OCTOBER 2020

Designing Alternatives to China's Repressive Surveillance State

CSET Policy Brief

AUTHOR
Dahlia Peterson

Executive Summary

Since the 1950s, China has built a formidable surveillance state increasingly reliant on artificial intelligence (AI) technologies. The COVID-19 pandemic has provided China an opportunity to soften the reputation of its surveillance technologies, which include tracking apps, surveillance by drones, cameras inside and outside houses, remote temperature scanning, and upgraded facial recognition to identify mask wearers. These technologies have now been legitimized for public health purposes. COVID-19 may accelerate China's domestic surveillance efforts and lead to investments creating capabilities preserved post-COVID.

Globally, China's surveillance model may gain even more legitimacy as a vital tool beyond the pandemic, further deepening normative advantages for China by allowing the strategic expansion of Chinese surveillance companies worldwide. Since 2008, at least 80 countries have adopted Chinese surveillance technology platforms. These platforms are more than just security cameras: they integrate multiple government databases and provide analytic capabilities that can support multiple command and control centers. If democratic governments do not successfully demonstrate how to protect public health and human rights, they risk losing the mantle of global leadership in the 21st century. The United States must therefore better understand China's surveillance infrastructure and why it appeals to adopting countries, using this knowledge to advance an alternate vision with its democratic allies.

China employs surveillance to repress broad swaths of its population—most notably the Uyghurs in Xinjiang and nationwide—and enables other countries to execute their own surveillance systems through export of its technologies. However, several nationwide surveillance programs have escaped sustained attention. This paper will detail how these programs work and how they have enabled the deployment of current COVID-19 surveillance techniques.

The United States and its allies can meet these challenges in several ways. First, the United States must reduce domestic human rights harms and racial injustice by its own companies and institutions. Second, the State Department's Bureau of Democracy, Human Rights and Labor (DRL) can host Track 1.5 dialogues modeled off State's Civil Society 2.0 and the Open Government Partnership to engage democratic government and non-government stakeholders in Europe, Asia, and beyond. These dialogues can

identify areas and companies engendering the greatest human rights harms from surveillance, compare and obtain best practices from existing privacy and surveillance legislation, and coordinate with the European approach to surveillance export controls—which aims to restrict surveillance technology exports on normative and non-military human rights grounds.

On the technical level, national research funding organizations such as the National Science Foundation (NSF) and the Defense Advanced Research Projects Agency should support research on privacy-preserving facial recognition systems. Bodies such as the National Institute of Standards and Technology should also expand prior research on error mitigation in facial recognition. U.S. representatives should actively engage the Global Partnership on AI's technical expertise to propose alternate facial recognition standards to Chinese companies' submissions at the United Nations' International Telecommunications Union.

Table of Contents

The Rise of China's Surveillance State

Since the advent of the People's Republic in 1949, China has honed its surveillance state to guarantee sociopolitical control. Tools deployed relied heavily, if not exclusively, on manual methods, including through *danwei* employment units, the *hukou* residency registration system, and *dang'an* secret political files.[1] As China began to reform and open up in 1979, traditional methods lost much of their effectiveness.[2] Not least, the 1989 pro-democracy protests and the following bloody crackdown, along with the domestic rise of the internet, led the Party-state leadership to tighten surveillance over an increasingly mobile and vocal citizenry. Starting in the early 1990s, technological methods began replacing many manual tools, giving rise to the modern surveillance state.

China's surveillance state combines automated and manual approaches. Officials maintain national DNA databases and extensive video surveillance networks of public and residential spaces, as well as monitor and censor internet and phone communications—enforcing de-anonymization through real-name registration requirements.[3] AI is increasingly used for facial recognition, identifying persons and patterns of interest through predictive policing, and automating content moderation.[4] Yet despite the government's vision of big data seamlessly updating dossiers in real time, implementation has been hindered by human inefficiency, unreliable and incomplete basic data, and incompatible datasets or systems.[5] These capabilities are often deployed as "programs" that integrate multiple databases and support command and control centers with analytic capabilities.[6]

Since 2003, the Chinese government has deployed several major national-level surveillance programs, overlapping with and in some cases advancing their predecessors' goals and physical infrastructure. This paper focuses on these programs due to the availability of open source information, their nationwide reach, or the possibility that their currently localized approaches may expand across China.

It is worth noting up front that the scope of these programs and their relationships to one another are frequently unclear, and there is no reliable local or nationwide breakdown of the number of facial recognition-equipped cameras.[7] There are also no independently verified figures for private versus publicly owned cameras, and whether these cameras feed both local and national surveillance systems. The same uncertainty applies to the number of

cameras dedicated to commercial applications—such as paying at retail stores by entering the phone number linked to your government-issued ID and verifying your face—versus public security applications.[8]

China's major surveillance programs are examined further in the following sections.

The Golden Shield Project (金盾工程)

The Ministry of Public Security (MPS) launched the Golden Shield Project in the early 2000s to meet the Party-state's growing demand for greater social control over the entire population—especially political dissidents. The project incorporates technologies now central to China's surveillance apparatus, such as internet censorship and facial and voice recognition.[9] It was initially rolled out in two main phases: first through population databases, ID tracking systems, and internet surveillance tools, then through surveillance camera systems.[10]

According to state-run media, between 2003 and 2006, the MPS logged personal information for 96 percent (or 1.2 out of 1.3 billion) of China's citizens.[11] Facial and voice recognition technologies are key to China's surveillance development, as examined in the following sections.

Safe Cities (平安城市) and Skynet (天网工程)

China achieved greater social control through Safe Cities and Skynet, two similar programs that work in tandem and are frequently thought of as synonymous within China. However, each program has distinct features. The Ministry of Public Security and the Ministry of Science and Technology launched Safe Cities in 2003.[12] It provides disaster warnings, urban and traffic management, and public security maintenance through three interlocking systems covering technical, physical, and civil air defense.[13] By 2005, it encompassed 22 provinces and 21 cities.[14]

Skynet (天网工程) was launched in 2005 by the MPS and the Ministry of Industry and Information Technology (MIIT) to "fight crime and prevent possible disasters" through a nationwide network of closed-circuit television cameras.[15] It uses network gateways to deliver surveillance footage captured by CCTV in public areas—such as main thoroughfares and security checkpoints—to command centers.[16] Skynet purportedly provides 24/7

coverage of major districts, streets, schools, and business areas, and timed surveillance over smaller streets.[17] Chinese media often portrays Skynet as a "facial recognition system," though it remains unclear how many cameras are facial recognition-equipped—especially given the rudimentary state of the technology in 2005.[18] By 2018, Safe Cities' scope still appeared broader than Skynet, which was purportedly active in 16 cities, provinces, and municipalities, with 20 million cameras in use.[19]

Chinese state-run media has claimed Skynet can scan the entire Chinese population in one second with 99.8 percent accuracy, yet such claims ignore glaring technical limitations.[20] The vice president of Chinese AI unicorn and facial recognition giant Megvii—which created Face++—said the technology cannot run 24/7 and would need a supercomputer to viably scan more than 1,000 faces at a time.[21] Connecting to supercomputing capabilities over the cloud is also considered too risky from a security perspective, meaning Face++ may rely more on slower, limited options.[22] More broadly, technical issues from retrofitting existing video surveillance systems with facial recognition will almost certainly produce lower grade images or slower response times.[23]

Deep learning may help overcome the technical limitations posed by retrofitting. Hikvision and Dahua Technologies—two Chinese companies commanding the world's largest market shares in video surveillance subjected to U.S. government usage bans[24] and export controls[25]—have been increasingly active in this area. Hikvision, which began exploring deep learning applications in 2012,[26] claims deep learning algorithms can achieve "comparable or even better-than-human pattern recognition accuracy and the ability to classify and recognize thousands of features," with average facial recognition accuracy increasing by 38 percent.[27] Dahua has likewise stated that systems trained on deep learning algorithms can be applied to poorer image quality and wider angles.[28]

Sharp Eyes (雪亮工程)

To extend and upgrade the infrastructure used by prior programs like Golden Shield, Safe Cities, and Skynet, China's National Development and Reform Commission (NDRC), the Central Political and Legal Affairs Commission, the MPS, and six other government bodies launched the national program Sharp Eyes (雪亮工程) in 2015.[29] The program expanded on a predecessor program from circa 2011 called Village-to-Village Surveillance (村村通视

频监控), which had begun integrating Skynet surveillance with civilian cameras.[30] It sought to better integrate rural-urban surveillance and to address high crime rates in rural areas, attributed to insufficient police and security camera coverage.[31] Sharp Eyes' chief goal was to provide full, real-time rural surveillance coverage by 2020.[32] It has mostly succeeded in establishing community-driven "grid management"(网格化管理), which divides cities into administrative units and integrates data to identify and resolve social management issues.[33] The program next seeks to enhance data integration, as video surveillance data is still siloed, and no standard data mining approach exists.[34]

Unlike prior programs, Sharp Eyes places surveillance capabilities in citizens' hands and encourages their direct participation. This strategy echoes the surveillance mechanisms of the Cultural Revolution, the period from which Sharp Eyes derives its name.[35] In Linyi, Shandong, where the program was born, cable boxes on citizens' televisions were upgraded to directly display surveillance feeds and enable crime reporting via TV remote controls.[36] One propaganda slogan from the MPS declared, "remote control in hand, safety in heart."[37] Yet breaching the private sphere has raised concerns among citizens that surveillance can be brought directly into their homes.[38]

Other examples of community-led Sharp Eyes surveillance in Linyi centered on mobile apps. One project—"Everyone is a Safety Officer" (人人都是平安员工程)—stemmed from a mobile app that pushed video surveillance and public security information to citizens. Similarly, the "Neighbors Help Each Other"(邻里互助工程) project established groups of households to monitor and report public security incidents via app.[39]

Predictive Policing

China has also made predictive policing—a data-driven approach to anticipatory, preventative law enforcement—a central aspect of its surveillance model, while certain U.S. cities have prioritized this at the local level.[40] Predictive policing underpins two platforms in China: the nationwide Police Cloud(警务云) program and the Integrated Joint Operations Platform(一体化联合作战平台), which originated and focuses primarily on widespread surveillance of individuals in Xinjiang.

Police Cloud (警务云)

In 2015, the MPS launched Police Cloud via provincial-level cloud-computing centers for police.[41] It links personal information to use of government-issued ID cards, and connects otherwise disparate databases across the public and private sector in a national Police Cloud database.[42] This repository includes CCTV footage, medical history, supermarket memberships, IP addresses, social media usernames, delivery records, residential addresses, hotel stays, records of petitioning to the government, and biometrics, among other information.[43] The authorities primarily use Police Cloud to enhance human-led policing activities, tracking individuals' locations and personal relationships, "visualizing" otherwise unseen correlations, and purportedly predicting future actions.[44]

Such dragnet surveillance raises human rights concerns for every individual unwittingly implicated, but is especially concerning for seven categories of "focus personnel." This label includes petitioners, those supposedly involved in terrorism, and those "undermining social stability."[45] Under such a definition, the Chinese police have a wide purview to surveil individuals they believe pose a threat to social stability and/or their rule. Moreover, a significant gray area exists in Chinese legal discourse: while citizens cannot be charged for crimes they are suspected of planning to commit, citizens can be charged for attempting to commit crimes.[46]

Xinjiang's Integrated Joint Operations Platform (一体化联合作战平台)

The northwestern region of Xinjiang has often been described as the "testbed" for Chinese surveillance technology, but the technology's spread within China has not been so unidirectional. Nonetheless, while neither Sharp Eyes nor Skynet originated in Xinjiang, the region has borne the brunt of China's most intrusive surveillance innovations, which act as a blueprint for police planning and implementation throughout China.[47] Xinjiang's innovations include a blend of predictive policing, biometric surveillance under the guise of public health checks, and facial and voice recognition with human policing methods like omnipresent "convenience police stations" and house stays by government officials—all of which have enabled widespread coercion.[48]

The Integrated Joint Operations Platform (IJOP, 一体化联合作战平台) serves as the most prominent example of testbed surveillance. It monitors

relationships by tracing phones, vehicles, and ID cards; it also connects to CCTV cameras enabled with facial recognition and night vision.[49] The platform treats many ordinary and lawful activities—such as using WhatsApp or VPNs, driving a car that is not theirs, or using "too much" electricity—as inherently suspicious.[50] It automatically alerts officers of these individuals for interrogation. Outside the camps, the IJOP forms a series of invisible or virtual fences, restricting movements based on perceived threat levels.[51]

The systematic deployment of advanced surveillance technology has facilitated the Chinese government's intensifying repression of Xinjiang's ethnic Uyghur and Turkic Muslim populations. IJOP surveillance has led to the mass arbitrary detention of innocent individuals in a network of nearly 1,200 internment camps, enabling the forced political indoctrination of between one and three million Turkic Muslims.[52]

China's COVID-19 Surveillance Toolkit

The commercial viability of China's surveillance technologies boosts their legitimacy and appeal, raising human rights concerns. The COVID-19 pandemic has provided the state with a bigger opportunity to tout its surveillance apparatus. These technologies—including tracking apps, surveillance by drones, cameras inside and outside houses, remote temperature scanning, and upgraded facial recognition to identify mask wearers—have been sanitized and legitimized for public health purposes.[53]

Location Tracking

Location tracking and data mining by apps underpin this approach.[54] One example is Alipay Health Code, developed by Alibaba's Ant Financial and used by 700 million people in more than 200 cities nationwide.[55] It provides a color-coded breakdown of predicted health risk based on user-inputted personal information, such as government-issued ID number, residence location, and human interactions.[56] In turn, the app changes colors, often arbitrarily, to determine freedom of movement.[57] Source code analysis revealed that Health Code shares data with the MPS, raising concerns of user location tracking continuing after the pandemic.[58]

Upgraded Video Surveillance

China's approach also relies on video surveillance, which has been upgraded to include non-facial recognition methods. The aforementioned Skynet program inspired a prominent Chinese scientist to propose a similar approach to tracking COVID-19.[59] Access control systems of some residential buildings use facial recognition-equipped technology, allowing only green Health Code holders to enter—an indication that Health Code and entry systems are linked.[60] Additionally, MIIT spotlighted a state-owned enterprise called Potevio（普天信息工程设计服务有限公司）for helping combat coronavirus with its "AI Close Contact Catcher."[61] It purportedly overcomes problems in existing systems such as Skynet, which is struggling with degraded facial recognition accuracy rates due to widespread mask wearing.[62] Potevio claims to rely instead on pedestrian detection and relocation technology to retrace close contacts of suspected cases, and detect unauthorized abnormal behaviors by quarantined individuals (such as intentional transmission by a confirmed case and/or violation of quarantine).[63]

Chinese AI unicorn SenseTime and Hanwang Technology (Hanvon)—two companies with ties to Xinjiang that count the MPS as customers—have also upgraded technology to identify masked faces.[64] Whether or not such detection methods prove viable for identifying and tracking individuals, these technologies could be used to track "focus personnel" and their contacts beyond the pandemic, even if they partially obscure their faces to evade identification.[65]

Key Concerns

China's coronavirus surveillance toolkit will likely outlast the pandemic for several reasons, raising serious concerns for the United States. First, China has a history of developing cutting-edge surveillance infrastructure, along with a clear willingness to pilot and deploy technologies in spite of human rights impacts. Second, while the Chinese Constitution claims to safeguard "privacy of correspondence," China does not have a comprehensive privacy protection law, and investigations have found Chinese authorities placed the personal data of millions of its citizens on unprotected servers and granted private contractors data access.[66] Privacy regulations are piecemeal and limited to the commercial sphere.[67] Overall, China's concept of "prevention

and control"（防控）to counter domestic unrest is also being applied for public health purposes.[68]

Additionally, no substantive legal discussion seems to exist within China on sunsetting these technologies or proactively building in sunset clauses—in fact, the opposite may be true. The only indications of self-imposed limitations come from a Cyberspace Administration of China (CAC) notice in February 2020 stating that personal information collected for epidemic prevention and control and disease prevention can only be collected by agencies authorized by the State Council's health department; moreover, the data cannot be used for other purposes, and cannot be disclosed without individuals' consent.[69] Additionally, a May draft civil code does not appear to extend protection to individuals from surveillance.[70] Otherwise, in Health Code's birthplace of Hangzhou, officials are considering releasing an app ranking citizens with a "personal health index" from zero to 100 by the end of June, while Shanghai wants to expand its app to a broader digital assistant to induce further use.[71] It is unclear how this data would be used, how the CAC guidance would precisely apply, or what punishments would be meted out for violations. At a minimum, such indexes penalizing drinking wine or insufficient sleep could discriminate against behaviors not considered problematic before the pandemic, nor necessarily relevant to preventing its spread.[72]

Given China's long-term poor human rights record, legal climate, and current messaging, these technologies will likely persist long after the pandemic.[73] China can continue to forcefully enforce quarantine and discriminate against, or crack down, on already repressed groups—such as religious minorities and political dissidents—for whatever reasons it chooses.[74] Even beyond China, history has shown that surveillance introduced under the guise of emergency measures often fails to meet its objectives, yet becomes more integral to surveillance regimes.[75] Human rights organizations agree that increased surveillance measures will be unlawful under international frameworks unless China can meet strict criteria, justifying the technology as necessary, proportionate, time-bound, transparent, and not doing more harm than good.[76] However, Chinese measures don't appear to meet these conditions and could violate the right to privacy.[77] Moreover, widespread tracking has created hurdles for China's most vulnerable population, the elderly. Older people without smartphones cannot take the public bus (which requires the Health Code app) or enter public hospitals (which requires making an online appointment).[78]

Aside from privacy concerns, China also faces challenges from data sharing and linking to form accurate assessments. First, despite its long-standing efforts to overcome what it calls "data islands," data sharing remains stunted among provinces and between provincial and central authorities, as those charged with fusing data may be risk-averse.[79] Second, if data sharing happens, it may be difficult to quickly draw conclusions from different data results—let alone perform real-time analysis—on individuals from public and private sector data streams.[80] While manual contact tracing has been upheld as a better model, interviewees' vague memories and occasionally erroneous information may increase epidemiological investigators' workloads.[81]

How U.S. and Chinese Surveillance Approaches Broadly Differ

Even before the emergence of COVID-19, the U.S. and Chinese approaches to surveillance differed in fundamental ways. U.S. surveillance has been dominated by private sector commercial collection, primarily to reap profits from targeted advertising.[82] Private companies are generally expected to not share the personally identifiable information they have collected with federal, state, or local governments unless presented with appropriate court orders or other suitable legal authorizations. The collection of surveillance data by government agencies is limited by law and generally requires agencies to obtain court warrants or other similar legal instruments. The widespread introduction of video cameras (including police body cameras) complicates this landscape, but the rules and procedures are being determined through established legislative and judicial processes.

In contrast to the United States, no accountability or transparency mechanisms exist in China for the MPS to publicly report any of its surveillance activities, except to the top Chinese Communist Party (CCP) leadership.[83] Moreover, U.S. companies are more proactive about lobbying for model standards and guardrails around use of technology, while under China's National Intelligence Law, Chinese companies cannot plausibly refuse Chinese government requests to cooperate, whether the data involves users inside or outside China.[84] Companies such as Megvii have deferred to the Chinese government to write the legal framework on when and how law enforcement can use facial recognition.[85] These are just some of the contrasts between the Chinese and American approaches to surveillance, and do not fully represent the differences between other authoritarian and democratic regimes' governance approaches.

The coronavirus presents a complex challenge vis-à-vis surveillance. The International Covenant on Civil and Political Rights recognizes that in the context of serious public health threats[86] and public emergencies threatening the life of the nation, restrictions on some rights can be justified when they have a legal basis, are strictly necessary, based on scientific evidence, are neither arbitrary or discriminatory in application, of limited duration, respectful of human dignity, subject to review, and proportionate to achieve the objective.[87] However, to date, COVID-19 surveillance technologies in both countries have not adequately met these criteria and run the risk of mission creep. This is especially the case for sunset clauses, limiting data collection to public health purposes, and independent oversight.[88] Without privacy laws, widespread collection of sensitive data from citizens can proceed without consent, and the amount of data that can be shared between agencies goes unspecified.[89] However, vibrant democracies, such as South Korea, Taiwan, and New Zealand, have shown it is possible to combat coronavirus while restraining surveillance overreach. These countries have carried out programs that are limited in scope, temporary, and subject to democratic review—approaches that should serve as models going forward.[90]

Overall, AI powers surveillance in several different ways, and is used by authoritarian and democratic nations alike.[91] AI enables facial recognition, and increasingly utilizes deep learning to improve intelligent video analytics through better pattern recognition accuracy and feature classification, and lowers traditional barriers such as low lighting and poor angles. It also enables voice recognition, increasing authorities' ability to narrow the space for anonymity and to track subjects of interest. Likewise, predictive policing assists authorities by flagging persons and patterns of interest in ways that may have been missed through human-led policing. AI is also present in more nascent areas, such as automating content moderation and border security.

The following section will provide policy recommendations on how democracies can differentiate their approach to surveillance from authoritarian nations.

Policy and Messaging Recommendations

If democracies fail to model a different approach to surveillance, they will lose ground to authoritarian governments, making it increasingly difficult to

criticize abusive surveillance activities and disadvantaging democracies in the battle to sustain global rights-based governance.[92]

To ameliorate these challenges, the United States should take a two-pronged approach focused on domestic reform and multilateral efforts. First, the United States must take action to reduce human rights harms and racial injustice by its own companies and institutions at home. IBM's departure from the facial recognition market and Amazon and Microsoft's decisions to temporarily cease selling to police are commendable, but much more needs to be done, as the following technical best practices recommendations will show.[93] Second, the United States can utilize Track 1 (government-to-government) and Track 1.5 (government officials in unofficial capacity with outside experts) dialogues to work with, and learn from, other democracies on several fronts, including legal, diplomatic, and technological, also enumerated below.

Strengthen an Allied Approach

1. The State Department's Bureau of Democracy, Human Rights and Labor (DRL) can help develop a concerted interagency strategy for engaging civil society on how facial recognition and other surveillance technologies harm human rights, and which companies are responsible. With this interagency strategy in mind, DRL can host Track 1.5 dialogues modeled on State's Civil Society 2.0 and/or the Open Government Partnership. Conversants should include European and Asian country partners with legal, technical, civil society, and business expertise. The State Department can also use the information gathered from these meetings to strengthen its interagency approach.

2. In such dialogues, government and non-government stakeholders can address which surveillance technologies are and are not captured by existing privacy and surveillance legislation in each country. These dialogues can help identify role model approaches for countries to advance both domestically and as an alternate global model. The European Union's General Data Protection Regulation (GDPR), which calls for privacy by design and explicit documentation of the video surveillance's purpose, is one model.[94] The approaches taken by South Korea, Taiwan, and New Zealand can also be explored as models for public health surveillance.

3. These dialogues can also identify areas requiring more work to curb domestic human rights harms from surveillance technologies, such as the concerning tendency in many democracies to trial facial recognition systems without legal oversight or public notification, and lack of legal accountability toward U.S. police forces' use of these technologies.[95]

4. In Track 1 dialogues run by the State Department and through the newly formed Inter-Parliamentary Alliance on China (IPAC) and the Global Partnership on AI, diplomats and U.S. representatives can utilize interagency findings to advance the IPAC's goals of upholding human rights and strengthening security, and the GPAI's goals of responsible development and use of AI grounded in human rights.[96]

Identify Actors and Apply Export Controls

1. DRL should compare how its guidance for surveillance technology exports can dovetail with the European approach to surveillance export controls, and discuss where its guidance can go further by comparing it with other democracies' approaches.[97] For instance, democracies might prohibit the combination of anonymized data with other personal data, as these linkages can re-identify individuals.[98]

2. DRL can encourage countries to have their companies sign the Safe Face Pledge, which calls on organizations to make public commitments to mitigate the abuse of facial analysis technology, and similar voluntary mechanisms of compliance.[99]

3. Where possible, create a repository and examine concrete instances of Chinese and non-Chinese companies contributing to rights abuses abroad. This repository can serve as a resource for the U.S. Bureau of Industry and Security (BIS) Entity List.

4. Identify Western companies contributing core hardware to surveillance efforts and entities in authoritarian nations, and engage each company in implementing stronger export due diligence.[100] Apply lessons learned from human trafficking and financial crimes cases to induce compliance among companies.[101]

Promote Technological Best Practices and Codify Reform

The United States should engage, fund, test and legislate in the following areas:

1. U.S. representatives to the GPAI should work with the initiative's technical expertise to propose alternate facial recognition standards at the United Nations' International Telecommunications Union, where Chinese companies have been proposing standards that will be fast-tracked for approval. The Chinese standards have been criticized for promoting policy recommendations over technical specifications, which can be particularly risky, as ITU standards are often adopted by developing nations in Africa, the Middle East and Asia.[102]

2. Organizations such as the National Science Foundation and/or Defense Advanced Research Projects Agency can fund research on privacy-preserving computer vision systems—for example, methods that obscure individuals' faces.[103] They can also fund research into counter-surveillance technologies, such as clothing and other techniques that can attack image systems.[104]

3. The Department of Commerce's National Institute of Standards and Technology can test these technologies for technical robustness and accuracy in a similar endeavor to its Facial Recognition Vendor Test. NIST can also expand its past research on mitigating false negatives and false positives, especially for women and people of color.[105] These findings can directly inform congressional efforts to regulate facial recognition or alternative technologies for both government and commercial use.

4. Congress should support and promote organizations and entities that share the U.S. government's goal of countering authoritarian use of information and communications technologies.

Acknowledgments

The author would like to sincerely thank Tarun Chhabra, Jack Clark, Sheena Chestnut Greitens, Andrew Imbrie, Dewey Murdick, Helen Toner, Igor Mikolic-Torreira, and Emily Weinstein for very helpful comments and suggestions, along with Lynne Weil, Alexandra Vreeman and Daniel Hague for superb editing work.

Endnotes

[1] Dahlia Peterson, "Foreign technology and the surveillance state" in Hannas and Tatlow, eds., *China's Quest for Foreign Technology: Beyond Espionage* (Routledge, 2020).

[2] Maya Wang, "China's Dystopian Push to Revolutionize Surveillance," *The Washington Post* , August 18, 2017, https://www.washingtonpost.com/news/democracy-post/wp/2017/08/18/chinas-dystopian-push-to-revolutionize-surveillance. See also Zhou Yongkang, "加强促进社会稳定和和谐" ["Strengthen and Facilitate Social Stability and Harmony"], People's Daily, October 26, 2006.

[3] 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; Li Yuan, "Learning China's Forbidden History, So They Can Censor It," *The New York Times* , January 2, 2019, https://www.nytimes.com/2019/01/02/business/china-internet-censor.html; Samm Sacks and Paul Triolo, "Shrinking Anonymity in Chinese Cyberspace," *Lawfare* , September 25, 2017, https://www.lawfareblog.com/shrinking-anonymity-chinese-cyberspace; "China: Police DNA Database Threatens Privacy," *Human Rights Watch* , May 15, 2017, https://www.hrw.org/news/2017/05/15/china-police-dna-database-threatens-privacy; Paul Mozur, "Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras," *The New York Times* , July 8, 2018, https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html.

[4] In 2019, the China Academy of Information and Communications Technology (CAICT), a think tank under the Ministry of Industry and Information Technology (MIIT), published an AI security white paper describing how Beijing plans to use AI to automate censorship, control public opinion, and improve public security. See excerpted translation at Lisbeth, "White Paper Outlines Potential Uses of AI," *China Digital Times,* November 19, 2018, https://chinadigitaltimes.net/2018/11/white-paper-outlines-potential-uses-of-artificial-intelligence.

[5] Maya Wang, "China's Bumbling Police State," *The Wall Street Journal* , December 26, 2018, https://www.hrw.org/news/2018/12/26/chinas-bumbling-police-state.

[6] See Sheena Greitens, "Dealing with demand for China's global surveillance exports" (The Brookings Institution, April 2020), https://www.brookings.edu/research/dealing-with-demand-for-chinas-global-surveillance-exports.

[7] "中国安装了 1.76 亿个监控摄像头，这表述还在增长" ["China Has Installed 176 Million Surveillance Cameras and the Market Is Still Expanding"], Q Daily, November 21, 2017, https://web.archive.org/web/20200605002203/https://www.qdaily.com/articles/47431.html; "旷视(Face)亮相中国安防服务联盟 人脸识别打造立体安防" ["Megvii (Face++) debuts at China Security Service Alliance, face recognition creates three-

dimensional security"] *科学中国* [*Science China*], August 5, 2016, https://web.archive.org/web/20200605002338/https://www.sohu.com/a/109282144_313468.

[8] Charles Rollet, "How China's Pay By Facial Recognition Works," *IPVM*, April 2, 2019, https://ipvm.com/reports/china-pay-face.

[9] Greg Walton, "China's Golden Shield: Corporations and the Development of Surveillance Technology in the People's Republic of China," (International Centre for Human Rights and Development, 2001). This report also has an in-depth look at how Cisco played a large role in the Golden Shield overall.

[10] Xu Xu, "To Repress or To Co-opt? Authoritarian Control in the Age of Digital Surveillance," *American Journal of Political Science* 64, no. 3 (July 2020):3.

[11] "金盾工程数据库包括12亿多中国人的信息" ["The Golden Shield Project database includes information on more than 1.2 billion Chinese"], *博讯新闻* [Boxun News], April 9, 2006, https://web.archive.org/web/20160305214310/http://www.boxun.com/news/gb/china/2006/04/200604091432.shtml; "China: The Public Security Bureau (PSB) Golden Shield Project, including implementation and effectiveness; Policenet, including areas of operation; level and effectiveness of information sharing by the authorities (2010-February 2014)" (Immigration and Refugee Board of Canada, March 7, 2014), https://www.refworld.org/docid/543ba3824.html.

[12] "从源起到未来 安防企业共话"平安城市" ["From its origins to the future: Security companies discuss "Safe Cities""] *千家网* [Qianjia], May 31, 2011, https://archive.vn/CSixz.

[13] "平安城市发展历程回顾及未来发展方向展望" ["Development history of Safe Cities and prospects for future development"] *千家网* [Qianjia], March 20, 2017, https://web.archive.org/web/20200515224631/http://www.qianjia.com/html/2017-03/20_267576.html; "雪亮工程、平安城市、天网工程这三者之间有什么不同" ["The difference between Sharp Eyes, Safe Cities and Skynet"], ASMag, April 11, 2018, https://web.archive.org/web/20200515224255/http://www.asmag.com.cn/baike/arc-1691.html.

[14] "平安城市" ["Safe Cities"] 百度百科, [Baidu Encyclopedia], accessed May 5, 2020, https://baike.baidu.com/item/%E5%B9%B3%E5%AE%89%E5%9F%8E%E5%B8%82/7737245?fr=aladdin#10.

[15] Zihan Zhang, "Beijing's guardian angels?" *Global Times*, October 10, 2012, https://web.archive.org/web/20200515220239/http://www.globaltimes.cn/content/737491.shtml.

[16] “天网工程是什么？有什么作用?” [“What is Skynet and what is its purpose?”] 第一监控 [No. 1 Surveillance Blog], November 3, 2018, https://web.archive.org/web/20200515220353/https://www.sohu.com/a/272865510_609710.

[17] “天网工程规划大纲” [“Skynet project planning outline”], accessed May 15, 2020, https://wenku.baidu.com/view/dbbdcbcec850ad02de8041a4.html.

[18] Yusha Zhao, “'Sky Net' tech fast enough to scan Chinese population in one second: report,” Global Times, March 25, 2018, https://web.archive.org/web/20200515221811/http://www.globaltimes.cn/content/1095176.shtml.

[19] Yusha Zhao, “'Sky Net' tech”; Chen Shixian and Li Zhen, “‘天网’网什么” [“What does Skynet capture?”] *人民周刊* [People’s Weekly], November 20, 2017, https://web.archive.org/web/20200515220622/http://paper.people.com.cn/rmzk/html/2017-11/20/content_1825998.htm. For instance, the number of video surveillance probes in Wuhan alone has reached 1 million. See “What is Skynet and what is its purpose?”.

[20] Yusha Zhao, “'Sky Net' tech.”

[21] Harrison Jacobs, “China's 'Big Brother' surveillance technology isn't nearly as all-seeing as the government wants you to think,” Business Insider, July 15, 2018, https://www.businessinsider.com/china-facial-recognition-limitations-2018-7.

[22] Harrison Jacobs, “China's 'Big Brother'.”

[23] Other issues also include non-cooperative users, camera placement, and low/changing lighting conditions. See Eifeh Strom, “Facing challenges in face recognition: one-to-one vs. one-to-many,” ASMag, September 19, 2016, https://www.asmag.com/showpost/21158.aspx.

[24] John Honovich, “Ban of Dahua and Hikvision Is Now US Gov Law,” IPVM, August 13, 2018, https://ipvm.com/reports/ban-law.

[25] Bureau of Industry and Security, “Addition of Certain Entities to the Entity List,” Department of Commerce, October 9, 2019, https://www.federalregister.gov/documents/2019/10/09/2019-22210/addition-of-certain-entities-to-the-entity-list.

[26] Wensan Fang, “2019年中国AI＋安防行业发展研究报告” [“2019 China AI+Security Industry Development Research Report”], *安防展览网* [Security Exhibition Network], May 10, 2019, https://archive.vn/juPQi.

[27] Hikvision staff also claim this is due to their "own excellent algorithm development team and using the most powerful GPUs in our computer platforms." See William Pao, "Applying deep learning to facial recognition cameras," ASMag, February 21, 2018, https://www.asmag.com/showpost/24600.aspx.

[28] William Pao, "Applying deep learning."

[29] "全国雪亮工程建设综述" ["A Summary of Sharp Eyes Construction"], *中国安防行业网* [China Security Industry Network], October 13, 2017, https://web.archive.org/web/20200608222240/http://www.21csp.com.cn/zhanti/xlgcfx/article/article_15370.html. See text of Sharp Eyes plan at "关于加强公共安全视频监控建设联网应用工作的若干意见" ["Several Opinions on Strengthening the Construction of Public Security Video Surveillance Network Applications"], National Development and Reform Commission, May 6, 2015, https://web.archive.org/web/20190920181020/http://www.ndrc.gov.cn/zcfb/zcfbtz /201505/t20150513_691578.html.

[30] "雪亮工程" 农村安防监控建设项目 你知多少" ["How much do you know about the construction of the "Sharp Eyes" rural security monitoring project?"] *中国安防展览网* [China Security Exhibition Network], December 19, 2016, https://archive.vn/UjkDN.

[31] "安防行业迎来雪亮工程重大机遇" ["The security industry welcomes major opportunities from Sharp Eyes"], *中国安防展览网* [China Security Exhibition Network], May 23, 2018, https://web.archive.org/web/20200515224915/http://www.qianjia.com/html/2018-05/23_292907.html. See also "Several Opinions on Strengthening." It is worth noting Sharp Eyes is not only a rural project. It also has projects in major metropolises such as Guangzhou and Beijing. See Dahlia Peterson and Josh Rudolph, "Sharper Eyes: Surveilling the Surveillers (Part 1)," China Digital Times, September 9, 2019, https://chinadigitaltimes.net/2019/09/sharper-eyes-surveilling-the-surveillers-part-1.

[32] "Several Opinions on Strengthening."

[33] For more on grid management, see Sheena Chestnut Greitens, "Domestic Security in China under Xi Jinping," China Leadership Monitor, March 1, 2019, https://www.prcleader.org/greitens; "网格化管理" ["Grid Management"], Baidu Encyclopedia, accessed June 20, 2020, https://baike.baidu.com/item/%E7%BD%91%E6%A0%BC%E5%8C%96%E7%AE%A1%E7%90%86/8559115?fr=aladdin.

[34] While Sharp Eyes was not mentioned earlier this year in a key Central Committee rural planning document (as it had in 2018 and 2019), Chinese industry observers argue this does not necessarily mean Sharp Eyes is going away anytime soon. See "雪亮工程步入最后一年，建设现状如何？"["Sharp Eyes is entering its final year, what is its construction status?"], *千家网* [Qianjia], February 24, 2020,

https://web.archive.org/web/20200515233244/http://security.qianjia.com/html/2020-02/24_361216.html.

[35] The Cultural Revolution era phrase is "The people have sharp eyes." ("群众的眼睛是雪亮的.")

[36] Dahlia Peterson and Josh Rudolph, "Sharper Eyes."

[37] Dahlia Peterson and Josh Rudolph, "Sharper Eyes." The slogan was: "老百姓把遥控器握在手里，安全感落在了心里." See "社会治安防控织密"人防网"让群众参与进来越来越多"朝阳群众"守护平安不打烊" ["Prevention and control weaves 'civil defense network' to let the masses participate more in 'Chaoyang masses' style safety"], Ministry of Public Security, https://archive.vn/QWW3V.

[38] Dahlia Peterson and Josh Rudolph, "Sharper Eyes."

[39] Dahlia Peterson and Josh Rudolph, "Sharper Eyes."

[40] The National Institute of Justice has defined predictive policing as "any policing strategy or tactic that develops and uses information and advanced analysis to inform forward-thinking crime prevention." See National Institute of Justice, "Overview of Predictive Policing," Department of Justice, June 9, 2014, https://nij.ojp.gov/topics/articles/overview-predictive-policing.

[41] "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.

[42] Echo Huang, "What do China's police collect on citizens in order to predict crime? Everything," Quartz, November 20, 2017, https://qz.com/1133504/to-predict-crime-chinas-tracking-medical-histories-cafe-visits-supermarket-membership-human-rights-watch-warns; "China: Police 'Big Data.'"

[43] In Xuzhou, Jiangsu, the police even purchase data from third parties. See "China: Police 'Big Data.'"

[44] For example, the Tianjin Police Cloud, which (at the time of writing) HRW identified as the largest project at 27 million RMB, claimed it could monitor "people of certain ethnicity," "people who have extreme thoughts," "petitioners who are extremely [persistent]," and "Uyghurs from South Xinjiang." See "China: Police 'Big Data.'"

[45] "China: Police 'Big Data.'"

[46] Justin Lee, "Chinese facial recognition firm developing AI to predict crimes," Biometric Update, July 25, 2017, https://www.biometricupdate.com/201707/chinese-facial-recognition-firm-developing-ai-to-predict-crimes.

[47] "China's Algorithms of Repression" (Human Rights Watch, May 1, 2019), https://www.hrw.org/report/2019/05/02/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass.

[48] Bethany Allen-Ebrahimian, "Exposed: China's Operating Manuals for Mass Internment and Arrest by Algorithm," International Consortium of Investigative Journalists, November 24, 2019, https://www.icij.org/investigations/china-cables/exposed-chinas-operating-manuals-for-mass-internment-and-arrest-by-algorithm; "China's Algorithms of Repression"; "Minority Region Collects DNA from Millions," Human Rights Watch, December 13, 2017, https://www.hrw.org/news/2017/12/13/china-minority-region-collects-dna-millions; Darren Byler, "China's Nightmare Homestay," ChinaFile (blog) on Foreign Policy, October 26, 2018, https://foreignpolicy.com/2018/10/26/china-nightmare-homestay-xinjiang-uighur-monitor; Isobel Cockerell, "Inside China's Massive Surveillance Operation," Wired, May 9, 2019, https://www.wired.com/story/inside-chinas-massive-surveillance-operation.

[49] "How Mass Surveillance Works in Xinjiang, China," Human Rights Watch, May 2, 2019, https://www.hrw.org/video-photos/interactive/2019/05/02/china-how-mass-surveillance-works-xinjiang; Nazish Dholakia and Maya Wang, "Interview: China's 'Big Brother' App," Human Rights Watch, May 1, 2019, https://www.hrw.org/news/2019/05/01/interview-chinas-big-brother-app.

[50] "How Mass Surveillance Works."

[51] Dholakia and Wang, "Interview."

[52] Allen-Ebrahimian, "Exposed: China's Operating Manuals"; Sheena Chestnut Greitens, Myunghee Lee, and Emir Yazici, "Counterterrorism and Preventive Repression," International Security vol. 44, no. 3 (Winter 2019): 10, https://www.mitpressjournals.org/doi/pdf/10.1162/isec_a_00368; Zamira Rahim, "Prisoners in China's Xinjiang concentration camps subjected to gang rape and medical experiments, former detainee says," The Independent, October 22, 2019, https://www.independent.co.uk/news/world/asia/china-xinjiang-uighur-muslim-detention-camps-xi-jinping-persecution-a9165896.html; Allen-Ebrahimian, "Exposed: China's Operating Manuals."

[53] Arjun Kharpal, "Use of surveillance to fight coronavirus raises concerns about government power after pandemic ends," CNBC, March 26, 2020, https://www.cnbc.com/2020/03/27/coronavirus-surveillance-used-by-governments-to-fight-pandemic-privacy-concerns.html; Nectar Gan, "China is installing surveillance cameras outside people's front doors ... and sometimes inside their homes," CNN Business, April 28, 2020, https://www.cnn.com/2020/04/27/asia/cctv-cameras-china-hnk-intl/index.html; Masha Borak, "Chinese police now have AI helmets for temperature screening," Abacus

(blog) on South China Morning Post, February 28, 2020, https://www.scmp.com/tech/article/3052879/chinese-police-now-have-ai-helmets-temperature-screening; Martin Pollard, "Even mask-wearers can be ID'd, China facial recognition firm says," Reuters, March 9, 2020, https://www.reuters.com/article/us-health-coronavirus-facial-recognition/even-mask-wearers-can-be-idd-china-facial-recognition-firm-says-idUSKBN20W0WL. Massive windfalls are expected for the global facial recognition market due to COVID-19, especially for edge computing devices: from $765.7 million in 2019 to $2.287 billion by 2025. See Chris Burt, "Edge facial recognition market to near $2.3B by 2025, while biometrics as a service grows to $3B," Biometric Update, April 13, 2020, https://www.biometricupdate.com/202004/edge-facial-recognition-market-to-near-2-3b-by-2025-while-biometrics-as-a-service-grows-to-3b.

[54] For more on other countries' approaches, see Patrick Howell O'Neill, Tate Ryan-Mosley, and Bobbie Johnson, "A flood of coronavirus apps are tracking us. Now it's time to keep track of them," MIT Technology Review, May 7, 2020, https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker.

[55] "To curb covid-19, China is using its high-tech surveillance tools," The Economist, February 29, 2020, https://www.economist.com/china/2020/02/29/to-curb-covid-19-china-is-using-its-high-tech-surveillance-tools and Maya Wang, "China: Fighting COVID-19 With Automated Tyranny," The Diplomat, April 1, 2020, https://thediplomat.com/2020/03/china-fighting-covid-19-with-automated-tyranny.

[56] Wang, "China: Fighting COVID-19."

[57] If the app is green, users can go anywhere; yellow and red mean seven and 14 days of quarantine, respectively. See Wang, "China: Fighting COVID-19."

[58] Paul Mozur, Raymond Zhong, and Aaron Krolik, "In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags," The New York Times, March 1, 2020, https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html.

[59] Masha Borak, "Chinese scientist wants a new Skynet-like system just for tracking viruses," Abacus (blog) on South China Morning Post, May 22, 2020, https://www.scmp.com/tech/big-tech/article/3085543/chinese-scientist-wants-new-skynet-system-just-tracking-viruses.

[60] Wang, "China: Fighting COVID-19."

[61] 医疗健康大数据和网络研究中心 [Healthcare Big Data and Network Research Center], "数字健康技术疫情防控应用案例集（第三期)" ["Digital Health Technology Epidemic Prevention and Control Application Case Collection (Phase 3)"], 中国信息通信研究院 [China Academy of Information and Communications Technology, CAICT], March 24, 2020,

http://www.caict.ac.cn/kxyj/qwfb/ztbg/202003/P020200324369446692496.pdf. Excerpted translation available upon request.

[62] 普天设计 [Potevio], "企业抗疫行动 | 中国普天人工智能助力疫情防控" ["Corporate Anti-epidemic Action | China Potevio Artificial Intelligence Helps Epidemic Prevention and Control"], *健康界* [CN-Healthcare], March 10, 2020, https://www.cn-healthcare.com/articlewm/20200309/wap-content-1093781.html.

[63] Potevio, "Corporate Anti-epidemic Action."

[64] Tom Simonite, "How Well Can Algorithms Recognize Your Masked Face?" Wired, May 1, 2020, https://www.wired.com/story/algorithms-recognize-masked-face; In Hanvon's case, it only took a month to release to the market after the system was trained on six million masked and a smaller pool of masked faces. It works by cross-referencing images with its own database of names and other information and then identifying and tracking people's movements. It claims it can detect crime suspects, terrorists or make reports or warnings. See Pollard, "Even mask-wearers."

[65] The MPS defines seven categories of "focus personnel": petitioners, those who "undermine stability," those who are involved in terrorism, major criminals, those involved with drugs, wanted persons, and those with mental health problems who "tend to cause disturbances." See "China: Police 'Big Data.'"

[66] Legal experts believe the National People's Congress (NPC) might draft one within the next five years. In a third draft of the Personal Rights of the Civil Code published August 2019, the Standing Committee of the NPC defined privacy statutorily for the first time as "private space, private activities and private information which a natural person is unwilling to be made known to other persons, and that no organization or individual may infringe the privacy rights of other persons through spying, intrusion, leakage or public disclosure (Article 811)." See Lester Ross and Tingting Liu, "China: China's Draft Civil Code To Extend Privacy Protection," Mondaq, September 11, 2019, https://www.mondaq.com/china/privacy-protection/844146/china39s-draft-civil-code-to-extend-privacy-protection; Paul Mozur and Aaron Krolik, "A Surveillance Net Blankets China's Cities, Giving Police Vast Powers," The New York Times, December 17, 2019, https://www.nytimes.com/2019/12/17/technology/china-surveillance.html.

[67] Winston Ma Wenyan, "China is waking up to data protection and privacy. Here's why that matters," World Economic Forum, November 12, 2019, https://www.weforum.org/agenda/2019/11/china-data-privacy-laws-guideline. However, state surveillance remains off-limits to media reporting as well as activism, according to Human Rights Watch senior researcher Maya Wang.

[68] Sheena Chestnut Greitens and Julian Gewirtz, "China's Troubling Vision for the Future of Public Health," Foreign Affairs, July 10, 2020,

https://www.foreignaffairs.com/articles/china/2020-07-10/chinas-troubling-vision-future-public-health.

[69] Authorized collection stems from China's Cybersecurity Law (中华人民共和国网络安全法), the Law of the People's Republic of China on the Prevention and Control of Infectious Diseases (中华人民共和国传染病防治法), and the Regulations on Public Health Emergencies (突发公共卫生事件应急条例). See "中央网信办：做好个人信息保护利用大数据支撑联防联控工作" ["Central Cyberspace Administration: Do a good job in personal information protection and use big data to support joint prevention and control work"], *新华社*, Xinhua, February 9, 2020, https://web.archive.org/web/20200526174208/http://www.gov.cn/xinwen/2020-02/09/content_5476472.htm.

[70] Huizhong Wu, "In land of big data, China sets individual privacy rights," Reuters, May 25, 2020, https://www.reuters.com/article/us-china-parliament-lawmaking-privacy/in-land-of-big-data-china-sets-individual-privacy-rights-idUSKBN2320EF.

[71] Helen Davidson, "Chinese city plans to turn coronavirus app into permanent health tracker," The Guardian, May 26, 2020, https://www.theguardian.com/world/2020/may/26/chinese-city-plans-to-turn-coronavirus-app-into-permanent-health-tracker#maincontent; Raymond Zhong, "China's Virus Apps May Outlast the Outbreak, Stirring Privacy Fears," The New York Times, May 26, 2020, https://www.nytimes.com/2020/05/26/technology/china-coronavirus-surveillance.html.

[72] Davidson, "Chinese city plans."

[73] June Ko, "How China used technology to combat COVID-19 – and tighten its grip on citizens," Amnesty International, April 17, 2020, https://www.amnesty.org/en/latest/news/2020/04/how-china-used-technology-to-combat-covid-19-and-tighten-its-grip-on-citizens.

[74] "Mobile Location Data and Covid-19: Q&A," Human Rights Watch, May 13, 2020, https://www.hrw.org/news/2020/05/13/mobile-location-data-and-covid-19-qa.

[75] "Covid-19 Apps Pose Serious Human Rights Risks," Human Rights Watch, May 13, 2020, https://www.hrw.org/news/2020/05/13/covid-19-apps-pose-serious-human-rights-risks.

[76] Ko, "How China used technology;" "Joint statement: States use of digital surveillance technologies to fight pandemic must respect human rights," Amnesty International, April 2, 2020, https://www.amnesty.org/download/Documents/POL3020812020ENGLISH.pdf.

[77] Ko, "How China used technology."

[78] "Mobile Location Data and Covid-19."

[79] "To curb covid-19."

[80] CAICT, "Digital Health Technology."

[81] "Covid-19 Apps Pose Serious Risks"; For instance, the developers of Singapore's TraceTogether contact tracing app have warned against "an over-reliance on technology" and argue that contact tracing "should remain a human-fronted process."See Mark Zastrow, "Coronavirus contact-tracing apps: can they slow the spread of COVID-19?" Nature, May 19, 2020, https://www.nature.com/articles/d41586-020-01514-2; CAICT, "Digital Health Technology."

[82] Zastrow, "Coronavirus contact-tracing."

[83] Peterson, "Foreign technology."

[84] "中华人民共和国国家情报法" ["National Intelligence Law of the People's Republic of China"], National People's Congress of the People's Republic of China, June 12, 2018, http://www.npc.gov.cn/npc/c30834/201806/483221713dac4f31bda7f9d951108912.shtml; Ryan Tracy, "Washington State OKs Facial Recognition Law Seen as National Model," The Wall Street Journal, March 31, 2020, https://www.wsj.com/articles/washington-state-oks-facial-recognition-law-seen-as-national-model-11585686897; Murray Scot Tanner, "Beijing's New National Intelligence Law: From Defense to Offense," Lawfare, July 20, 2017, https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense; Jonathan Shieber, "Zoom admits to shutting down activist accounts at the request of the Chinese government," TechCrunch, June 11, 2020, https://techcrunch.com/2020/06/11/zoom-admits-to-shutting-down-activist-accounts-at-the-request-of-the-chinese-government.

[85] Jacobs, "China's 'Big Brother.'"

[86] "China: The Public Security Bureau (PSB) Golden Shield."

[87] "Human Rights Dimensions of COVID-19 Response," Human Rights Watch, March 19, 2020, https://www.hrw.org/news/2020/03/19/human-rights-dimensions-covid-19-response.

[88] Donahoe, "The COVID-19 Test."

[89] Justin Sherman, "The Troubling Rise of Facial Recognition Technology in Democracies," World Politics Review, April 23, 2020, https://www.worldpoliticsreview.com/articles/28707/the-troubling-rise-of-ai-facial-recognition-technology-in-democracies.

[90] Greitens and Gewirtz, "China's Troubling Vision."

[91] Over 50 percent of the world's advanced democracies use AI surveillance systems at the national or local level. See Steven Feldstein, "The Global Expansion of AI Surveillance" (Carnegie Endowment for International Peace, September 17, 2019), https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847.

[92] Donahoe, "The COVID-19 Test."

[93] Jay Peters, "IBM will no longer offer, develop, or research facial recognition technology," The Verge, June 8, 2020, https://www.theverge.com/2020/6/8/21284683/ibm-no-longer-general-purpose-facial-recognition-analysis-software; "We are implementing a one-year moratorium on police use of Rekognition," Day One (blog) on Amazon, June 10, 2020, https://blog.aboutamazon.com/policy/we-are-implementing-a-one-year-moratorium-on-police-use-of-rekognition; Jon Fingas, "Microsoft won't sell facial recognition to police without federal regulation," Engadget, June 11, 2020, https://www.engadget.com/microsoft-stops-selling-facial-recognition-to-police-184549162.html; Shira Ovide, "A Case for Banning Facial Recognition," The New York Times, June 9, 2020, https://www.nytimes.com/2020/06/09/technology/facial-recognition-software.html; Joy Buolamwini, "IBM Leads, More Should Follow: Racial Justice Requires Algorithmic Justice," Artificial Intelligence (blog) on Medium, June 9, 2020, https://medium.com/@Joy.Buolamwini/ibm-leads-more-should-follow-racial-justice-requires-algorithmic-justice-and-funding-da47e07e5b58.

[94] European Data Protection Service, The EDPS Video-Surveillance Guidelines (Brussels: EDPS Europa, 2010), 10, https://edps.europa.eu/sites/edp/files/publication/10-03-17_video-surveillance_guidelines_en.pdf; Dentons and Marc Elshof, "GDPR Update - EDPB video surveillance guidelines," JD Supra, September 3, 2019, https://www.jdsupra.com/legalnews/gdpr-update-edpb-video-surveillance-94566.

[95] Examples include New Zealand, the UK, Australia, and the United States. See Madison Reidy, "Prime minister expresses concern over facial recognition technology used by supermarkets," Stuff, May 15, 2018, https://www.stuff.co.nz/business/industries/103921136/prime-minister-expresses-concern-over-facial-recognition-technology-used-by-supermarkets; Lucy Ingham, "UK police adopting facial recognition, predictive policing without public consultation," Verdict, May 11, 2020, https://www.verdict.co.uk/uk-police-facial-recognition-predictive-policing; Asha Barbaschow, "AFP used Clearview AI facial recognition software to counter child exploitation," ZDNet, April 15, 2020, https://www.zdnet.com/article/afp-used-clearview-ai-facial-recognition-software-to-counter-child-exploitation; Jennifer Lynch, "Face Off: Law Enforcement Use of Face Recognition Technology," Electronic Frontier Foundation, February 12, 2018, https://www.eff.org/wp/law-enforcement-use-face-recognition. For discussion on historical lack of legal accountability for U.S. police, see Barry Friedman, "Law Enforcement's Facial Recognition Law-lessness: Comparing European and US Approaches,"

Just Security, March 10, 2020, https://www.justsecurity.org/69090/law-enforcements-facial-recognition-law-lessness-comparing-european-and-us-approaches.

[96] "Inter-Parliamentary Alliance on China," 2020, https://www.ipac.global; "Launch of the Global Partnership on Artificial Intelligence by 15 founding members," France Diplomacy, June 15, 2020, https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/news/article/launch-of-the-global-partnership-on-artificial-intelligence-by-15-founding.

[97] Hannah Edmonds-Camara, Seán Finan, Peter Lichtenbaum and Doron Hindin, "U.S. Draft Human Rights Guidance for Exporters of Surveillance Technology," Global Policy Watch (blog) from Covington & Burling LLP, October 2, 2019, https://www.globalpolicywatch.com/2019/10/u-s-draft-human-rights-guidance-for-exporters-of-surveillance-technology. The guidance says "Before a transaction, Exporters should consider what the Item is capable of, and how it could be used or misused by authorities. Exporters might consider integrating safety and 'privacy by design' features that enable them to track the Item's deployment and alert them to misuse, strip certain capabilities from the Item, auto-delete data and provide a kill-switch." See full text at Bureau of Democracy, Human Rights, and Labor, "Guidance on Implementing the UN Guiding Principles for Transactions Linked to Foreign Government End-Users for Products or Services With Surveillance Capabilities," U.S. Department of State, September 30, 2020, https://www.state.gov/wp-content/uploads/2020/10/DRL-Industry-Guidance-Project-FINAL-1-pager-508-1.pdf.

[98] Sara Harrison, "When Is Anonymous Not Really Anonymous?" The Markup, March 24, 2020, https://themarkup.org/ask-the-markup/2020/03/24/when-is-anonymous-not-really-anonymous. In South Korea, for instance, excessive information sharing by the government led to the identification and targeting of individuals. See "Mobile Location Data and Covid-19."

[99] Algorithmic Justice League and the Center on Technology & Privacy at Georgetown Law, "Safe Face Pledge Overview," Safe Face Pledge, December 2018, https://www.safefacepledge.org.

[100] For examples of companies involved, see Peterson, "Foreign technology."

[101] From discussion with members of the Center for a New American Security's Digital Freedom Forum, November 2019.

[102] 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.

[103] Lucas Matney, "Traces AI is building a less invasive alternative to facial recognition tracking," TechCrunch, August 15, 2019, https://techcrunch.com/2019/08/15/traces-ai-is-building-a-less-invasive-alternative-to-facial-recognition-tracking/.

[104] Kaidi Xu et al, "Adversarial T-shirt! Evading Person Detectors in A Physical World," arXiv (October 2019), https://arxiv.org/abs/1910.11099.

[105] National Institute of Standards and Technology, "NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software," U.S. Department of Commerce, December 19, 2019, https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software.