tr_sl=sr&_x_tr_tl=en&_x_tr_hl=en&_x_tr_pto=sc.

76 Stojkovski, "Big Brother Comes to Belgrade."

77 "MUP Decision," letter published by SHARE Foundation, 7 March 2019, https://resursi.sharefoundation.info/wp-content/uploads/2019/03/Resenje-MUP-7.3.2019..pdf.

78 The archived page can be found at https://archive.ph/pZ9HO. For more information, please see: "Huawei Knows Everything About Cameras in Belgrade—And They Are Glad to Share," SHARE Foundation, 29 March 2019, www.sharefoundation.info/en/huawei-knows-everything-about-cameras-in-belgrade-and-they-are-glad-to-share/.

79 For a brief overview of these findings, please see: "Consultation on the proposal for the Zakon o Unutrašnjim Poslovima," published letter from EDRi, SHARE Foundation, 17 September 2021, https://www.sharefoundation.info/wp-content/uploads/EDRi-Civil-Society-consultation-on-the-proposal-for-the-Zakon-o-unutrasnjim-poslovima.pdf.

80 "Hiljade.Kamera.rs: Community Strikes Back against Mass Surveillance," SHARE Foundation, 19 May 2020, www.sharefoundation.info/en/hiljade-kamera-rs-community-strikes-back/.

81 "Draft Withdrawal A Step Towards Moratorium on Biometric Surveillance," SHARE Foundation, 23 September 2019, www.sharefoundation.info/en/draft-withdrawal-a-step-towards-moratorium-on-biometric-surveillance/.

ACKNOWLEDGMENTS

Steven Feldstein would like to thank Brian Kot for his editing and research assistance, and two anonymous peer reviewers for their insightful comments. The authors also appreciate the contributions of the International Forum's staff and leadership, including Christopher Walker, John Glenn, Kevin Sheives, John Engelken, Rachelle Faust, Lily Sabol, and Daniel Cebul, all of whom played important roles in the editing and publication of this paper. Particular acknowledgment goes to Beth Kerley, whose support and vision for this project were invaluable to its completion. The Forum wishes to thank Factor3 Digital for their efforts and invaluable support in designing this report for publication.

PHOTO CREDITS

Cover image: Photo by Trismegist san/Shutterstock

Page 4: Photo by Sergey Nivens/Shutterstock

Page 6: Photo by zmpixes/Shutterstock

Page 9: Photo by Karolis Kavolelis/Shutterstock

Page 12: Photo provided by Danilo Krivokapić of the SHARE Foundation

Page 14: Photo provided by Eduardo Ferreyra of ADC

Page 17: Photo by Thierry Monasse/Getty Images

Page 20: Photo by STEKLO/Shutterstock

Page 23: Danilo Krivokapić of the SHARE Foundation