Foreign Policy at BROOKINGS

POLICY BRIEF | JUNE 2022

GEOPOLITICAL IMPLICATIONS OF AI AND DIGITAL SURVEILLANCE ADOPTION

DAHLIA PETERSON AND SAMANTHA HOFFMAN

Executive summary

The increasing sophistication and spread of artificial intelligence (AI) and digital surveillance technologies has drawn concerns over privacy and human rights. China is indisputably one of the leaders in developing these technologies both for domestic and international use. However, other countries that are active in this space include the United States, Israel, Russia, multiple European countries, Japan, and South Korea. U.S. companies are particularly instrumental in providing the underlying hardware for surveillance technologies.

In turn, these technologies are used in a range of settings. Some of its most severe use cases include helping to spy on political dissidents, and enabling repression of the Uyghur and Turkic Muslim populations across China. However, concerns arise even in its more "mundane" uses, which include one-to-one verification at banks and gyms. The higher quality of the data collected can help companies improve the accuracy of their facial recognition technology. Over time, these increasingly effective technologies can be used elsewhere for authoritarian purposes.

The United States and partner democracies have implemented sanctions, export controls, and investment bans to rein in the unchecked spread of surveillance technology, but the opaque nature of supply chains leaves it unclear how well these efforts are working. A major remaining vacuum is at the international standards level at institutions such as the United Nations' International Telecommunication Union (ITU), where Chinese companies have been the lone proposers of facial recognition standards that are fast-tracked for adoption in broad parts of the world.

To continue addressing these policy challenges, this brief provides five recommendations for democratic governments and three for civil society. In short, these recommendations are:

- The U.S. and its allies should demonstrate that they can produce a viable alternative model by proving that they can use facial recognition, predictive policing, and other AI surveillance tools responsibly at home.

- The State Department should work with technical experts, such as those who convene at the Global

Partnership on AI, to propose alternate facial recognition standards at the ITU.

- The United States and like-minded countries should jointly develop systems to improve the regulation of data transfers and reduce risks.
- The United States and partner democracies should subsidize companies to assist with creating standards to propose at bodies such as the ITU.
- The National Science Foundation and the Defense Advanced Research Projects Agency should fund privacy-preserving computer vision research, where computer vision is deriving information from images or video.
- Civil society organizations (CSOs) should engage in outreach efforts with local communities and community leaders to strengthen public discourse on the advantages and disadvantages of using AI in policing and surveillance.
- CSOs should engage in or support research on issues related to rights abuses using AI and digital surveillance technologies and the export of these technologies.
- CSOs should actively participate in the setting of international technology standards.

Introduction

Governments and law enforcement agencies worldwide are increasingly leveraging AI and digital surveillance technology to enhance their policing efforts. At a basic level, AI and digital surveillance technologies support police work by helping to streamline operations and solve everyday problems. They can also improve predictive and emergency response capacities. However, because what is deemed legal and illegal is heavily influenced by politics and the definition of problem solving is subjective, the motivations for adopting these technologies vary between countries and even between the localities within them.[1] Therefore, who sets the standards for and direction of the technology matters. As tech development advances, it will be ever more crucial to monitor the implications and risks of the proliferation and export of AI and digital surveillance technologies from a geopolitical perspective.

Authoritarian and democratic states alike are adopting AI and digital surveillance technologies at a pace that is not allowing for suitable public debate on the implications of their use and boundaries for their use.

Authoritarian and democratic states alike are adopting AI and digital surveillance technologies at a pace that is not allowing for suitable public debate on the implications of their use and boundaries for their use. For authoritarian regimes, these technologies simultaneously strengthen a state's capacity to exercise coercive power — for example, by helping to track specific individuals — and to improve police work generally. Meanwhile, for liberal democracies and hybrid regimes, these technologies help to reduce burdens on law enforcement agencies and through automation of certain operations, sometimes remove racial and other biases and improve a state's capacity to solve and predict crime. In practice however, these technologies can also undermine the rights and interests of the people that law enforcement claims to protect, and reinforce the biases that such technologies were intended to eliminate.

Yet, although many states have adopted these technologies, few states have leading companies in the AI and digital surveillance technology market. China is arguably the leading exporter of comprehensive AI surveillance systems. Many researchers

and journalists have tracked the global expansion of these systems, including for improved data integration and analytics, 911 operations, and biometric recognition.[2] Well-known Chinese companies operating in this space include Dahua, Hikvision, Megvii, and SenseTime. The United States is also a leading producer of AI and surveillance technologies. Well-known American companies include Clarifai, CLEAR, Clearview AI, and Intel. European producers include Sweden's Axis Communications and Germany's Bosch. Israel has Oosto (previously AnyVision) and OrCam. Russia has AxxonSoft, NtechLab, and VisionLabs. Other Asian producers include South Korea's Hanwha and Japan's NEC.

The problem with China being the leading exporter is that these technologies in the People's Republic of China (PRC) are being designed specifically to meet the party-state's political needs, and as such there are few ethical impediments to the research and development (R&D) and deployment of these AI surveillance systems. In fact, when combined with state-centered priorities and incentives, the lack of obstacles may be a reason why China leads in this space. Authoritarian regimes don't face the same balancing act and are able to leverage their coercive power to determine which subsets of their populations should be targeted for intensified surveillance. In China, for example, the direct, coercive use of surveillance technologies concentrates on "focus/key personnel" lists, which include individuals petitioning the government and those suspected of being involved in terrorism.[3] Under such broadly defined categories, the Chinese police can monitor anyone who might destabilize regime stability and can more easily mobilize against protests.[4] China's surveillance toolkit — which has evolved iteratively to add predictive policing and facial, voice, and other biometric recognition tools — has enabled genocide in Xinjiang and political spying abroad.[5]

Naturally, repressive countries that see eye to eye with China's geopolitical aims, such as Iran, aim to replicate the Chinese approach.[6] But it is not just authoritarian regimes that adopt Chinese technologies. Numerous researchers have shown how democracies across Europe and Latin America are also adopting them.[7]

As governments continue to embrace AI and digital surveillance technologies, democracies need to develop strong governance models for these technologies as well as strategies for countering states' misuse of them. This is particularly important because China is a heavyweight in dictating global technology standards, including through the United Nations' International Telecommunication Union (ITU). China's ITU facial recognition standards — which recommend use cases — have been widely adopted across Africa, Asia, and the Middle East, largely because no other countries have proposed viable alternatives.[8]

In undertaking these and other efforts, however, it will be important to remember that existing prescriptive policy solutions will not address all of the issues around AI and cyber-driven surveillance technology. Current policy frameworks and toolkits were not designed to be responsive to evolving technologies and the political intent driving their development. Therefore, the creation of new frameworks that do so will be essential. Innovative action and understanding are required in a wide range of areas, including the ethical use of AI, the mitigation of risks embedded in specific AI and surveillance technologies, the setting of R&D priorities, and the funding of and collaboration on the design of competing technologies and technology standards globally.

An overview of AI and digital surveillance technologies

Broadly, AI and digital surveillance technologies include the technologies that support government policing and surveillance efforts — everything from public-facing cameras and remote-sensing equipment to the underlying hardware and software systems used for data storage, integration, processing, and analysis. It is helpful to visualize these technologies by thinking of them as layers sitting within a standard Internet of Things (IoT) technology stack.[9] The stack can be divided into four layers:

- **Smart devices:** These are physical IoT-connected devices, which include smart security cameras, biometric scanners, local storage, processors, digital software (applications and operating systems), sensors, and actuators.

- **Data transmission and communications technologies:** These enable connectivity and the transmission of data between the physical IoT device and the cloud. Communications technologies include Bluetooth, WiFi networks, 3G, 4G LTE networks, and 5G networks.

- **Cloud infrastructure components:** These, like hardware and software, enable cloud-based services for ingesting and storing data streams from IoT devices.

- **Cloud applications:** These store and process the IoT data, which can be used to conduct analysis and to visualize outputs for the user.

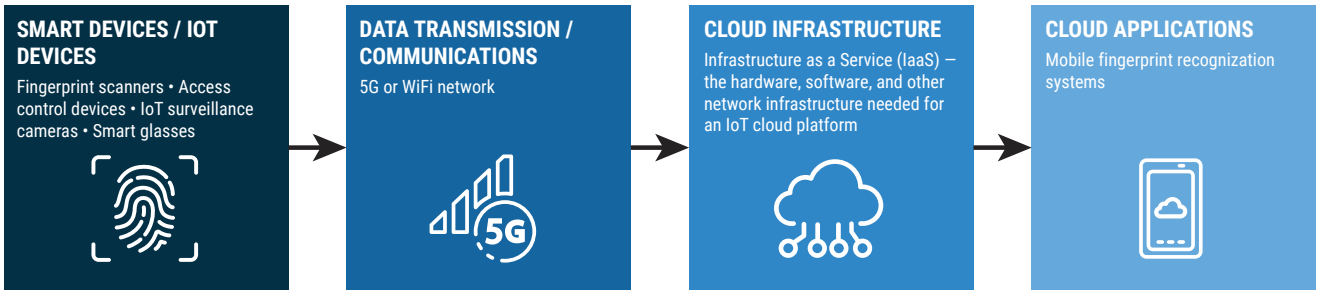
This brief focuses on the technologies that enable biometric surveillance. Note, however, that these systems do not always exist in isolation. Multiple types of smart systems data from different government cloud networks can be integrated and shared with other government information systems. Moreover, how a technology and the data it helps generate are used depends mostly on the intent/objectives of (1) the end user controlling the device or system and (2) any actor who has access to the data generated from it.

BIOMETRIC SURVEILLANCE TECHNOLOGY

Biometric surveillance refers to the groupings of technology that allow a user to identify a person based on biometric indicators, including faces, irises, fingerprints, gait (measure of body movement and body mechanics), and DNA data. Biometric recognition systems are commonly used globally, for example by border control agents and in the context of domestic law enforcement.[10] In these instances, the systems are used to enhance border security and identify individuals entering the country fraudulently.[11]

FIGURE 1

Biometric surveillance technology stack



Face surveillance is one of the most prominent types of surveillance and includes the distinct categories of facial recognition and facial analysis. Facial recognition technology converts facial features into a mathematical formula, or "faceprint," before performing either (1) face verification, or one-to-one matching, or (2) face identification, or one-to-many matching. Facial analysis technology estimates factors such as emotion, engagement level, age, gender, and ethnicity, but this technology has been criticized as fundamentally inaccurate and flawed.[12] Both facial recognition and facial analysis are challenged by issues such as underexposed or overexposed lighting and face masks.

Biometric surveillance is widely used across democracies. In the United States, local police departments have deployed facial recognition systems in cities such as Detroit, but its use has been controversial.[13] These technologies, despite sometimes being used to reduce racial biases in policing, have been criticized for actually reinforcing them due to relying on historically biased training data, and computationally legitimizing problematic police practices.[14] While the European Union has barred biometric data sharing to third parties without consent under the General Data Protection Regulation (GDPR) and called for ending private facial recognition databases and police use of facial recognition technology in public places, it is still actively pursuing police use of facial recognition in other areas. For example, millions of faces will be shared in the inter-European Prüm II police biometric database.[15]

In China, the Ministry of Public Security oversees smart cities' public security platforms, such as video and image information databases (VIID) and police geographic information systems (PGIS). The biometric data collected by the agencies are ingested on these platforms. VIID and PGIS systems are connected to more far-reaching public security projects — such as Skynet and Sharp Eyes — that seek to problem-solve in real time and improve predictive capabilities.[16] Skynet is the older of the two projects and seeks to perform 24/7 video surveillance of public areas, and timed surveillance over minor streets, additionally relying on GIS systems to improve public security monitoring. Sharp Eyes builds on Skynet infrastructure to include more comprehensive data fusion and cover more rural areas. China's use of the data is broader and feeds into work ranging from state security to logistics.

Researchers have found that China purposefully builds in biases and connects these to coercive state practices that target specific ethnic groups, especially the Uyghurs and Tibetans.

These projects are also linked to state coercive practices that employ facial recognition technology. Researchers have found that China purposefully builds in biases and connects these to coercive state practices that target specific ethnic groups, especially the Uyghurs and Tibetans. Facial analysis systems specifically look for ethnic and nationality identifiers. Chinese standards bodies are actively codifying national and provincial biometric surveillance approaches. In December 2017, the Ministry of Public Security released facial recognition guidelines calling for Uyghur detection.[17] Other standards have called for detecting "personal attributes" including "ethnicity" (Uyghurs are one of 56 official ethnic groups in China) and "skin color."[18] Ethnicity recognition is also codified nationally at the design level via the Standardization Administration of China, which issues standard technical requirements for facial recognition technologies used in security systems.[19]

In reality, the standards already encompass Uyghur detection. This targeting is reinforced when police directly request more specific or advanced Uyghur-detection capabilities, as they appeared to have done in at least 12 nationwide projects by 2019.[20] Furthermore, numerous major Chinese surveillance

companies reportedly claim to provide Uyghur detection.[21] And database schema for VIID databases appear to include not just the ethnic identifiers but also recorded facial data of foreign citizens in China for facial recognition. In 2021, media reports highlighted that provincial and municipal governments have been developing and implementing systems for tracking individuals, including foreigners such as journalists.[22]

CONSTRAINTS ON BIOMETRIC SURVEILLANCE TECHNOLOGY

Police use of AI and digital surveillance technologies is first determined by the political and legal systems in which the technologies are being deployed. A core contrast between authoritarian regimes and democracies is the existence of safeguards in legal frameworks and to what extent they are followed. For example, Huawei freely gave 240 facial recognition cameras to the city of Valenciennes, France, in 2017. But French law bans real-time facial recognition, which means local authorities do not use the full features built into Huawei's technology.[23] That said, while some democracies have legal frameworks and political systems designed to protect the rights of individuals and put *actual* limits on the state's power, technology is still being rolled out faster than technology-specific legal safeguards and faster than decisionmakers can understand the risks and benefits of the technologies.

Moreover, even if safeguards are in place, regime change can result in their removal. For example, under Myanmar's resumption of junta rule, protections against warrantless surveillance, search, and seizure have been removed.[24] This is particularly concerning when combined with the fact that Myanmar's capital city Naypyidaw now uses 335 cameras purchased from Huawei. (Although, the company claims not to be the developer behind the cameras' facial and license plate recognition).[25] The technology is used to alert authorities to individuals on the wanted list.[26]

The use of surveillance technology is also shaped by how problem-solving or public security is defined in the state. Leaders in Latin America and Southeast Asia justify AI surveillance adoption with the need to increase public safety and reduce burdens on police. But several problems exist with such justifications.[27] First, authorities often do not define what "public security" means, leaving systems prone to abuse.[28] Second, laws passed to authorize AI surveillance are often used as a fig leaf to retroactively permit existing surveillance.[29] Furthermore, despite local and federal data protection laws, public security needs can trump users' ability to rectify incorrect data, as has been the case in Argentina.[30]

EXPORTATION OF BIOMETRIC SURVEILLANCE TECHNOLOGY AND CENSORSHIP

Companies developing biometric surveillance technologies are exporting them globally. The export of Chinese biometric surveillance technologies, in particular, has been well documented in recent years. For instance, Taigusys, a Chinese company specializing in emotion recognition, has exported its facial analysis equipment to Thailand and several African countries.[31] Chinese AI unicorns, including CloudWalk, SenseTime, and Yitu, have exported their one-to-many facial recognition across the globe.[32] AI unicorn Megvii is also active in exporting its one-to-one verification technology, which is deployed in places as diverse as a large oil rig builder in the United Arab Emirates and a gym in Thailand.[33]

In addition to exporting their one-to-many facial recognition systems, Chinese companies have supported projects to improve policing and surveillance using digital technology. For example, Dahua has built complete platforms in Peru;[34] ZTE has been integral to the development of Venezuela's "Fatherland Card," or smart ID card;[35] and China National Electronics Import & Export Corporation (CEIEC) has constructed — and Huawei has provided the equipment for — Ecuador's ECU 911 public security system.[36] Across Latin America, Chinese companies have spurred the use of surveillance technology and primed the market for further expansion by offering equipment and software either at discounted prices or for free.[37]

Beyond individual surveillance technology exports, China also exports platform solutions. Huawei, with several other companies' participation, is the lead developer of these multilayer platforms, which are typically referred to as "Safe Cities."[38] Other major Chinese companies involved are the world's two largest surveillance companies, Dahua and Hikvision, as well as ZTE and CEIEC.[39] According to the Australian Strategic Policy Institute, Huawei has exported its smart and safe cities technologies and projects to over 100 locations worldwide.[40]

The export of Chinese technologies stands out largely because of the political system that influences the technologies' development and the innovation ecosystem that encourages companies to design technologies that meet the Chinese state's priorities.

The export of Chinese technologies stands out largely because of the political system that influences the technologies' development and the innovation ecosystem that encourages companies to design technologies that meet the Chinese state's priorities. But China is not the only exporter of these technologies. Other technologies also have been developed to serve inherently coercive political aims. For instance, Israel's Oosto is a vision AI company that exports recognition technology and provides surveillance equipment at checkpoints in the West Bank.[41]

In addition, technologies designed in democratic countries are not all used for advancing democratic interests. In 2019, for example, the U.S.-based OpenPOWER Foundation led by Google and IBM executives reportedly set up a collaboration with IBM, the Chinese company Semptian, and U.S. chip manufacturer Xilinx to develop the SuperVessel cloud platform to "analyze vast amounts of data more efficiently."[42] (Semptian is a company specializing in internet surveillance and censorship technology in China.) However, this relationship began in 2015, and more recently in 2020, IBM called for controls on facial recognition technology exports to prevent uses that "undermine American values."[43] While IBM also stopped conducting skin tone analysis in 2020, there is still no industry or government-wide guidance on the ethics of "race" analytics or even the ethics of selling AI surveillance to authoritarian governments.[44]

Companies in democratic countries have also been exporting their digital surveillance products to illiberal regimes. These products are then used by the regimes' security forces. For example, in 2010, reports emerged that Libyan security agents under Moammar Gadhafi's regime had spied on journalists' communications using surveillance technology purchased from the French company Amesys.[45] In another case, Bahraini authorities likely used technology from Germany-based Trovicor to intercept emails and text messages from political activists who were detained and abused.[46] Israeli companies Candiru, Cognyte, NSO Group, and Paragon are also pioneering zero-click hacks (which don't require user action and instead exploit system vulnerabilities) and selling their services to government clients worldwide.[47]

Nevertheless, exported surveillance technologies developed in authoritarian countries, namely China, pose greater risks because they are often explicitly designed for coercive purposes. And companies such as Hikvision and Huawei export them to countries with poor human rights track records — such as Kazakhstan, Kyrgyzstan, Saudi Arabia, and the United Arab Emirates.[48]

Other end users may not be using digital surveillance to advance rights-violating policies, but that doesn't make their use less concerning overall. For example, cameras are commonly deployed commercially or for critical infrastructure sectors such as energy.

Since 2019, Chinese company Uniview has installed more than 4,000 security cameras in People's Bank of Indonesia ATMs.[49] By 2018, it installed intrusion detection video surveillance systems across nearly 100 state-run electricity substations in Jakarta.[50] What's worrying is that the higher-quality data collected help not only the end user but also the company providing the technology by improving the accuracy of facial recognition. Over time, the increased effectiveness of that technology can be put to use elsewhere for clear authoritarian purposes or purposes that embed authoritarian concepts of security and policing.

Even if an end user only aims to use surveillance technology for the greater good (from a liberal democratic perspective), it does not mean that no harm will be done. An end user isn't fully in control of how the data generated or stored are used by actors with downstream data access.[51] This means that if suppliers are not monitored, the data from systems deployed overseas can advance authoritarian interests elsewhere. There are also issues associated with the standards that a technology carries with it and how these standards are set globally through market penetration.

Thinking beyond the end use of AI and digital surveillance technology

As AI and digital surveillance technologies are further integrated into information and security systems, states might increasingly use them to extend their power globally and pursue their interests — whether through extra-territorial police and surveillance activity or technical standards setting.

For instance, in China, national agenda setting, policies, and laws enable the state to exert its control over companies and advance its interests through their activities. When Chinese-developed technologies are then exported, this same control allows the state to leverage this power to make further political and economic advancements globally. This is evidenced by the Belt and Road Initiative's Digital Silk Road, which uses Chinese-developed technologies to support telecommunications, cloud computing, e-commerce, and mobile payments in recipient nations.[52] Notably, these kinds of digital projects not only extend China's influence but also risk eroding the sovereignty of these nations.

China has established regulations on data transmission and privacy protection, including the Data Security Law (2021), the Intelligence Law (2017), the Cyber Security Law (2016), and the State Security Law (2015). But these laws are arguably not strong enough to protect against the risks inherently embedded in Chinese technology. It is normal for any company — no matter where it is based — to collect data and transfer it to other countries where they have servers for internal use, such as for improving their product. But, in many countries, there are legal reasons why law enforcement may be allowed to access that data, even if it was generated overseas. In China, those reasons are far broader because what is considered lawful or unlawful is far more vague and slippery than it is in a liberal democracy.[53] What data are subject to "national security or law enforcement requirements" can be extremely broad.

The issue is not just that data collection may enable Chinese companies to conduct overseas surveillance. For the supplier of the technology, the high-quality data collected can improve the accuracy of the facial- and voice-recognition systems, which can in turn be marketed and used for future repressive purposes.

China's approach to AI and digital surveillance also has global impacts, which are clearly seen in how it seeks to set technology standards through bodies such as the ITU, magnifying the risks their technologies could create. The Financial Times reported in 2019 that China Mobile, China Telecom, Dahua, and ZTE have proposed international standards that are very similar to Chinese domestic standards.[54] The standards also cross the line into policy recommendations, as they recommend where facial recognition

should be deployed: for example, in public spaces (for use by the police), in workplaces (for use by employers to confirm employees' work attendance), and in local libraries (for use by law enforcement to compare with the country's "fugitive library" to find hiding criminals). Although developing nations in Africa, Asia, and the Middle East are widely adopting Chinese standards, companies in the United States and other democratic nations have yet to propose viable alternatives.[55]

Policy responses and remaining hurdles

Given the unchecked spread of Chinese surveillance technology both from within China and around the world, the U.S. and other democratic states have taken commendable steps to tackle this issue on multiple fronts. These steps include, but are not limited to, establishing U.S. State Department surveillance export guidance, Customs and Border Protection withhold release orders, Commerce Department Entity List export controls, Treasury Department Global Magnitsky sanctions, and investment bans by White House executive orders. Multilaterally, the United States is cooperating with Australia, Canada, Denmark, France, the Netherlands, Norway, and the United Kingdom as well as working with the European Union through the Trade and Technology Council.[56]

But how well these states' actions are working remains unclear. Chinese companies are heavily reliant on U.S. chips and storage solutions to power their AI surveillance technologies.[57] But given the surveillance industry's opaque supply chains and sometimes inscrutable supplier networks, it is not clear if leading Chinese facial- and voice-recognition companies on the Commerce Entity List are successfully securing supply chain alternatives from non-American sources. For less hardware reliant companies such as SenseTime, hardware is a smaller concern, and they develop most of their software in-house.[58] Chinese homegrown R&D efforts may or may not be producing meaningful breakthroughs, but even without alternatives, China's thousands of surveillance companies not on the Entity List could freely continue to access U.S.-origin technology because they are not subject to any import restrictions. Furthermore, no stringent Magnitsky sanctions have yet been applied to surveillance companies, although Hikvision is under consideration as reported in May this year, and it is expected the sanctions would significantly jeopardize the company's ability to operate globally.[59]

The promise of big payouts and a wide sea of willing Chinese customers means it may be difficult to stem the tide of non-Chinese surveillance inputs and technology exports.

In 2020, the U.S. State Department released thorough guidance for companies' export considerations.[60] However, the document is nonbinding, and the pull of commercial interests is hard to resist. The promise of big payouts and a wide sea of willing Chinese customers means it may be difficult to stem the tide of non-Chinese surveillance inputs and technology exports. Nonetheless, global public exposure is slowly turning this tide, and it is getting increasingly hard for companies worldwide to claim ignorance of their involvement in China's surveillance state.

Once the investment bans set by the White House in June 2021 and December 2021 go into effect, the ramifications will be interesting to watch. U.S. officials have noted that American investment is problematic partly because it brings a degree of prestige and validation to the Chinese businesses' operations.[61] Loopholes are also likely, as in the case of SenseTime, which has a subsidiary listed on the banned list, as opposed to its parent company.[62]

To augment these steps, democratic governments and civil societies should consider the following recommendations, respectively.

- *First and foremost, the U.S. and its allies should demonstrate that they can produce a viable alternative model by proving that they can use facial recognition, predictive policing, and other AI surveillance tools responsibly at home.* As a first good step, the U.S. Congress should pass a law that requires law enforcement agencies to have warrants for running facial searches and should also place guardrails around search criteria. For example, this law could (1) at minimum, prohibit law enforcement agencies from running any facial recognition searches on individuals peacefully exercising their First Amendment rights, (2) mandate search warrant requirements before running any facial recognition searches for suspected criminal acts, (3) when facial recognition is necessary, require agencies to obtain implicit consent through clearly listed bulletins of facial recognition deployment in public areas, and (4) require explainability in algorithms by design (or "white box" algorithms).[63]

- *Second, the State Department should work with technical experts, such as those that convene at the Global Partnership on AI to propose alternate facial recognition standards at the ITU.*[64] The department should also continue dialogue with EU partners (through the Trade and Technology Council) on how to dovetail their approach to surveillance exports, as well as with Quad partners (Australia, India, and Japan) on R&D and the production of critical technology including AI to ensure that core democratic principles are baked into the technology developed in democracies.

- *Third, the United States and like-minded countries should jointly develop systems to improve the regulation of data transfers and reduce risks.* These should be built around the understanding that AI and digital surveillance technologies also enable data collection that is valuable to actors with downstream data access via the digital supply chain. More needs to be done to ensure that the risks are well understood and that the responses to mitigate them keep up with the current threat landscape. This effort will require (1) a better understanding of the researchers and companies most directly contributing to coercive state surveillance and (2) steps to reduce exposure to them in supply chains.

- *Fourth, the United States and partner democracies should subsidize companies to assist with creating standards to propose at bodies such as the ITU.* It is often prohibitively expensive to participate, with work and travel costing $300,000 per engineer yearly.[65] In response to a recent National Institute of Standards and Technology (NIST) request for information, 12 of the 15 industry groups who replied recommended that the U.S. government subsidize companies' participation through grant funding, potentially via industry associations, and revise the R&D tax credit to include standards development work.[66] NIST could also consider implementing an ethics process whereby companies whose technology abuses human rights cannot take part in their voluntary testing.

- *Fifth, the National Science Foundation and the Defense Advanced Research Projects Agency should fund privacy-preserving computer vision research, where computer vision is deriving information from images or video.* The goals are to automatically anonymize all faces in a crowd and deanonymize only those necessary to pursue investigative leads. This would represent another technical alternative to the Chinese approach and would be similar to approaches already adopted by companies in Europe adhering to the GDPR.[67]

But democratic governments cannot rely on policy alone to shape a more positive vision for AI and digital surveillance technologies and their applications. Civil society must also be engaged in the process. We recommend that:

- *First, civil society organizations (CSOs) should engage in outreach efforts with local communities and community leaders to strengthen public discourse on the advantages and disadvantages of using AI in policing and surveillance.* The organizations should seek to help illuminate and

develop public opinion on democratic frameworks that cover the use of these technologies and then push for policies that align with public opinion.

- *Second, CSOs should engage in or support research on issues related to rights abuses using AI and digital surveillance technologies and the export of these technologies.* In doing so, these organizations could apply increasing pressure on companies through a name and shame approach and engage local leaders on the risks of lock-in, the erosion of sovereignty, and the cybersecurity risks of data leakage.
- *Third, CSOs should actively participate in the setting of international technology standards.* Principally, they should do so by (1) pushing for greater transparency about the development of technical standards on AI and digital surveillance technologies, including facial recognition systems, and (2) advocating for standards to include protections for civil liberties.[68]

References

1 This paper focuses on state actors. For examples of differences in and the management of local U.S. approaches to the adoption of AI and digital surveillance technologies, see these resources: Trisha Thadani, "San Francisco bans city use of facial recognition surveillance technology," *San Francisco Chronicle*, May 14, 2019, https://www.sfchronicle.com/politics/article/San-Francisco-bans-city-use-of-facial-recognition-13845370.php; "Community Control Over Police Surveillance," American Civil Liberties Union, https://www.aclu.org/issues/privacy-technology/surveillance-technologies/community-control-over-police-surveillance; "Atlas of Surveillance," Electronic Frontier Foundation, https://atlasofsurveillance.org/; Clare Garvie and Laura M. Moy, "America Under Watch: Face Surveillance in the United States," (Washington, DC: Georgetown Law Center on Privacy and Technology, May 16, 2019), https://www.americaunderwatch.com.

2 For example: "Mapping China's Tech Giants," International Cyber Policy Centre, Australian Strategic Policy Institute, June 2021, https://chinatechmap.aspi.org.au/; Steven Feldstein, "The Global Expansion of AI Surveillance," (Washington, DC: Carnegie Endowment for International Peace, September 2019), https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847; Paul Mozur, Jonah M. Kessel, and Melissa Chan, "Made in China, Exported to the World: The Surveillance State," *The New York Times*, April 24, 2019, https://www.nytimes.com/2019/04/24/technology/ecuador-surveillance-cameras-police-government.html; Sheena Chestnut Greitens, "Dealing with demand for China's global surveillance exports," (Washington, DC: The Brookings Institution, April 2020), https://www.brookings.edu/research/dealing-with-demand-for-chinas-global-surveillance-exports/; Emily de La Bruyère, Doug Strub, and Jonathon Marek, "China's Digital Ambitions: A Global Strategy to Supplant the Liberal Order," (Washington, DC: The National Bureau of Asian Research, March 2022), https://www.nbr.org/publication/chinas-digital-ambitions-a-global-strategy-to-supplant-the-liberal-order; Arjun Kharpal, "China's surveillance tech is spreading globally, raising concerns about Beijing's influence," CNBC, October 8, 2019, https://www.cnbc.com/2019/10/08/china-is-exporting-surveillance-tech-like-facial-recognition-globally.html; Charles Rollet, "Tiandy's Iran Business, Sells to Revolutionary Guard and Military," IPVM, December 6, 2021, https://ipvm.com/reports/tiandy-iran-business.

3 "China: Police 'Big Data' Systems Violate Privacy, Target Dissent," Human Rights Watch, November 19, 2017, https://www.hrw.org/news/2017/11/19/china-police-big-data-systems-violate-privacy-target-dissent.

4 Dahlia Peterson, "How China harnesses data fusion to make sense of surveillance data," The Brookings Institution, September 23, 2021, https://www.brookings.edu/techstream/how-china-harnesses-data-fusion-to-make-sense-of-surveillance-data/; "China: Police 'Big Data' Systems Violate Privacy, Target Dissent," Human Rights Watch.

5 James Millward and Dahlia Peterson, "China's system of oppression in Xinjiang: How it developed and how to curb it," (Washington, DC: The Brookings Institution, September 2020), https://www.brookings.edu/research/chinas-system-of-oppression-in-xinjiang-how-it-developed-and-how-to-curb-it; Joe Parkinson, Nicholas Bariyo, and Josh Chin, "Huawei Technicians Helped African Governments Spy on Political Opponents," *The Wall Street Journal*, August 15, 2019, https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017; Maya Wang,

"China's Techno-Authoritarianism Has Gone Global: Washington Needs to Offer an Alternative," *Foreign Affairs*, April 8, 2021, https://www.foreignaffairs.com/articles/china/2021-04-08/chinas-techno-authoritarianism-has-gone-global.

6 Tate Ryan-Mosley, "This huge Chinese company is selling video surveillance systems to Iran," *MIT Technology Review*, December 15, 2021, https://www.technologyreview.com/2021/12/15/1042142/chinese-company-tiandy-video-surveillance-iran/.

7 Projects that estimate global tallies of Chinese surveillance exports differ due to the researchers' various definitions of what constitutes AI surveillance exports and due to the intended purpose, research method, and timeline of the project. For example projects, see Sheena Chestnut Greitens, "Dealing with demand for China's global surveillance exports"; Danielle Cave, Samantha Hoffman, Alex Joske, Fergus Ryan, and Elise Thomas, "Mapping China's Tech Giants," (Barton, Australia: Australian Strategic Policy Institute, April 2019), https://www.aspi.org.au/report/mapping-chinas-tech-giants; Danielle Cave, Fergus Ryan, and Vicky Xiuzhong Xu, "Mapping more of China's tech giants: AI and surveillance," (Barton, Australia: Australian Strategic Policy Institute, November 2019), https://www.aspi.org.au/report/mapping-more-chinas-tech-giants. Also see Charles Rollet, "Ecuador's All-Seeing Eye Is Made in China," *Foreign Policy*, August 9, 2018, https://foreignpolicy.com/2018/08/09/ecuadors-all-seeing-eye-is-made-in-china/; Katherine Atha, Jason Callahan, John Chen, Jessica Drun, Ed Francis, Kieran Green, Brian Lafferty, Joe McReynolds, James Mulvenon, Benjamin Rosen, and Emily Walz, "China's Smart Cities Development," (Washington, DC: U.S.-China Economic and Security Review Commission, January 2020), https://www.uscc.gov/sites/default/files/China_Smart_Cities_Development.pdf.

8 Meng Jing, "Chinese tech companies are shaping UN facial recognition standards, according to leaked documents," *South China Morning Post*, December 2, 2019, https://www.scmp.com/tech/policy/article/3040164/chinese-tech-companies-are-shaping-un-facial-recognition-standards.

9 For example: Daniel Elizalde, "The 5 Layers of the IoT Technology Stack," https://danielelizalde.com/iot-primer/; "An introduction to the IoT technology stack and its components," i-SCOOP, https://www.i-scoop.eu/internet-of-things-iot/iot-technology-stack-devices-gateways-platforms/; "IoT Technology Stack," PTC, https://www.designtechproducts-ptc-iiot.com/articles/iot-technology-stack; Itikar Sarkar, "IoT Technology Stack," IoTEDU, April 26, 2020, https://iot4beginners.com/iot-technology-stack/.

10 "Biometric security systems: a guide to devices, fingerprint scanners and facial recognition access control," IFSEC Global, August 12, 2020, https://www.ifsecglobal.com/global/biometric-security-systems-guide-devices-fingerprint-scanners-facial-recognition/; "Biometrics," U.S. Department of Homeland Security, https://www.dhs.gov/biometrics; "Notice on Fingerprints Collection of Visa Applicants," Embassy of the People's Republic of China in the Commonwealth of Australia, February 3, 2021, https://www.mfa.gov.cn/ce/ceau/eng/tzgg/t1850768.htm; Asha Barbaschow, "Australia has a new biometric border processing system," ZDNet, June 3, 2020, https://www.zdnet.com/article/australia-has-a-new-biometric-border-processing-system/.

11 Australia's Department of Home Affairs, for example, says biometrics "protect you [a visa applicant] from identity fraud," "make travel to Australia safer," and "secure our [Australia's] borders." The United States Department of Homeland Security says biometric surveillance is used "to detect and prevent illegal entry into the U.S., grant and administer proper immigration benefits, vetting and credentialing, facilitating legitimate travel and trade, enforcing federal laws, and enabling verification for visa applications to the U.S. See "Biometrics," U.S.

Department of Homeland Security; "Biometrics," Australian Government Department of Home Affairs, https://immi.homeaffairs.gov.au/help-support/meeting-our-requirements/biometrics.

12 Kate Crawford, "Time to regulate AI that interprets human emotions," *Nature*, April 6, 2021, https://www.nature.com/articles/d41586-021-00868-5.

13 Alex Najibi, "Racial Discrimination in Face Recognition Technology," Science in the News, Harvard University, October 24, 2020, https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/; Amy Harmon, "As Cameras Track Detroit's Residents, a Debate Ensues Over Racial Bias," *The New York Times*, July 8, 2019, https://www.nytimes.com/2019/07/08/us/detroit-facial-recognition-cameras.html.

14 Alex Najibi, "Racial Discrimination in Face Recognition Technology"; Russell Contreras, "Technology, Policing and Racial Bias," Axios, October 16, 2021, https://www.axios.com/technology-policing-and-racial-bias-bb0de2a2-0bce-4d40-a327-7a478bb16cb8.html; Nick David Dee Delgado, "U.N. Panel: Digital Technology in Policing Can Reinforce Racial Bias," *The New York Times*, November 26, 2020, https://www.nytimes.com/2020/11/26/us/un-panel-technology-in-policing-can-reinforce-racial-bias.html.

15 Eileen Li, "Europe's Next Steps in Regulating Facial Recognition Technology," *Columbia Journal of Transnational Law*, November 7, 2021, https://www.jtl.columbia.edu/bulletin-blog/europes-next-steps-in-regulating-facial-recognition-technology; Melissa Heikkilä, "European Parliament calls for a ban on facial recognition," *Politico*, October 6, 2021, https://www.politico.eu/article/european-parliament-ban-facial-recognition-brussels; Luca Bertuzzi, "Facial recognition technologies already used in 11 EU countries and counting, report says," Euractiv, October 26, 2021, https://www.euractiv.com/section/data-protection/news/facial-recognition-technologies-already-used-in-11-eu-countries-and-counting-report-says.

16 "Dahua and Hikvision Co-Author Racial and Ethnic PRC Police Standards," IPVM, March 30, 2021, https://ipvm.com/reports/racial-ethnic-standards; Leo Kelion, "Huawei patent mentions use of Uighur-spotting tech," BBC News, January 13, 2021, https://www.bbc.com/news/technology-55634388; "China: Police 'Big Data' Systems Violate Privacy, Target Dissent," Human Rights Watch; "Mapping China's Tech Giants," Australian Strategic Policy Institute.

17 Charles Rollet, "China Government Spreads Uyghur Analytics Across China," IPVM, November 25, 2019, https://ipvm.com/reports/ethnicity-analytics.

18 Conor Healy, "Uyghur Surveillance & Ethnicity Detection Analytics in China," (Bethlehem, PA: IPVM, August 20, 2021), 4, https://uyghurtribunal.com/wp-content/uploads/2021/09/Conor-Healy.pdf.

19 "Standardization Law of the People's Republic of China," Standardization Administration of China, March 23, 2018, https://archive.vn/1z3sJ. The Standardization Law was revised and adopted at a meeting of the Standing Committee of the National People's Congress in November 2017 and came into force on January 1, 2018; "China—Standards for trade," Export.gov, July 20, 2019, https://www.export.gov/apex/article2?id=China-Trade-Standards; "Dahua and Hikvision Co-Author Racial and Ethnic PRC Police Standards," IPVM; Samantha Hoffman, "Double-Edged Sword: China's Sharp Power Exploitation of Emerging Technologies," (Washington, DC: National Endowment for Democracy, April 2021), https://www.ned.org/sharp-power-democratic-resilience-chinas-exploitation-of-emerging-technologies/; "Mapping China's Tech Giants," Australian Strategic Policy Institute.

20 Charles Rollet, "China Government Spreads Uyghur Analytics Across China."

21 These include Huawei, Hikvision, Dahua, Megvii, Alibaba, Tiandy, and SenseTime. See Conor Healy, "Uyghur Surveillance & Ethnicity Detection Analytics in China."

22 Conor Healy and Donald Maye, "Punishing Journalists PRC Province's Latest Mass Surveillance Project, Won by Neusoft Powered By Huawei," IPVM, November 29, 2021, https://ipvm.com/reports/henan-neusoft.

23 Chris Burt, "Ready facial recognition market among French soccer clubs restrained by regulator," Biometric Update, October 29, 2021, https://www.biometricupdate.com/202110/ready-facial-recognition-market-among-french-soccer-clubs-restrained-by-regulator; "Mapping Huawei's Smart Cities creep," Privacy International, November 17, 2021, https://privacyinternational.org/long-read/4689/mapping-huaweis-smart-cities-creep.

24 "Myanmar: Post-Coup Legal Changes Erode Human Rights," Human Rights Watch, March 2, 2021, https://www.hrw.org/news/2021/03/02/myanmar-post-coup-legal-changes-erode-human-rights.

25 "Myanmar: Facial Recognition System Threatens Rights," Human Rights Watch, March 12, 2021, https://www.hrw.org/news/2021/03/12/myanmar-facial-recognition-system-threatens-rights.

26 Ibid.

27 Gaspar Pisanu, Verónica Arroyo, Leandro Ucciferri, Eduardo Ferreyra, Thiago Moraes, José Renato Laranjeira, Eduarda Costa Almeida, Fernando Fellows Dourado, Carolina Reis, Felipe Rocha da Silva, Jonathan Finlay, and Anais Córdova-Páez, "Surveillance Tech in Latin America: Made Abroad, Deployed at Home," (Brooklyn, NY: Access Now, August 2021), https://www.accessnow.org/surveillance-tech-in-latin-america-made-abroad-deployed-at-home/; Myat Thura, "Nay Pyi Taw authorities activate 335 cameras able to detect faces, *The Myanmar Times*, December 23, 2020, https://www.mmtimes.com/news/nay-pyi-taw-authorities-activate-335-cameras-able-detect-faces.html.

28 Gaspar Pisanu, Verónica Arroyo, Leandro Ucciferri, Eduardo Ferreyra, Thiago Moraes, José Renato Laranjeira, Eduarda Costa Almeida, Fernando Fellows Dourado, Carolina Reis, Felipe Rocha da Silva, Jonathan Finlay, and Anais Córdova-Páez, "Surveillance Tech in Latin America"; Verónica Arroyo, "Instead of banning facial recognition, some governments in Latin America want to make it official," Access Now, December 16, 2020, https://www.accessnow.org/facial-recognition-latin-america.

29 Verónica Arroyo, "Instead of banning facial recognition, some governments in Latin America want to make it official."

30 Ibid.

31 Michael Standaert, "Smile for the camera: the dark side of China's emotion-recognition tech," *The Guardian*, March 3, 2021, https://www.theguardian.com/global-development/2021/mar/03/china-positive-energy-emotion-surveillance-recognition-tech.

32 See the data for the companies within "Mapping China's Tech Giants," International Cyber Policy Centre, Australian Strategic Policy Institute, https://chinatechmap.aspi.org.au/#/map/f2-CloudWalk,f2-Dahua,f2-Hikvision,f2-Megvii,f2-SenseTime,f2-YITU,f5-Facial%20recognition.

33 "Megvii accelerates international roll-out of Koala smart access solution," PR Newswire, November 16, 2020, http://web.archive.org/web/20201121224932/http://www.itnewsonline.com/PRNewswire/Megvii-accelerates-international-roll-out-of-Koala-smart-access-solution/720159.

34 Specific projects can be found in "Mapping China's Tech Giants," International Cyber Policy Centre, Australian Strategic Policy Institute, https://chinatechmap.aspi.org.au/#/map/marker-2119.

35 "The New Big Brother: China and Digital Authoritarianism," (Washington, DC: Committee on Foreign Relations, United States Senate, July 21, 2020), 32, https://www.foreign.senate.gov/imo/media/doc/2020%20SFRC%20Minority%20Staff%20Report%20-%20The%20New%20Big%20Brother%20-%20China%20and%20Digital%20Authoritarianism.pdf.

36 Specific projects can be found in "Mapping China's Tech Giants," International Cyber Policy Centre, Australian Strategic Policy Institute, https://chinatechmap.aspi.org.au/#/map/marker-749.

37 Gaspar Pisanu, Verónica Arroyo, Leandro Ucciferri, Eduardo Ferreyra, Thiago Moraes, José Renato Laranjeira, Eduarda Costa Almeida, Fernando Fellows Dourado, Carolina Reis, Felipe Rocha da Silva, Jonathan Finlay, and Anais Córdova-Páez, "Surveillance Tech in Latin America."

38 Sheena Chestnut Greitens, "Dealing with demand for China's global surveillance exports."

39 Ibid.

40 Specific projects can be found in "Mapping China's Tech Giants," International Cyber Policy Centre, Australian Strategic Policy Institute, https://chinatechmap.aspi.org.au/#/map/f2-Huawei,f5-Smart%20City-Public%20Security%20project.

41 "Visual AI Company AnyVision Changes its Name to Oosto," Oosto, October 27, 2021, https://oosto.com/press/anyvision-now-oosto/; Sophia Goodfriend, "How the Occupation Fuels Tel Aviv's Booming AI Sector," *Foreign Policy*, February 21, 2022, https://foreignpolicy.com/2022/02/21/palestine-israel-ai-surveillance-tech-hebron-occupation-privacy.

42 Ryan Gallagher, "How U.S. Tech Giants are Helping to Build China's Surveillance State," The Intercept, July 11, 2019, https://theintercept.com/2019/07/11/china-surveillance-google-ibm-semptian.

43 Christopher A. Padilla, "A Precision Regulation Approach to Controlling Facial Recognition Technology Exports," ThinkPolicy Blog, IBM, September 11, 2020, https://www.ibm.com/blogs/policy/facial-recognition-export-controls/.

44 John Honovich, "IBM Video Analytics Reborn," IPVM, May 1, 2020, https://ipvm.com/reports/ibm-2020.

45 Margaret Coker and Paul Sonne, "Life Under the Gaze of Gadhafi's Spies," *The Wall Street Journal*, December 14, 2011, https://www.wsj.com/articles/SB10001424052970203764804577056230832805896.

46 Trevor Timm and Jillian C. York, "Surveillance Inc: How Western Tech Firms Are Helping Arab Dictators," *The Atlantic*, March 6, 2012, https://www.theatlantic.com/international/archive/2012/03/surveillance-inc-how-western-tech-firms-are-helping-arab-dictators/254008/.

47 Ryan Gallagher, "'Zero-Click' Hacks Are Growing in Popularity. There's Practically No Way to Stop Them," Bloomberg Businessweek, February 17, 2022, https://www.bloomberg.com/news/articles/2022-02-17/-zero-click-hacks-by-nso-group-and-others-growing-in-popularity.

48 "Huawei, controversial in the West, is going strong in the Gulf," France 24, February 25, 2021, https://www.france24.com/en/live-news/20210225-huawei-controversial-in-the-west-is-going-strong-in-the-gulf; Bradley Jardine, "China's Surveillance State Has Eyes on Central Asia," *Foreign Policy*, November 15, 2019, https://foreignpolicy.com/2019/11/15/huawei-xinjiang-kazakhstan-uzbekistan-china-surveillance-state-eyes-central-asia/; Alessandra Briganti, "Serbia's smart city has become a political flashpoint," *Wired*, October 8, 2021, https://www.wired.co.uk/article/belgrade-huawei-cameras.

49 "ATM BRI, Jakarta," Uniview, February 6, 2021, https://archive.vn/ZSH9e.

50 "PLN Substations in Jakarta, Indonesia," Uniview, July 26, 2018, https://archive.ph/Wvvbm.

51 Samantha Hoffman and Nathan Attrill, "Mapping China's Tech Giants: Supply chains & the global data collection ecosystem," (Barton, Australia: Australian Strategic Policy Institute, June 2021), https://www.aspi.org.au/report/mapping-chinas-tech-giants-supply-chains-and-global-data-collection-ecosystem.

52 Joshua Kurlantzick, "Assessing China's Digital Silk Road: A Transformative Approach to Technology Financing or a Danger to Freedoms?," Council on Foreign Relations, December 18, 2020, https://www.cfr.org/blog/assessing-chinas-digital-silk-road-transformative-approach-technology-financing-or-danger.

53 For example, Alibaba Cloud's exemption for personal data disclosures to authorities follows "lawful requests by public authorities, including to meet national security or law enforcement requirements." See "Mapping China's Tech Giants," International Cyber Policy Centre, Australian Strategic Policy Institute.

54 Anna Gross, Madhumita Murgia, and Yuan Yang, "Chinese tech groups shaping UN facial recognition standards," *Financial Times*, December 1, 2019, https://www.ft.com/content/c3555a3c-0d3e-11ea-b2d6-9bf4d1957a67.

55 Meng Jing, "Chinese tech companies are shaping UN facial recognition standards, according to leaked documents."

56 Ana Swanson, "U.S. and Others Pledge Export Controls Tied to Human Rights," *The New York Times*, December 10, 2021, https://www.nytimes.com/2021/12/10/business/economy/human-rights-export-controls.html; "Fact Sheet: Export Controls and Human Rights Initiative Launched at the Summit for Democracy," The White House, December 10, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/12/10/fact-sheet-export-controls-and-human-rights-initiative-launched-at-the-summit-for-democracy.

57 Dahlia Peterson, "Foreign Technology and the Surveillance State" in *China's Quest for Foreign Technology: Beyond Espionage*, eds. William C. Hannas and Didi Kirsten Tatlow (London: Routledge, 2021).

58 Johana Bhuiyan, "US sanctioned China's top facial recognition firm over Uyghur concerns. It still raised millions," *The Guardian*, January 7, 2022, https://www.theguardian.com/world/2022/jan/06/china-sensetime-facial-recognition-uyghur-surveillance-us-sanctions.

59 Demetri Sevastopulo, "US moves towards imposing sanctions on Chinese tech group Hikvision," *Financial Times*, May 3, 2022, https://www.ft.com/content/7bc70335-138e-4f56-afe1-ae4383eefb2b; Dahlia Peterson, "The Case for Applying Global Magnitsky Sanctions Against Hikvision," *The National Interest*, June 6, 2022, https://nationalinterest.org/blog/techland-when-great-power-competition-meets-digital-world/case-applying-global-magnitsky.

60 "Guidance on Implementing the UN Guiding Principles for Transactions Linked to Foreign Government End-Users for Products or Services with Surveillance Capabilities," (Washington, DC: U.S. Department of State, September 2020), https://www.state.gov/key-topics-bureau-of-democracy-human-rights-and-labor/due-diligence-guidance/.

61 Ellen Nakashima and Jeanne Whalen, "Biden administration concerned about U.S. investments in Chinese tech companies with military or surveillance ties," *The Washington Post*, December 16, 2021, https://www.washingtonpost.com/national-security/us-investments-china-biden/2021/12/15/835876a0-5772-11ec-a808-3197a22b19fa_story.html.

62 Johana Bhuiyan, "US sanctioned China's top facial recognition firm over Uyghur concerns. It still raised millions."

63 Bills H.R.4021 and S.3284 from the 116th Congress called for warrant requirements on law enforcement facial recognition use. See FACE Protection Act of 2019, H.R.4021, 116th Cong. (2019), https://www.congress.gov/bill/116th-congress/house-bill/4021; Ethical Use of Facial Recognition Act, S.3284, 116th Cong. (2020), https://www.congress.gov/bill/116th-congress/senate-bill/3284. For more on black box versus white box algorithms, see Octavio Loyola-González, "Black-Box vs. White-Box: Understanding Their Advantages and Weaknesses From a Practical Point of View," *IEEE Access* 7, no.1 (October 2019): 154096-154113, https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8882211.

64 "About GPAI," The Global Partnership on Artificial Intelligence, https://gpai.ai/about.

65 Jeanne Whalen, "Government should take bigger role in promoting U.S. technology or risk losing ground to China, commission says," *The Washington Post*, December 1, 2020, https://www.washingtonpost.com/technology/2020/12/01/us-policy-china-technology.

66 Jacob Feldgoise and Matt Sheehan, "How U.S. Businesses View China's Growing Influence in Tech Standards," Carnegie Endowment for International Peace, December 23, 2021, https://carnegieendowment.org/2021/12/23/how-u.s.-businesses-view-china-s-growing-influence-in-tech-standards-pub-86084.

67 Adam Bannister, "Face-pixellating module is first video surveillance product to be declared 'GDPR-ready' by EuroPriSe," IFSEC Global, November 20, 2017, https://www.ifsecglobal.com/video-surveillance/face-pixellating-module-first-video-surveillance-product-declared-gdpr-ready-europrise.

68 Samantha Hoffman, "Double-Edged Sword."

About the authors

Dahlia Peterson is a research analyst at Georgetown University's Center for Security and Emerging Technology (CSET). At CSET, she focuses on how China harnesses predictive policing algorithms and facial, voice, and gait recognition technologies for AI-powered surveillance programs within China and globally, as well as how China is developing its AI education and workforce pipelines. Her work has been published by the Brookings Institution, Routledge, The Hill, The National Interest, and The Diplomat. She has been quoted in The Wall Street Journal, Marketplace, and multiple foreign media outlets. She previously worked for the U.S.-China Economic and Security Review Commission (USCC), the State Department's Virtual Student Federal Service, and the Foreign Commercial Service at the U.S. Embassy in Beijing. She holds a B.A. in Economics and Chinese Language with a minor in China Studies from the University of California, Berkeley and is pursuing a M.A. in Security Studies from Georgetown University.

Samantha Hoffman is a senior analyst at the Australian Strategic Policy Institute's International Cyber Policy Centre and an independent consultant. Her work explores the domestic and global implications of China's expansive approach to state security. It offers new ways of thinking about understanding and responding to China's pursuit of AI and big data-enabled capabilities to augment political and social control. Hoffman has publicly testified in the U.S. Congress, the House of Commons of the United Kingdom, and the European Parliament. She has been frequently quoted in outlets such as the BBC, The New York Times, the Financial Times, The Washington Post, The Wall Street Journal, Foreign Policy, and The Guardian. Hoffman holds a Ph.D. in Politics and International Relations from the University of Nottingham, an MSc in Modern Chinese Studies from the University of Oxford, a B.A. in International Affairs and Chinese Language and Culture from Florida State University.

Acknowledgements

Lori Merritt and Ted Reinert edited this paper, and Rachel Slattery provided layout. The authors would like to thank Steven Feldstein, Brian Kot, Chris Meserole, and Charles Rollet for helpful feedback on drafts.

Disclaimer