TECHNOLOGY-ENHANCED AUTHORITARIANISM

Findings

- In contravention of its signed and ratified commitment to the International Convention to End All Forms of Racial Discrimination, the People's Republic of China (PRC) has continued to facilitate the development and use of domestic standards and surveillance technologies that employ racial profiling and thus encourage discrimination on the basis of ethnicity.
- The Central Committee of the Chinese Communist Party and the State Council jointly released the "Plan for the Overall Layout of Building a Digital China," which prioritizes the digitalization of governance in China, interconnectedness and efficiency across China's digital infrastructure, and expansive control of data using next-generation technologies.
- International observers reported that PRC authorities have increased investment in next-generation data-intensive technologies, such as "smart city" projects and police geographic information systems designed to better surveil and control society.
- This past year, Party and government agencies released regulations concerning generative artificial intelligence (AI) to ensure that AI-generated content puts the PRC in a positive light, downplays criticism, and excludes content that authorities deem to be a threat to social stability.
- PRC authorities carried out digital surveillance and censorship to suppress the White Paper protests that took place throughout China in late November 2022 in opposition to harsh zero-COVID measures. Leaked directives revealed that Chinese authorities initiated the highest "emergency response" level to restrict protesters' access to virtual private networks (VPNs) and instructional materials for accessing foreign news and social media apps.
- During the reporting year, a report documented PRC authorities using advanced technology and ethnic minority online "influencers" to present a rosy picture of life in the Xinjiang Uyghur Autonomous Region in 1,741 videos spread out amoung 18 YouTube accounts with 2,000 to 205,000 followers, as part of a larger effort to deny the PRC's ongoing genocide in the region.
- Authorities implemented technological upgrades to the PRC's censorship mechanisms, together known as the Great Firewall, during the 20th National Congress of the Chinese Communist Party. Information emerged this past year about blogger **Ruan Xiaohuan,** an information security expert who provided online guidance to circumvent the Great Firewall, and who was sentenced to seven years' imprisonment for "inciting subversion of state power."

Recommendations

Members of the U.S. Congress and Administration officials are encouraged to take the following actions:

- Urge the U.S. State Department to submit an inter-state complaint to the Committee on the Elimination of Racial Discrimination (CERD) to hold PRC authorities and complicit companies accountable for the development and use of "ethnicity tracking" technology. The CERD is obligated to hear all inter-state complaints.
- Consider legislation to prohibit foreign governments from exploiting information and communications technology products that operate in the U.S. to protect citizens' data and freedom of expression.
- Consider adopting legislation to ban the social media app WeChat from federal employees' and contractors' devices. The U.S. Department of Defense, Transportation Security Administration, and several states have already banned WeChat from their employees' devices.
- Encourage the U.S. representatives to the Freedom Online Coalition and other bodies to leverage the coalition's AI and human rights expertise to support alternate facial recognition standards for surveillance, such as privacy-preserving computer vision systems that automatically censor faces and deanonymize those necessary for investigative leads.
- Urge cloud infrastructure providers to offer preferential rates to U.S. Government-funded circumvention tools, to ensure that federal funds have the maximum impact by enabling a greater number of users to circumvent the Great Firewall.
- Impose diplomatic and financial penalties on PRC officials and state media outlets that engage in bullying, intimidation, and harassment of journalists.
- In interactions with Chinese officials, call for the release of political prisoners currently detained or imprisoned for the peaceful exercise of their human rights, such as **Ruan Xiaohuan, He Binggang,** and **Zhang Yibo,** all three of whom aimed to assist Chinese citizens in circumventing PRC censorship. The records of detained individuals in the Commission's Political Prisoner Database provide a useful resource for such advocacy. Urge PRC officials, law enforcement, and security forces to end the use of arbitrary detention, disappearance, beatings, torture, and intimidation to suppress and punish individuals for the peaceful exercise of their rights.

TECHNOLOGY-ENHANCED AUTHORITARIANISM

Introduction

During the Commission's 2023 reporting year, the Chinese Communist Party and government expanded their use of technology in an attempt to control public opinion in China and internationally, and to restrict freedom of expression and freedom of movement, often in violation of international treaties. Authorities have widely deployed such technology at the expense of human rights and democratic principles and institutions.

Violations of International Commitment to Prevent Racial Discrimination

Prior to and during the reporting year, Chinese surveillance companies promoted the use of standards and the sale of surveillance equipment that has the capacity to target Uyghurs, Tibetans, and members of other ethnic minority groups by tracking people's skin color and using facial attributes as an analytical factor. Several reports published during this reporting year showed that PRC public security bureaus had contracted with Chinese surveillance technology companies Dahua, Hikvision, and Uniview to continue to develop surveillance systems that tracked protesters and ethnic and religious minorities.[1] The PRC government's use of these technologies violated its ratified commitments to the International Convention to End All Forms of Racial Discrimination (ICERD).[2] According to Committee on the Elimination of Racial Discrimination (CERD) general recommendation No. 36 on Preventing and Combating Racial Profiling by Law Enforcement Officials, "States should also ensure the adoption and periodical revision of guidelines and codes of conduct . . . in the programming, use and commercialization of algorithms that may lead to racial discrimination . . .."[3]

In 2021, IPVM, a U.S.-based company that monitors security technology, reported that Uniview, Hikvision, Dahua, and NetPosa coordinated with PRC public security authorities to write "ethnicity tracking" standards—including the use of various "personal attributes, such as skin color"—to facilitate the surveillance of Uyghurs, Tibetans, and other ethnic groups in China.[4] While official guidance reportedly only "recommended" the use of these racial and ethnic-coded standards in police surveillance work, one source indicated that Chinese public security bureaus must use the standards when conducting camera surveillance.[5] Examples of such "recommended" standards are national standards said to be produced by the Ministry of Public Security using ethnicity detection and skin color in facial recognition applications and searchable databases for video analysis systems; and another standard, issued by the Xinjiang Uyghur Autonomous Region's (XUAR) Market Supervision Administration Bureau, for "technical database requirements" for XUAR public security officials to estimate the probability that someone belongs to a particular ethnic group.[6] In October 2022, a Dahua salesperson reportedly remarked that the company used cameras with ethnicity tracking features.[7] In an August 2022 letter to the Federal Communications Commission, Dahua

stated it had "never implemented" a product to target a specific ethnic group for commercial use, but was silent as to government use.[8]

This past year, two think tanks concluded that PRC authorities provide strong commercial incentives for companies to develop surveillance technology for public security, giving them little reason not to follow the government's policy direction.[9] For example, one researcher determined that Chinese artificial intelligence (AI) companies, specifically those working on facial recognition, that received public security contracts from a city with "above median surveillance capacity," developed more software products than those that did not receive such contracts.[10] Chinese governments at different levels are some of the largest purchasers of AI surveillance products because local government officials' prospects for promotion depend, at least in part, on their track record in "maintaining social stability."[11] Researchers also found a direct relationship between social unrest and a subsequent increase in the next quarter of public security technology contracts.[12]

Expansion of Surveillance Capabilities for Social Control

This past year, authorities expanded surveillance capabilities to increase social control by promoting new data-intensive technologies. Analysts estimated that local governments and companies in Chinese cities would spend US$50 billion by the end of 2024 on "smart city" technologies, such as collecting data through smartphones, quick response (QR) code readers, point of sale machines, air quality monitors, and radio frequency identification chips used to store biometric information in identification cards.[13] The PRC's capacity to collect data was illustrated by the leak in July 2022 of the Shanghai National Police database, which contains information on 1 billion Chinese residents and several billion case records, including names, addresses, birthplaces, national ID numbers, mobile telephone numbers, ethnicity, and details of related police cases.[14] The database also included a label for "people who should be closely monitored," a reference to people whom public security authorities deem to be risks or possible threats to social stability, and whom they thus target for surveillance.[15] In May 2023, IPVM reported that Songjiang district in Shanghai municipality was designated a digitization "case study," with the goal of digitally transforming Shanghai's public security bureaus so that they are able to access a set of data modules, one of which can alert public security about foreign journalists in Shanghai who have traveled to the XUAR.[16] Another of the data modules reportedly can identify Uyghurs arriving in Shanghai and verify their addresses.[17] According to an analysis of government procurement notices published in May 2023 by China Digital Times, 30 provincial governments over a period of 17 years signed at least 803 contracts, worth 6.2 billion yuan (almost US$902 million), for police geographic information systems (PGIS).[18] PGISs are used to predict and plot unlawful activities and patterns, which in China can include anti-government protests, and other measures related to social stability.[19] As late as May 2023, Dahua marketed a surveillance system called "Jinn" that conducts grassroots-level monitoring or "social governance," and that reportedly has a feature

that can alert public security officers if a banner is unfurled in public for too long.[20]

Surveillance and Tracking of White Paper Protests Using Artificial Intelligence

Chinese authorities carried out digital surveillance and censorship to suppress individuals who participated in protests against harsh zero-COVID measures known as the White Paper protests that took place throughout China in late November 2022. Leaked directives revealed that Chinese authorities had initiated the highest "emergency response" level to restrict protesters' access to virtual private networks (VPNs) and related instructional materials for promoting access to foreign news and social media apps.[21] The Cyberspace Administration of China (CAC) issued draft rules in June 2023 to regulate the creation of ad hoc networks, using tools such as Bluetooth and Apple's AirDrop, by requiring real-name verification, and automatically defaulting them to the "off" position ten minutes after activation.[22] While Chinese authorities used AI to identify people in videos, the surveillance system struggled to capture the variety of videos that protesters uploaded.[23] Observers believe Chinese authorities used data from cell phone towers to identify and interview individuals whose phone signals were determined to be in the same area as the protests.[24] Chinese telecommunication companies are legally required to turn over certain metadata including user accounts' real ("legal") names, operating time and type, network source and destination address, network source ports, client hardware characteristics, user-released information records, and chat logs related to activity that "mobilizes" public sentiment or causes "major changes in public opinion."[25] [For information about the detention of White Paper protesters, see Chapter 1—Freedom of Expression, Chapter 2—Civil Society, and Chapter 6—Governance.]

"Digital China" Policy Developments

PRC officials continued to promote "Digital China," one of Party General Secretary Xi Jinping's long-term strategic plans, which prioritizes the digitalization of governance in China and expansive control of data.[26] In March 2023, the Party Central Committee and State Council jointly released the "Plan for the Overall Layout of Building a Digital China" (Digital China),[27] which a commentator on technology observed[28] provides "a framework for contextualizing the roles of digital infrastructure [and] the data economy."[29] The same commentator highlighted Digital China's ambitious timeframe and scale, noting that "the plan" specifies that the foundation for a Digital China should be completed by 2025 and should include building an interconnected and efficient digital infrastructure, expanding data resources, and increasing government digitalization.[30] An analysis from Bitter Winter, an online magazine that reports primarily on religious repression in China, called attention to one dimension of the Party's role in Digital China's implementation, whereby "local [Chinese] Communist Party committees" will expand internet access to every village in China while also "bringing control and surveillance" over all Chinese citizens.[31]

In an analysis of the strategic underpinnings of Digital China, experts at the Pacific Forum concluded that the Party "considers the 'control of data' to be essential to its own survival, on par with the control of media, the military, and personnel."[32] They contend that Digital China is a "grand strategy" to create the world's first data-driven governance society—which PRC officials refer to as Smart Society—the success of which is meant to demonstrate the Party's supremacy by wielding technology to better provide for Chinese citizens.[33] The March 2023 planning document on Digital China added an international development component overlapping with the Digital Silk Road, as one of the points of Digital China is to ". . . establish an international exchange and cooperation system for the digital domain . . . jointly establish a high quality 'Digital Silk Road'; and actively develop 'Silk Road e-commerce.'"[34] In March 2023, authorities created a new ministry-level national data bureau, under the State Council's National Development and Reform Commission (NDRC), per the Digital China mandate.[35] An NDRC researcher characterized the new bureau as responsible for the "management of data through its entire life cycle," saying that "processes like data generation, transmission, storage, processing and handling, circulation and trading, and development and use, will all be within the scope of the new bureau's overall planning and management responsibilities."[36] Data and technology are central to Digital China's implementation, not only in more effectively providing public goods to Chinese citizens, but also in manipulating artificial intelligence (AI) and big data for social and political control.[37]

Malign Influence and Data Sharing on TikTok and WeChat

Under PRC law, technology companies operating in China are required to share data with authorities upon request, thus infringing on users' privacy.[38] The government has passed a range of legal provisions that require technology companies' and their employees' compliance regarding state secrets and information harming national security and economic development.[39] The PRC Cybersecurity Law requires companies and individuals within China to provide technical support and assistance to public security and state security entities, which a researcher at the Hoover Institution interpreted as making networks, data, and communication available to these entities.[40]

Both TikTok and WeChat continued to collect data internationally and send it back to China, where PRC authorities could access it. Internet 2.0, a joint U.S. and Australian cybersecurity firm, published a report in July 2022 showing that TikTok had sent a large amount of data to China and concluded that it was engaging in data harvesting.[41] In May 2023, Forbes revealed that foreign content creators' tax data is stored on servers in China and is accessible by Chinese employees.[42] In December 2022, TikTok's parent company ByteDance said that two of its employees, in the course of investigating a company information leak, had improperly accessed user data, including the internet protocol (IP) addresses of two journalists that would reveal their physical location.[43] The Australian Financial Times (AFT) reported that TikTok had updated its algorithms for broadcast and moderation of livestreams,

relying on a team of engineers that included at least a dozen affiliated with ByteDance, some of whom were working in China.[44] An Australian senator told AFT that he was concerned the engineers' access to overseas data could be used to create algorithms that suppress content critical of the Party and elevate supportive content.[45]

In September 2022, Freedom House reported that in 21 of 30 assessed countries, PRC state-owned media outlets strongly influenced the direction of news content accessible to Chinese speakers, especially via the social media platform WeChat.[46] Diaspora outlets that post on WeChat must conform to WeChat's censorship requirements.[47] Since WeChat does not have an advanced search function, users view stories determined by WeChat's algorithm instead of actively searching for content that must conform with PRC provisions requiring technology companies to spread "positive energy" and not "disrupt economic and social order."[48] According to two Wall Street Journal reporters who wrote a book on digital surveillance in China, Chinese security personnel may have access to a "back-end portal" to monitor conversations and behavioral data on WeChat.[49] Authorities also have used WeChat as a tool of political repression against foreign entities and individuals.[50] This past year, Allen Shen, a candidate for the Minnesota House of Representatives, alleged that he could not post on WeChat because of his political positions about China.[51]

Increased Repression and Censorship Online

The PRC increased digital repression with targeted censorship campaigns and digital upgrades to the Great Firewall timed to the 20th National Congress of the Chinese Communist Party in October 2022. One expert expressed the belief that China's internet censorship likely had a technological upgrade with better deep packet inspection to identify and block transmitted data deemed undesirable.[52] Around the same time, the PRC blocked transport layer security (TLS) data for anti-censorship programs, and not just the ports, on a massive scale for the first time.[53]

Ruan Xiaohuan, Anonymous Blogger and Guide to Circumventing the Great Firewall, Sentenced to Seven Years in Prison

In February 2023, the Shanghai Municipal No. 2 People's Court sentenced **Ruan Xiaohuan,** an anonymous blogger with professional expertise in information security, to seven years' imprisonment, two years' deprivation of political rights, and a fine on the charge of "inciting subversion of state power."[54] Until his detention in May 2021, Ruan not only provided guidance on how to circumvent China's censorship tools to access information outside China, he also wrote about sensitive topics, such as political analysis critical of Chinese authorities, the 1989 Tiananmen protests, and the hidden wealth of Chinese officials.[55] Authorities reportedly used the registration information from an old account on Douban, a social media website, that used a similar online name and had content criticizing the government, in order to apprehend him.[56]

Increased Regulation of Generative AI for Social and Political Control

PRC agencies are regulating the technology behind generative AI, such as ChatGPT, to ensure that AI-generated content depicts China in a positive light, downplays criticism, and excludes other content that Party and government authorities deem to be threats to social stability. One analyst found that the PRC's approach to governing generative AI products is relatively "piecemeal," focused on specific usages of the technology, in contrast with, e.g., the European Union's attempt at a more comprehensive governance plan.[57] Two such regulatory efforts this past year included the following:

- In December 2022, the Cyberspace Administration of China (CAC), Ministry of Industry and Information Technology, and Ministry of Public Security jointly released new provisions on AI-generated text, images, videos, and virtual scenes.[58] The provisions are meant to "dispel rumors," prevent the dissemination of "fake news," and prohibit the use of AI content generation in "activities . . . endangering national security" or "disrupting economic and social order."[59]
- In April 2023, the CAC released draft measures requiring that generative AI technology "must not subvert state power, . . . incite separatism, . . . promote ethnic hatred, ethnic discrimination, . . . [or] promote content that may disrupt economic and social order."[60] PRC authorities frequently cite "social stability" to justify controlling online content, and these draft measures suggest officials are concerned about ChatGPT reporting on issues that authorities deem to be politically sensitive, such as the genocide in the XUAR.[61]

Manipulating International Opinion and Increased Harassment Online

This past year, the Commission observed reports of PRC authorities using advanced technology and third parties as "influencers" to present a rosy picture of life in the Xinjiang Uyghur Autonomous Region (XUAR) as part of a larger effort to deny the ongoing genocide in the XUAR. In a statement published in August 2022, the U.S. State Department concluded that the PRC had engaged in efforts to "manipulate" and "dominate" global discourse about the XUAR and to "discredit" reporting about genocide and crimes against humanity against ethnic and religious minority groups in the region.[62] In a related propaganda effort studied by researchers at the Australian Strategic Policy Institute (ASPI), multichannel corporations closely tied to the Party and government have used and in some cases produced videos of young "influencers" from among Uyghur, Kazakh, and other ethnic minority groups in China to promote propaganda on foreign media platforms.[63] The ASPI researchers analyzed 1,741 videos distributed among 18 YouTube "influencer" accounts, with an estimated 2,000 to 205,000 followers for each account.[64] The Party reportedly has paid as much as US$620,000 to online influencers and production companies for propaganda and to counter international human rights documentation.[65]

PRC authorities continued to harass and intimidate individuals who tried to report on China's human rights record or report stories that diverge from official narratives. An ASPI report concluded that the Party was "successfully silencing governments, businesses and civil society organizations globally and deterring them from criticising the CCP's [human] rights record and actions," in part by using Facebook as a tool in information operations, both to heighten PRC preferred "positive" narratives and to disseminate disinformation.[66] Freedom House reported that online harassment of journalists, especially of women of East Asian descent, had increased, and linked the increase to Chinese official media outlets naming specific journalists.[67] [For more information, see Chapter 20—Human Rights Violations in the U.S. and Globally.]

Notes to Chapter 16—Technology-Enhanced Authoritarianism

[1] Donald Maye and Charles Rollet, "Dahua Race and Skin Color Analytic Cameras," IPVM, October 17, 2022; Charles Rollet and Conor Healy, "Uniview PRC China Investigation: State Surveillance, Xinjiang/Tibet, and the CCP," IPVM, February 20, 2023; IPVM, "Hikvision Platform Set Alarms on Falun Gong, Protesters, Religion," December 29, 2022; Johana Bhuiyan, "Police in China Can Track Protests by Enabling 'Alarms' on Hikvision Software," *Guardian,* December 29, 2022.

[2] "Dahua and Hikvision Co-Author Racial and Ethnic PRC Police Standards," March 30, 2021; International Convention on the Elimination of All Forms of Racial Discrimination, adopted by U.N. General Assembly resolution 2106 (XX) of December 21, 1965, entry into force January 4, 1969. Ethnicity tracking standards are defined as using race, including skin color, to search video surveillance footage and databases. IPVM found evidence that while "ethnicity tracking" could be focused on any ethnic group, the standards are focused on Uyghurs and Tibetans.

[3] U.N. Committee on the Elimination of Racial Discrimination, General Recommendation No. 36 on Preventing and Combating Racial Profiling by Law Enforcement Officials, CERD/C/GC/36, November 24, 2020, para. 63.

[4] "Dahua and Hikvision Co-Author Racial and Ethnic PRC Police Standards," March 30, 2021; ChineseStandard.net, "Chinese Standard GB/T, GBT, GB," accessed May 31, 2023.

[5] "Dahua and Hikvision Co-Author Racial and Ethnic PRC Police Standards," March 30, 2021; ChineseStandard.net, "Chinese Standard GB/T, GBT, GB," accessed May 31, 2023.

[6] Xinjiang Uyghur Autonomous Region Market Supervision Administration Bureau, "Gong'an shipin tuxiang xinxi xinyong xitong—Di er bufen: shujuku jishu yaoqiu" [Video and image information application system for public security—Part 2: Technical requirements for database], December 15, 2018, reprinted in IPVM; "Dahua and Hikvision Co-Author Racial and Ethnic PRC Police Standards," March 30, 2021.

[7] "Dahua Racial Analytics and Human Rights Abuses—Explainer Video," IPVM, November 17, 2022.

[8] "Dahua Racial Analytics and Human Rights Abuses—Explainer Video," IPVM, November 17, 2022; Andrew D. Lipman, "Dahua Technology USA Inc. Request for Confidential Treatment of Dahua Ex Parte ET Docket No. 21–232," IPVM, August 29, 2022.

[9] Bulelani Jili, "China's Surveillance Ecosystem & the Global Spread of Its Tools," *Digital Forensic Research Lab,* Atlantic Council, October 2022, 4–5; Ilaria Massocco, "The AI-Surveillance Symbiosis in China," *Big Data China,* Center for Strategic and International Studies, July 27, 2022.

[10] Ilaria Massocco, "The AI-Surveillance Symbiosis in China," *Big Data China,* Center for Strategic and International Studies, July 27, 2022.

[11] Ilaria Massocco, "The AI-Surveillance Symbiosis in China," *Big Data China,* Center for Strategic and International Studies, July 27, 2022.

[12] Ilaria Massocco, "The AI-Surveillance Symbiosis in China," *Big Data China,* Center for Strategic and International Studies, July 27, 2022.

[13] Josh Chin and Liza Lin, *Surveillance State: Inside China's Quest to Launch a New Era of Social Control* (New York: St. Martins' Press, 2022), 126–27.

[14] Brenda Goh, Sophie Yu, Stella Qiu, Eduardo Baptista and Josh Ye, "Hacker Claims to Have Stolen 1 Bln Records of Chinese Citizens from Police," *Reuters,* July 6, 2022; Karen Hao and Rachel Liang, "China Police Database Was Left Open Online for Over a Year, Enabling Leak," *Wall Street Journal,* July 6, 2022; Zack Whittaker and Carly Page, "A Huge Data Leak of 1 Billion Records Exposes China's Vast Surveillance State," *TechCrunch,* July 7, 2022.

[15] Karen Hao and Rachel Liang, "China Police Database Was Left Open Online for Over a Year, Enabling Leak," *Wall Street Journal,* July 6, 2022; Qian Gang, "Preserving Stability," *China Media Project,* September 14, 2012.

[16] "Shanghai Police Track Uyghurs and Foreign Journalists Visiting Xinjiang," May 2, 2023; International Business Machines Corporation, "Creating a Data Module," November 4, 2021.

[17] "Shanghai Police Track Uyghurs and Foreign Journalists Visiting Xinjiang," IPVM, May 2, 2023.

[18] Arthur Kaufman and Adam Yu, "Cloud Cover: Police Geographic Information System Procurement across China, 2005–2022," *China Digital Times,* May 2023, 1–2.

[19] Arthur Kaufman and Adam Yu, "Cloud Cover: Police Geographic Information System Procurement across China, 2005–2022," *China Digital Times*, May 2023, 1–2, 4.

[20] Charles Rollet, "Dahua Selling Protestor / Banner Alarms, Deletes Evidence," IPVM, May 30, 2023; Gulchehra Hoja and RFA Investigative, "In China, AI Cameras Alert Police When a Banner Is Unfurled," *Radio Free Asia*, June 5, 2023; Samantha Hoffman and Peter Mattis, "China's Proposed 'State Security Council', Social Governance under Xi Jinping," *Asia Dialogue,* University of Nottingham Asia Research Institute, November 21, 2013.

[21] Cindy Carter, "Minitrue: Three Leaked Censorship Directives Target Anti-Lockdown Protests and Censorship-Circumvention Tools," *China Digital Times,* November 30, 2022; Helen Davidson, "China Brings in 'Emergency' Level Censorship over Zero-COVID Protests," *Guardian,* December 2, 2022; Liza Lin, "China Clamps Down on Internet as It Seeks to Stamp Out COVID Protests," *Wall Street Journal,* December 1, 2022.

[22] TechSlang, "What Is an Ad Hoc Network? A Short Definition of Ad Hoc Network," accessed June 12, 2023. Ad hoc networks, which are often called peer-to-peer networks, allow devices (such as computers and cell phones) to connect to each other without the use of internet/Wi-Fi, similar to tools such as Bluetooth and Apple's AirDrop. Alexander Boyd, "Netizen Voices: Apple Restricts AirDrop in China after Sitong Bridge Protest," *China Digital Times,* November 11, 2022. Protesters reportedly used Bluetooth and Apple's AirDrop to share content about protests or to coordinate actions, as the decentralized nature of the devices allowed them to evade Great Firewall censorship and the requirements to use one's real name and identity. Kelly Ng, "Chinese Censors Take Aim at AirDrop and Bluetooth," *BBC,* June 8, 2023; Paul Best, "Apple

Restricts AirDrop File-Sharing in China That Protesters Have Used," *Fox Business,* November 27, 2022; Cyberspace Administration of China, *Jin Juli Zizuwang Xinxi Fuwu Guanli Guiding (zhengqiu yijian gao)* [Provisions on the Management of Proximity Ad Hoc Networks (draft for public comment)], issued June 6, 2023, arts. 2, 6–8.

[23] Paul Mozur, Muyi Xiao, and John Liu, "'Breach of the Big Silence': Protests Stretch China's Censorship to Its Limits," *New York Times,* November 30, 2022; Paul Mozur, Claire Fu, and Amy Chang Chien, "How China's Police Used Phones and Faces to Track Protesters," *New York Times,* December 2, 2022.

[24] Paul Mozur, Claire Fu, and Amy Chang Chien, "How China's Police Used Phones and Faces to Track Protesters," *New York Times,* December 2, 2022; Cate Cadell and Christian Shepherd, "Tracked, Detained, Vilified: How China Throttled Anti-COVID Protests," *Washington Post,* January 5, 2023.

[25] Cate Cadell and Christian Shepherd, "Tracked, Detained, Vilified: How China Throttled Anti-COVID Protests," *Washington Post,* January 5, 2023; Cyberspace Administration of China, *Juyou Yulun Shuxing huo Shehui Dongyuan Nengli de Hulianwang Xinxi Fuwu Anquan Pinggu Guiding* [Provisions for Security Assessments of Internet Information Services with Public Opinion Attributes or Social Mobilization Capabilities], issued November 15, 2018, arts. 3, 5. For additional information on "real-name registration," see Jyh-An Lee and Ching-Yi Liu, "Real-Name Registration Rules and the Fading Digital Anonymity in China," *Washington International Law Journal* 25, no. 1 (January 1, 2016): 11–17.

[26] David Dorman and John Hemmings, "Digital China: The Strategy and Its Geopolitical Implications," *Issues and Insights,* Pacific Forum International, 23, no. 2 (February 2023): 1–3; China Cyberspace, "'Zhongguo Wangxin' zazhi fabiao 'Xi Jinping zongshuji zhiyin woguo shuzi jichu sheshi jianshe shuping'" ["China Cyberspace" magazine publishes a "Review of General Secretary Xi Jinping's Guide to the Construction of My Country's Digital Infrastructure"], reprinted in *People's Daily,* April 10, 2023; "Xi Jinping: shishi Guojia Dashuju Zhanlüe jiakuai jianshe Shuzi Zhongguo" [Xi Jinping: implement the National Big Data Strategy to accelerate the construction of Digital China], December 9, 2017.

[27] Zac Haluza, "Building a Digital China," *Root Access* (Substack), March 7, 2023; "Zhonggong Zhongyang Guowuyuan yinfa 'Shuzi Zhongguo Jianshe Zhengti Buju Guihua'" [Central Committee and State Council publish "Plan for the Overall Layout of the Construction of Digital China"], *Xinhua*, February 27, 2023.

[28] Zac Haluza, "Building a Digital China," *Root Access* (Substack), March 7, 2023; "Zhonggong Zhongyang Guowuyuan yinfa 'Shuzi Zhongguo Jianshe Zhengti Buju Guihua" [Central Committee and State Council publish "Plan for the Overall Layout of the Construction of Digital China"], *Xinhua*, February 27, 2023.

[29] Zac Haluza, "Building a Digital China," *Root Access* (Substack), March 7, 2023; "Zac Haluza," *Root Access* (Substack), accessed June 30, 2023; "'Zhonggong Zhongyang Guowuyuan yinfa 'Shuzi Zhongguo Jianshe Zhengti Buju Guihua'" [Central Committee and State Council publish "Plan for the Overall Layout of the Construction of Digital China"], *Xinhua*, February 27, 2023.

[30] Zac Haluza, "Building a Digital China," *Root Access* (Substack), March 7, 2023; "Zac Haluza," *Root Access* (Substack), accessed June 30, 2023; "'Zhonggong Zhongyang Guowuyuan yinfa 'Shuzi Zhongguo Jianshe Zhengti Buju Guihua'" [Central Committee and State Council publish "Plan for the Overall Layout of the Construction of Digital China"], *Xinhua*, February 27, 2023.

[31] Tan Liwei, "The Digital China 2023 Plan: Is There Something New?," *Bitter Winter,* March 6, 2023; "'Zhonggong Zhongyang Guowuyuan yinfa 'Shuzi Zhongguo Jianshe Zhengti Buju Guihua'" [Central Committee and State Council publish "Plan for the Overall Layout of the Construction of Digital China"], *Xinhua*, February 27, 2023.

[32] David Dorman and John Hemmings, "Digital China: The Strategy and Its Geopolitical Implications," *Issues and Insights,* Pacific Forum International, 23, no. 2 (February 2023): 1.

[33] David Dorman and John Hemmings, "Digital China: The Strategy and Its Geopolitical Implications," *Issues and Insights,* Pacific Forum International, 23, no. 2 (February 2023): 1.

[34] "Zhonggong Zhongyang Guowuyuan yinfa 'Shuzi Zhongguo Jianshe Zhengti Buju Guihua'" [Central Committee and State Council publish "Plan for the Overall Layout of the Construction of Digital China"], *Xinhua*, February 27, 2023; "Assessing China's Digital Silk Road Initiative: A Transformative Approach to Technology Financing or a Danger to Freedoms?," Council on Foreign Relations, 2020.

[35] Jian Xu, "What Does China's Newly Launched National Data Bureau Mean to China and Global Data Governance?," *Internet Policy Review,* April 25, 2023.

[36] Li Guangqian, "Wei Shuzi Zhongguo jianshe zhuru xin dongli" [Injecting new momentum in the construction of Digital China], *Legal Daily,* reprinted in *Economic Daily*, March 15, 2023; David Dorman, "The National Data Bureau's Five Toughest Battles," *Digital China Wins the Future*, March 16, 2023. See also Qin Chen, "Why Does China Want to Build a National Data Center System?," *TechNode,* May 17, 2022.

[37] David Dorman and John Hemmings, "Digital China: The Strategy and Its Geopolitical Implications," *Issues and Insights,* Pacific Forum International, 23, no. 2 (February 2023): 1; Mercator Institute for China Studies, "The CCP's Vision for Digital Transformation, with Rebecca Arcesati," May 6, 2022, 0:00–6:05; Matthew Johnson, "China's Grand Strategy for Global Data Dominance," *CGSP Occasional Papers Series,* Hoover Institution, no. 2 (April 2023): 7.

[38] U.N. Human Rights Council, The Right to Privacy in the Digital Age, Report of the U.N. High Commissioner for Human Rights, A/HRC/48/31, September 13, 2021.

[39] *Hulianwang Xinxi Fuwu Guanli Banfa* [Measures for the Management of Internet Information Services], issued September 25, 2000, amended January 8, 2011, arts. 5, 14–16; *Zhonghua Renmin Gongheguo Guojia Anquan Fa* [PRC National Security Law], passed and effective July 1, 2015, art. 77; *Zhonghua Renmin Gongheguo Guojia Qingbao Fa* [PRC National Intelligence Law], passed July 1, 2015, art. 7; *Zhonghua Renmin Gongheguo Wangluo Anquan Fa* [PRC Cy-

bersecurity Law], passed November 7, 2016, effective June 1, 2017, arts. 6, 9, 12, 28, 67–68; Matthew Johnson, "China's Grand Strategy for Global Data Dominance," *CGSP Occasional Papers Series,* Hoover Institution, no. 2 (April 2023): 32; *Zhonghua Renmin Gongheguo Mima Fa* [PRC Password Law], passed October 26, 2019, art. 26; *Guowuyuan Bangongting Guanyu Yunyong Dashuju Jiaqiang Dui Shichang Zhuti Fuwu he Jianguan de Ruogan Yijian* [Several Opinions of the General Office of the State Council Regarding Using Big Data to Strengthen Market Principle Service and Supervision], June 24, 2015; Cyberspace Administration of China, *Jishi Tongxin Gongju Gongzhong Xinxi Fuwu Fazhan Guanli Zanxing Guiding* [Interim Provisions on the Management of the Development of Instant Messaging Tools of Public Information Services], issued and effective August 7, 2014, arts. 2, 6, 8. This is a sample and not an exhaustive list.

[40] *Zhonghua Renmin Gongheguo Wangluo Anquan Fa* [PRC Cybersecurity Law], passed November 7, 2016, effective June 1, 2017, art. 28; Matthew Johnson, "China's Grand Strategy for Global Data Dominance," *CGSP Occasional Papers Series,* Hoover Institution, no. 2 (April 2023): 32.

[41] Thomas Perkins and David Robinson, "TikTok Analysis," *Internet 2.0*, July 17, 2022, 1, 13–14; "Data Harvesting vs Data Mining," *Java T point*, accessed June 6, 2023.

[42] Alexandra Levine, "TikTok Creators' Financial Info, Social Security Numbers Have Been Stored in China," *Forbes,* May 30, 2023.

[43] Salvador Rodriguez, "TikTok Parent ByteDance Says Employees Improperly Accessed User Data," *Wall Street Journal,* December 22, 2022; Glenn Thrush and Sapna Maheshwari, "Justice Dept. Investigating TikTok's Owner over Possible Spying on Journalists," *New York Times,* March 17, 2023.

[44] Max Mason, "TikTok Code Being Worked On from China Prompts Fresh Alarm," *Australian Financial Review,* June 5, 2023.

[45] Max Mason, "TikTok Code Being Worked On from China Prompts Fresh Alarm," *Australian Financial Review,* June 5, 2023.

[46] Sarah Cook, Angeli Datt, Ellie Young, and BC Han, Freedom House, "Beijing's Global Media Influence: Authoritarian Expansion and the Power of Democratic Resilience," September 2022, 8.

[47] Sarah Cook, Angeli Datt, Ellie Young, and BC Han, Freedom House, "Beijing's Global Media Influence: Authoritarian Expansion and the Power of Democratic Resilience," September 2022, 8–9.

[48] Cyberspace Administration of China, Ministry of Industry and Information Technology, Ministry of Public Security, and State Administration for Market Regulation, *Hulianwang Xinxi Fuwu Suanfa Tuijian Guanli Guiding* [Provisions on the Administration of Internet Information Service Algorithm Recommendations], issued December 31, 2021, effective March 1, 2022, art. 6; "Positive Energy," *China Media Project,* April 16, 2021. "Positive energy" in this context means content that puts the PRC in a positive light and is not critical or negative. Zeyi Yang, "The Dark Side of a Super App like WeChat," *MIT Technology Review,* October 18, 2022; Tracy Qu, "China's Algorithm Law Takes Effect to Curb Big Tech's Sway in Public Opinion," *South China Morning Post,* March 1, 2022.

[49] Josh Chin and Liza Lin, *Surveillance State: Inside China's Quest to Launch a New Era of Social Control* (New York: St. Martin's Press, 2022), 111.

[50] Seth Kaplan, "China's Censorship Reaches Globally through WeChat," *Foreign Policy,* February 28, 2023.

[51] Seth Kaplan, "China's Censorship Reaches Globally through WeChat," *Foreign Policy,* February 28, 2023.

[52] Gu Ting, "China Steps Up Social Media Censorship, 'Upgrades' Great Firewall Ahead of Congress," *Radio Free Asia,* October 17, 2022; Ericka Chickowski, "Deep Packet Inspection Explained," *AT&T Cybersecurity Blog,* AT&T Business, October 20, 2020. Deep packet inspection refers to the creation of a virtual "checkpoint" to monitor and stop specific data in transit between devices.

[53] Rita Liao and Zack Whittaker, "Popular Censorship Circumvention Tools Face Fresh Blockade by China," *TechCrunch*, October 5, 2022; Great Firewall Report, "Large Scale Blocking of TLS-Based Censorship Circumvention Tools in China," *Net4People* BBS, GitHub, October 4, 2022. TLS is an encrypted method for users to communicate with websites.

[54] Rights Defense Network, "Yishen huoxing qi nian de wangluo gongchengshi Ruan Xiaohuan (wangming Biancheng Suixiang) ershen yanqi" [Second-instance hearing of network engineer Ruan Xiaohuan (webname Program-Think), who was sentenced to seven years, has been postponed], May 21, 2023; Gao Feng, "Shanghai Court Jails Blogger for Seven Years over 'Subversive' Posts," *Radio Free Asia,* March 22, 2023; Nectar Gan, "An Influential Chinese Blogger Disappeared from the Internet. This Woman Says She Knows Why," *CNN,* March 29, 2023. For more information about Ruan Xiaohuan, see the Commission's Political Prisoner Database record 2023-00101.

[55] Rights Defense Network, "Yishen huoxing qi nian de wangluo gongchengshi Ruan Xiaohuan (wangming Biancheng Suixiang) ershen yanqi" [Second-instance hearing of network engineer Ruan Xiaohuan (webname Program-Think), who was sentenced to seven years, has been postponed], May 21, 2023; Nectar Gan, "An Influential Chinese Blogger Disappeared from the Internet. This Woman Says She Knows Why," *CNN,* March 29, 2023.

[56] Rights Defense Network, "Yishen huoxing qi nian de wangluo gongchengshi Ruan Xiaohuan (wangming Biancheng Suixiang) ershen yanqi" [Second-instance hearing of network engineer Ruan Xiaohuan (webname Program-Think), who was sentenced to seven years, has been postponed], May 21, 2023.

[57] Graham Webster, "How Will China's Generative AI Regulations Shape the Future? A DigiChina Forum," *DigiChina,* April 19, 2023; Spencer Feingold, "The EU's Artificial Intelligence Act, Explained," *World Economic Forum,* March 28, 2023. The European Union AI Act, also known as the Artificial Intelligence Act, focuses on strengthening rules around data quality,

transparency, human oversight, and accountability, and addresses ethical questions regarding the implementation of artificial intelligence in various sectors and scenarios through a risk classification system.

[58] Cyberspace Administration of China, Ministry of Industry and Information Technology, and Ministry of Public Security, *Hulianwang Xinxi Fuwu Shendu Hecheng Guanli Guiding* [Provisions on the Management of Deep Synthesis of Internet Information Services], issued December 11, 2022, effective January 10, 2023, arts. 4, 6, 11, 23; Karen Hao, "China, a Pioneer in Regulating Algorithms, Turns Its Focus to Deepfakes," *Wall Street Journal,* January 8, 2023; Afiq Fitri, "China Has Just Implemented One of the World's Strictest Laws on Deepfakes," *Tech Monitor,* January 10, 2023.

[59] Cyberspace Administration of China, Ministry of Industry and Information Technology, and Ministry of Public Security, *Hulianwang Xinxi Fuwu Shendu Hecheng Guanli Guiding* [Provisions on the Management of Deep Synthesis of Internet Information Services], issued December 11, 2022, effective January 10, 2023, arts. 4, 6, 11, 17, 23; Karen Hao, "China, a Pioneer in Regulating Algorithms, Turns Its Focus to Deepfakes," *Wall Street Journal,* January 8, 2023; Afiq Fitri, "China Has Just Implemented One of the World's Strictest Laws on Deepfakes," *Tech Monitor,* January 10, 2023; Hine Emmie and Luciano Floridi, "New Deepfake Regulations in China Are a Tool for Social Stability, but at What Cost?," *Nature Machine Intelligence* 4, no. 7 (2022): 608–10.

[60] Cyberspace Administration of China, *Guojia Hulianwang Xinxi Bangongshi Guanyu "Shengchengshi Rengong Zhineng Fuwu Guanli Banfa (Zhengqiu Yijian Gao)" Gongkai Zhengqiu Yijian de Tongzhi* [Cyberspace Administration of China Circular on Public Comment on the Administrative Measures for Generative Artificial Intelligence Services (draft for public comment)], April 11, 2023, arts. 4 (1),7.

[61] Helen Davidson, "'Political Propaganda': China Clamps Down on Access to ChatGPT," *Guardian,* February 23, 2023; China Daily (@zhongguoribo), "#ChatGPT zai shejiang wenti shang he Mei zhengfu koujing yizhi," [#ChatGPT is consistent with the US government on Xinjiang-related issues#], Weibo post, February 19, 2023, 8:00 p.m.; Hine Emmie and Luciano Floridi, "New Deepfake Regulations in China Are a Tool for Social Stability, but at What Cost?," *Nature Machine Intelligence* 4, no. 7 (2022): 608–10.

[62] U.S. Department of State, "PRC Efforts to Manipulate Global Public Opinion on Xinjiang," August 24, 2022; U.S. Department of Justice, "40 Officers of China's National Police Charged in Transnational Repression Schemes Targeting U.S. Residents," April 17, 2023.

[63] Fergus Ryan, Daria Impiombato, and Hsi-Ting Pai, "Frontier Influencers: The New Face of China's Propaganda," International Cyberpolicy Centre, Australian Strategic Policy Institute, Policy Brief 65 (October 20, 2022): 11–12, 36–42.

[64] Fergus Ryan, Daria Impiombato, and Hsi-Ting Pai, "Frontier Influencers: The New Face of China's Propaganda," International Cyberpolicy Centre, Australian Strategic Policy Institute, Policy Brief 65 (October 20, 2022): 11–12, 36–42; Daria Impiombato and Hsi-ting Pai, "How Chinese Influencers Are Dodging YouTube's Anti-Propaganda Rules," *Rest of World*, November 30, 2022; Fergus Ryan, "'Guerrilla' Influencers Are Pushing Chinese Propaganda on YouTube," *Nikkei Asia,* December 4, 2022.

[65] Max Mason, "How Beijing Uses TikTok's Sister App to Spread Propaganda," *Australian Financial Review,* December 6, 2022.

[66] Albert Zhang and Tilla Hoja, "China's Information Operations Are Silencing and Influencing Global Audiences on Xinjiang," *Strategist* (blog), Australian Strategic Policy Institute, July 20, 2022.

[67] Sarah Cook, Freedom House, "Beijing's Global Media Influence 2022: Authoritarian Expansion and the Power of Democratic Resilience," September 2022.