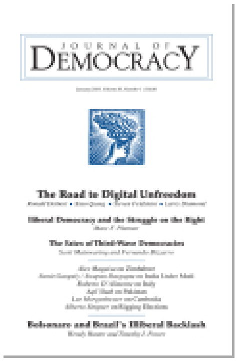
The Road to Digital Unfreedom: President Xi's Surveillance State

Xiao Qiang

Journal of Democracy, Volume 30, Number 1, January 2019, pp. 53-67 (Article)

Published by Johns Hopkins University Press
DOI: *https://doi.org/10.1353/jod.2019.0004*


JOURNAL OF DEMOCRACY

[illegible]

The Road to Digital Unfreedom
Ronald Deibert • Xiao Qiang • Steven Feldstein • Larry Diamond

Illiberal Democracy and the Struggle on the Right
Marc F. Plattner

The Fates of Third-Wave Democracies
Scott Mainwaring and Fernando Bizzarro

Alex Magaisa on Zimbabwe
Sumit Ganguly / Swapan Dasgupta on India Under Modi
Roberto D'Alimonte on Italy
Aqil Shah on Pakistan
Lee Morgenbesser on Cambodia
Alberto Simpser on Rigging Elections

Bolsonaro and Brazil's Illiberal Backlash
Wendy Hunter and Timothy J. Power

The Road to Digital Unfreedom

PRESIDENT XI'S SURVEILLANCE STATE

Xiao Qiang

Xiao Qiang *is research scientist and director of the Counter-Power Lab at the University of California–Berkeley's School of Information. He is also founder and editor-in-chief of the* China Digital Times. *Between 1991 and 2002, he served as executive director of Human Rights in China, an NGO based in New York.*

Since the internet's arrival in the People's Republic of China (PRC) in 1994, digital technologies have provided a critical channel of communication for Chinese citizens. In an environment where speech and access to information are heavily restricted, the internet has enabled citizens to get uncensored news, speak their minds, and even organize protests. Over the last two decades, the use of internet and digital technologies in the PRC has been growing rapidly. According to a mid-2018 estimate by the official China Internet Network Information Center (the body in charge of the .cn country code), there were 29.7 million first-time internet users in China in the first part of that year. Altogether, the agency reported, those using the internet in China numbered approximately eight-hundred million.[1]

Yet as the technologies that once promised to enable a free flow of information have spread, authorities have intensified their efforts to bend these systems to their own purposes. The Chinese government has set up a series of mechanisms aimed at asserting its dominance in cyberspace. It has also increasingly combined an extensive physical infrastructure of surveillance and coercion with cutting-edge digital technologies. Censorship and propaganda have gone hand in hand: Those who express unorthodox views online may become the subjects of targeted personal attacks in the state media. Surveillance and intimidation are further supplemented by outright coercion, including police visits and arrests.

China's current leader Xi Jinping, who ascended to the posts of PRC president and Chinese Communist Party (CCP) general secretary in 2012, has prioritized control over the information sphere in a bid to forestall challenges to the CCP's legitimacy. Xi has placed considerable emphasis on the concept of "internet sovereignty," asserting the primacy of rules made by national governments and the authority of national-level regulators over web content and providers. Rather than limiting themselves to playing defense against opposition activity, PRC officials have employed digital technologies to monitor and control society, especially in the era of "big data," artificial intelligence (AI), and the Internet of Things (IoT).

By leveraging information and resource asymmetries, state agencies and the companies that cooperate with them can turn these innovative technologies into tools for manipulating ordinary citizens. Big data, for instance, is an invaluable resource for making predictions. Officials can draw on this capacity to anticipate protests and even major surges in online public opinion, enabling them to act preemptively to quash opposition. In another authoritarian application of big data, PRC authorities are working to integrate information from a wide array of sources into a nationwide Social Credit System (SCS) that would assess the conduct of every person in the country, an innovation worthy of George Orwell's *Nineteen Eighty-Four*. As *Wired* magazine has put it, China's new generation of surveillance operations is indeed where "big data meets Big Brother."[2]

Internet Control in Xi Jinping's "New Era"

Under Xi Jinping, Chinese authorities have been cracking down on subversive speech on the internet while reinforcing the digital bulwark of PRC information control—the so-called Great Firewall of China—with new technology. Shortly after Xi's November 2012 accession to the post of general secretary, Chinese authorities began honing their tools for monitoring and penalizing subversive commentary on the internet. In December of that year, the Standing Committee of the National People's Congress passed regulations mandating that those wishing to use the internet via mobile phones or register social-media accounts supply their real names to internet providers. The regulations also required companies to take on a greater role in removing and reporting offending posts.[3] In September 2013, a groundbreaking ruling by the Supreme People's Court and Supreme People's Procuratorate authorized prison terms of up to three years for the posting of comments that spread rumors and are deemed to be defamatory if these posts have been reposted more than five-hundred times or viewed by five-thousand people. Jail sentences may also be imposed over posts that organize protests or incite ethnic unrest.[4] Soon after that, state media revealed that the government had hired more than two-million individuals as "microblog monitors" to report on online postings to official censors (these "monitors" do not themselves have the power to delete posts).[5]

The PRC government has also been developing new instruments for policing cyberspace more broadly. Early in 2014, the CCP formed a Central Leading Group for Cyberspace Affairs chaired by President Xi. In November 2016, the country adopted its first cybersecurity law. On 2 May 2017, the Cyberspace Administration of China (CAC) issued the first comprehensive update in twelve years to regulations requiring government licenses for all websites that distribute news—including not only traditional websites, but also messaging and other apps, blogs and microblogs, and internet forums.

The 2016 cybersecurity law places a series of demands on internet companies, with the cumulative effect of facilitating state control and data access. For instance, companies must conduct increased surveillance of their networks and supply information to state investigators on request, in addition to having their equipment reviewed for security. They are also required to censor prohibited content and to reduce user anonymity by requiring real-name registration. Service providers classed as "critical information infrastructure operators" must keep certain information (including personal data) in data centers within China's borders, and companies must undergo a security assessment if they are to transfer their data out of the country.[6]

On top of these legal and institutional innovations, Chinese authorities have stepped up their administrative efforts to keep internet providers in line. Instances of what the CAC calls "Yuetan" ("Called in for Meetings with the Authorities") have become more frequent after major internet companies Sina and NetEase were found to be in "serious violation of regulations" and were subsequently called in for meetings.[7] On 1 June 2015, the CAC released a new set of regulations that call on the agency's central and local branches to hold meetings with the responsible persons at internet news and information-service organizations following major violations. Meetings involve pointing out concerns, issuing warnings, and giving instructions for rectifying behavior. If changes are not satisfactory, the targeted company can be given further warnings, or it may face a fine or even a revocation or suspension of its business license. Before mid-2017, authorities' targets were largely online news portals; the focus has since shifted, and entertainment and video platforms, together with live broadcasts, now make up the primary subjects of Yuetan. The number of Yuetan conducted nationwide grew from 820 in 2015 and 678 in 2016 to 2,003 in 2017. In the first half of 2018, 760 of these meetings were held.

Finally, Chinese authorities continue to refine their technical countermeasures against online activity deemed a threat to their control. To limit cross-border internet connections and keep PRC residents from accessing what are viewed as dangerous sites, officials have made regular updates to the Great Firewall. This system renders tens of thousands of websites off limits to users in the PRC, in addition to serving as a tool of surveillance. A research project from the Counter-Power Lab at the University of California–Berkeley School of Information has identified the domain names of 1,382 blocked sites, which include YouTube, Google, Facebook, Flickr, Twitter, and WordPress.[8]

Early in 2017, the Ministry of Industry and Information Technology launched a sweeping effort to shut down unauthorized internet connections. This has particularly affected virtual private network (VPN) services—encrypted connections through a remote server used by some in the PRC to circumvent the Great Firewall.[9] China has made a systematic effort to disrupt VPN services since at least September 2012, when it began deploying technology that is "able to 'learn, discover and block' the encrypted communications methods used by a number of different VPN systems." Telecom giants such as China Unicom can cut connections when they identify a VPN in use. Some limited internal use of VPNs by companies is permitted, but a usage record is required. Moreover, only specially licensed vendors may supply the necessary systems.[10]

Enforcement of the restrictions on VPN usage has been tightened since the new cybersecurity law was passed in 2016. In addition to bringing about the shuttering of Chinese VPN services, this campaign appears to have proven compelling to Apple: In July 2017, the global tech giant confirmed that it would cease offering prohibited VPN apps through the version of its app store aimed at PRC users.[11]

China's intensified internet-control mechanisms are now entering the "big data" era, and they have increasingly come to intersect with the PRC's wider surveillance and information-collection infrastructure. In the past five years, both Chinese state agencies and their private-sector partners have begun exploiting their access to a wide array of systematic data about citizens.

Face, Voice, and DNA

China has been the world's fastest-growing user of surveillance cameras, a trend mainly driven by government usage. Over the past decade, technological advances have made these cameras ever more effective instruments for monitoring China's 1.4 billion people. Today, facial recognition and intelligent analysis—technology that flags objects or events of interest when these are picked up by the camera—are becoming standard features of video surveillance. The recognition of faces by cameras began to become a reality in 2010, when researchers made a breakthrough in the deep-learning algorithm used for speech and image recognition. The algorithm can also assess in real time the number and density of people in the frame, individuals' gender, and the characteristics of clothing and vehicles. Compared to other countries, China—with both a vast population and an extensive video-surveillance system—has a huge amount of face data ready for use in the machine-learning process that is used to refine facial-recognition systems. Furthermore, the government's strong interest in this area helps to ensure that the industry stays supplied with ample resources for upgrades to equipment and research algorithms.

In 2015, the PRC's National Development and Reform Commission set in motion a project by the name of "Sharp Eyes," an ambitious plan for video surveillance that builds on the "Skynet" video-surveillance program initiated in 2005. The plan calls for government bodies from local CCP committees on up to participate in creating an "omnipresent, fully networked, always working and fully controllable" system, incorporating facial-recognition technology. The goal is for this system to provide "100 percent" coverage in specified types of areas—including public spaces in residential communities—by 2020. With assistance from an associated database, officials will be able to cross-check data from cameras all over China.[12]

In 2017, it was reported on CCTV that China's "Skynet" project had been completed, bringing into being the largest video-surveillance network in the world.

In 2017, it was reported on CCTV that the "Skynet" project had been completed, bringing into being the largest video-surveillance network in the world. By that year, China's network included 176 million surveillance cameras, and there were plans to increase this number to a staggering 626 million by the decade's close. The network's many AI-equipped cameras monitor the gender, clothing, and height of passersby, transforming the information captured on screen into data.[13]

Voice-recognition software is also increasingly used around China to identify speakers in phone calls. In May 2012, the regional government of Anhui—which has been a "pilot province" in this area—and the Ministry of Public Security (MPS) launched a public-private partnership with the Anhui-based company iFlytek, China's leading supplier of speech-recognition systems. The objective was to create the "Key Laboratory of the Ministry of Public Security for Intelligent Voice Technology." As of 2015, seventy-thousand voice samples had been collected in Anhui alone. In 2017, the MPS launched pilot programs with iFlytek aimed at automatically detecting particular voices when these are picked up over the phone.[14] Chinese state media assert that voice-recognition software will be used to assist with counterterrorism efforts and "stability maintenance," and that these capabilities have already proved an asset in cases of drug trafficking, kidnapping, fraud, and blackmail.[15]

In recent years, the PRC's ever-tighter surveillance network has been strengthened by a new form of data collection: National officials, employing controversial methods, have been rapidly building up the country's DNA database. Work on this database, which is supervised by the

MPS, reportedly began in the early years of the new millennium, under the tenth five-year plan for science and technology. The Chinese government now boasts a vast DNA database synchronized with hundreds of local databases, and official documents suggest that it aims to nearly double the number of records included from the present 54 million to 100 million by 2020.[16] Combined with other forms of big data and powerful technologies such as facial recognition and AI, this database has the potential to become a formidable instrument of surveillance and repression. The PRC's massive program of DNA-data collection seriously infringes on the privacy of Chinese citizens. It also is unfair in its treatment of vulnerable groups, including ethnic minorities.

While nationwide databases assessing the financial credibility of individuals exist in many countries, social-credit systems assign citizens a comprehensive score that takes into account not only finances, but also personal behavior.

Since privacy protections and other regulations are lacking, the compulsory gathering of DNA samples extends well beyond individuals with criminal convictions. Citizens under no suspicion of criminal activity may be required to offer their DNA, particularly if they belong to groups regarded as "high-risk" or singled out for heightened surveillance. These categories include not only dissidents and members of the largely Muslim Uyghur ethnic minority, but also migrant workers and even coal miners and property tenants in a particular city. Even if these individuals have committed no crimes, they are officially viewed as possible dangers to social stability.[17]

China's western Xinjiang region, home to the Uyghurs, has effectively become "a 'frontline laboratory' for data-driven surveillance." Cameras are ubiquitous in Xinjiang, and their view extends well outside urban centers. The methods employed in this province may well foreshadow the nationwide implementation of similar "predictive-policing tactics" in the months to come.[18] Xinjiang is also the place in which DNA-collection efforts have taken their most extreme form.

As of September 2016, those applying for passports in Xinjiang had to provide a blood sample for DNA testing, along with other forms of biometric data (fingerprints, a voice recording, and a 3-D image of themselves).[19] More recently, authorities have begun using obligatory health checks to obtain residents' DNA and other identifying information. According to guidelines issued in 2017, the PRC government has now mandated that DNA samples be collected from all Xinjiang residents between the ages of 12 and 65, as well as from individuals seen as particular dangers to stability (known as "focus personnel") and their family members, even if outside this age range. The guidelines detail the proper methods to be used and the authorities responsible for biometric-data collection, which is carried out either in the home or at the closest of a number of central stations. Once collected, biometric data is bundled with an individual's *hukou,* a form of household registration. Notably, the requirement to submit to biometric-information collection extends to individuals registered in Xinjiang but who reside elsewhere in mainland China.[20] As anthropologist Darren Byler told the *Diplomat,* the data obtained will be "correlated to ethnicity, employment, gender, age, foreign travel history, household registration, individual and family criminal history, and religious practice."[21]

Social Credit

In 2014, China's State Council announced an ambitious plan made possible by new digital technology: a nationwide Social Credit System that "covers the entire society." This project would involve tracking the activities and offering assessments of people as well as enterprises. By the target date of 2020, the Council anticipated an entry on each PRC citizen. This information was to be drawn from private as well as from public sources, although the entries that had been added to the relevant platform as of mid-2017 came chiefly from government sources: More than thirty bureaucratic bodies had collectively supplied four-hundred datasets. Officials are to be able to search this system by biometric indicators, including fingerprints. Meanwhile, China's government in 2015 authorized a number of private actors—including Alibaba, China's Amazon—to begin work on social-credit platforms of their own.[22]

While nationwide databases assessing the financial credibility of individuals exist in many countries, social-credit systems assign citizens a comprehensive score that takes into account not only finances, but also personal behavior. For instance, the system operated by Alibaba collects data on individuals' personal circles of friends, their shopping habits, and even the remarks they make on social media. Social-credit scores can determine the results of applications for personal loans, jobs, visas, and more.[23] A Chinese government document outlining plans for the SCS over the period 2014–20 calls for promoting "the widespread use of unified social-credit codes in economic and social activities."[24]

In a state distinguished by its pervasive efforts at monitoring and surveillance, the quantity of data that may eventually be incorporated into the SCS is vast. We have already mentioned the government's growing activities in the areas of video surveillance and DNA collection. Chinese citizens are also regularly photographed and fingerprinted, and personal information is collected when they engage in basic activities such as shopping, traveling on airplanes, or even entering some public places. This surveillance encompasses both in-person and online behavior: The "real-name" system that China has gradually implemented (under the official slogan "Strengthening the construction of network integrity, cultivating the concept of legally operating the internet and using the network with integrity") will ensure that online activity is open to official scrutiny. Internet companies and regular users alike have their behavior assessed in order to produce a credit rating, and these assessments will serve as the basis for a blacklisting of "enterprises and individuals with serious online dishonesty behaviors."[25] The SCS may also come to incorporate existing blacklists—maintained by websites per official requirements—of internet users whose comments are found to contain "illegal" remarks.[26]

Through the SCS, Chinese authorities can bundle with a citizen's national ID code information about matters ranging from tax payments, personal finances, and business registrations to traffic violations and more. Once credit information is linked to documents establishing the personal status of citizens, such as household registrations and ID cards, state authorities as well as the cooperating companies operating social-credit systems can quietly guide and influence behavior. Individuals with good credit records can be rewarded, and those with bad ones may face negative consequences. For example, citizens with unpaid taxes, debts, or traffic fines can be kept from purchasing certain kinds of transportation tickets and rejected when applying for bank loans or credit cards. Measures of this kind have already been put into effect: By mid-2018, due to poor social-credit scores, more than 11 million people had reportedly been placed under limits on the purchase of airline tickets, and 4.25 million people were restricted in buying high-speed rail tickets.[27] For those whose political activity draws negative official attention, this system is likely to have serious repercussions. The experiences of individuals currently on social-credit blacklists suggest that those subject to restrictions may not be notified when listed, and will not have easy access to appeal procedures.

In China's one-party dictatorship, there is no independent rule of law, nor are there checks on the government's power. This means that many of the restraints on the handling of personal data that are present in democratic societies do not apply. Under the new cybersecurity law and other security legislation, authorities can freely access nearly all personal information.[28] Once fully operative, the SCS—premised on a massive invasion of citizens' privacy through large-scale monitoring—will provide the state with a range of new mechanisms by which it can exert control over China's people.

During China's ongoing wave of digitalization, the country's tech giants have frequently shown "willingness to share users' personal data with the state as part of a tacit bargain that allows them to expand with minimal regulatory interference."[29] On 21 October 2016, Alibaba Group chairman Jack Ma told the Central Politics and Law Committee, a top security body, that "the future legal and security system cannot be separated from the internet and big data." His remarks, which emphasized crime-fighting, offered support for the vast surveillance project on which PRC authorities have embarked.[30] Regulation and other levers give officials considerable influence on corporate decision making in China, and their presence may soon take a more tangible form: A draft document disseminated in 2016 proposed that the government purchase a 1 percent stake in large tech companies and be entitled to representation on their boards. Such an arrangement would amplify the CCP's voice at the companies to which multitudes of PRC consumers turn for services ranging from online shopping to transportation.[31]

"Internet Sovereignty" and the "China Model"

With the PRC striving to build world-leading industries in AI, big-data analytics, and other emerging fields, high-tech companies that have already been working closely with the government on censorship and surveillance, including Alibaba, Baidu (China's Google), and Tencent (owner of the widely used messaging and payments app WeChat), are on their way to providing key applications and services worldwide. There are now fifteen countries in which WeChat has begun offering its payment services. In November 2017, Malaysia became the first foreign jurisdiction with access to the platform's full functionality after Malaysian authorities granted a license that permits WeChat payments through the nation's banks. WeChat has also become a player in democracies such as Australia, where its payments branch has formed partnerships with local operators of cross-border payment services. Customers in more than ten-thousand Australian restaurants and stores also have the option of paying through WeChat.[32]

The rapid global expansion of Chinese high-tech companies and their products warrants vigilance for several reasons. First, when users traveling outside the PRC continue to rely on Chinese applications such as WeChat, the applications' built-in content restrictions travel with them. Second, these platforms can double as tools for information collection. The University of Toronto–based Citizen Lab, for instance, has revealed a number of surveillance mechanisms embedded in Chinese social-media platforms.[33] In early December 2017, Indian authorities reportedly instructed armed-service members to avoid 42 apps, including WeChat, on the grounds that "a number of Android/IOS apps developed by Chinese developers or having Chinese links are reportedly either spyware or other malicious ware."[34] This is particular cause for concern since the Chinese government has a dark history of using its high-tech exports for espionage activities. Such activities are part of a broader pattern of high-tech spying: On 11 December 2017, Germany's intelligence agency accused China of harvesting the personal information of German officials through the career-networking site LinkedIn.[35] Finally, researchers and advocates are rightfully concerned by the prospect that the Chinese government will export its censorship and surveillance technologies, as well as the social-credit system that they have enabled, to other authoritarian governments.

While Chinese people embrace the convenience brought by a new generation of digital technology, China's rulers are turning their information, habits, and desires into powerful levers of control.

In July 2016, President Xi Jinping began promoting the concept of the "China model for a better social governance system." The "China model," in this case, is nothing but a more appealing term for a comprehensive system of state repression, bolstered by the latest digital technologies and coupled with limited openness in the economic sphere. But the CCP is increasingly self-confident due to its economic success and increased control over society.

One telling example of the China model's influence is that the Wuzhen World Internet Congress, held from 3–5 December 2017, attracted CEOs from leading global tech companies such as Apple, Google, and Cisco Systems. Their presence suggests that these companies are offering their tacit blessing to the China model of managing cyberspace. At the Wuzhen meeting, Wang Huning, member of the Standing Committee of the Political Bureau of the CCP Central Committee, emphasized "cyber sovereignty" and called on participants not only to "encourage innovation and entrepreneurship" but also, among other points, to "stimulate security cooperation" and "build a good order."[36] Also at Wuzhen, Apple CEO Tim Cook observed that his company's app store has helped 1.8 million software developers in China to earn collectively US$17 billion in revenue, taking the lead among their peers; Cook failed to mention that more than six-hundred VPN applications had been removed from the app store's Chinese version in 2017.[37]

In the past several years, Facebook CEO Mark Zuckerberg has made several high-profile overtures to Beijing. In December 2014, Zuckerberg hosted "internet czar" Lu Wei, then head of the Cyberspace Administration of China, at Facebook headquarters. During the televised visit, Facebook's billionaire founder deliberately displayed an English version of President Xi Jinping's book on his desk. Zuckerberg also met with Xi on 25 September 2015 and asked Xi to choose a Chinese name for his soon-to-be-born daughter. In 2016, the *New York Times* revealed that Facebook had secretly been at work on software capable of ensuring that users in particular regions—for instance, within China—will not come across certain posts in their news feeds. Facebook clearly undertook this project in order to meet PRC requirements for online censorship.[38]

Facebook is not alone in its effort to enter the blocked China market. In August 2018, the *Intercept* revealed that Google has been preparing a special version of its search service for use in China. This secret initiative, named "Project Dragonfly," produced an Android app apparently designed to enable Google's return to China by satisfying official demands, including the blocking of search results and even search terms related to such topics as free speech, protests, democracy, human rights, and religion. Since Google's project would draw a connection between searches made and individual phone numbers, there are concerns that it would facilitate state surveillance.[39]

If Facebook and Google indeed enter or re-enter the China market, they will be two perfect examples of the Chinese state's success in promoting "internet sovereignty." The 2016 cybersecurity law, which mandates that internet-service operators must store user data and communication content within China, came into effect in June 2017. Apple has already taken action to comply, first declaring its intention to make China's Guizhou Province the site of an Apple cloud-computing center and then apprising users that a Chinese partner company would be taking over iCloud services in mainland China.[40] Combined with requirements to submit to official security assessments and cooperate with official surveillance of "crime," these mandates for local storage of data would give the government unfettered access to search histories and other personal information regularly acquired by global tech companies. The concessions these companies make might end up endangering those whose searches or messaging contain sensitive content.

While Chinese people embrace the convenience brought by a new generation of digital technology, China's rulers are turning their information, habits, and desires into powerful levers of control. By consolidating vast quantities of data from state agencies, with assistance from such companies as Alibaba, Baidu, and Tencent, PRC authorities are well on their way to constructing the world's largest "dataveillance" infrastructure under the flag of the China model. If the trend toward accommodation of PRC censorship and surveillance requirements continues, global tech companies may soon be making their own contributions to this authoritarian edifice.

Digital Totalitarianism

In July 2017, China's State Council released a policy plan for attaining global leadership in AI. The PRC aspires to achieve primacy in this cutting-edge field by 2030, investing enough to develop an AI sector worth roughly $150 billion. The State Council document envisions AI "playing an irreplaceable role in effectively maintaining social stability."[41] It anticipates the use of these capabilities not only in such areas as education, healthcare, or environmental protection, but also in the field of state security, where relevant applications include internet censorship and analyzing surveillance-camera footage to trace people's movements. As we have noted, AI might also be used to predict protests. Investing in this technology is thus a means for China's ruling party to firm up its grip on power.[42]

In February 2018, Xi Jinping orchestrated the elimination from China's constitution of the two-term limit for the presidency. The addition of digital technology to the apparatus of centralized authoritarianism may well enable Xi to realize his aspiration of holding onto China's highest office indefinitely.

In Xi Jinping's "Brave New China," it has become increasingly clear that the digitalization of Chinese society is amplifying the state's capacity to monitor and control the country's 1.4 billion people. As PRC authorities augment their formidable collection of high-tech instruments for surveillance and control, they are increasingly cultivating the "ability to persistently link people's identities and activities." This is the constant thread running through not only the SCS, but also mandatory real-name registration for internet users; the collection of face, voice, and DNA data; and the ID checks now required in order to perform everyday activities such as mailing a package or getting on a bus.[43] A new generation of digital technology, including AI, will empower the state to identify and quash opposition in advance by combining clues from its many channels of mass information collection. In short, China is well on its way to building the world's first "responsive tyranny," perhaps even a "digital totalitarian state."[44] Although this may be a dream come true for a dictator hoping to exert maximum control over his society, it is a nightmare for Chinese citizens and for those all over the world who value human freedom.

NOTES

1. Jon Russell, "China Reaches 800 Million Internet Users," *TechCrunch*, 21 August 2018, *https://techcrunch.com/2018/08/21/china-reaches-800-million-internet-users.*

2. Rachel Botsman, "Big Data Meets Big Brother as China Moves to Rate Its Citizens," *Wired,* 21 October 2017, *www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion.*

3. Keith Bradsher, "China Toughens Its Restrictions on Use of the Internet," *New York Times,* 28 December 2012.

4. Keith Zhai, "Up to Three Years in Prison for Chinese Internet Users Who Spread Rumours," *South China Morning Post,* 10 September 2013; "China Issues New Internet Rules That Include Jail Time," BBC, 9 September 2013, *www.bbc.com/news/world-asia-china-23990674.*

5. "China Employs Two Million Microblog Monitors State Media Say," BBC, 4 October 2013, *www.bbc.com/news/world-asia-china-24396957.*

6. Sue-Lin Wong and Michael Martina, “China Adopts Cyber Security Law in Face of Overseas Opposition,” Reuters, 6 November 2016, *www.reuters.com/article/us-china-parliament-cyber/china-adopts-cyber-security-law-in-face-of-overseas-opposition-idUSKBN132049*.

7. “Youzhong: Wangxinban yuetan shilu” [Daring: The Cyberspace Administration of China’s interview records], *China Digital Times,* 10 August 2018, *https://chinadigitaltimes.net/chinese/2018/08/%E6%9C%89%E7%A8%AE%E4%B8%A8%E7%BD%91%E4%BF%A1%E5%8A%9E%E7%BA%A6%E8%B0%88%E5%AE%9E%E5%BD%95*.

8. *Information Controls, Global Media Influence, and Cyber Warfare Strategy: Hearing Before the U.S.-China Economic and Security Review Commission,* 115th Cong. (2017) (statement of Xiao Qiang), *www.uscc.gov/sites/default/files/transcripts/May%20Final%20Transcript.pdf*; Simon Denyer, “China’s Scary Lesson to the World: Censoring the Internet Works,” *Washington Post*, 23 May 2016.

9. Sijia Jiang, “China Cracks Down on Unauthorized Internet Connections,” Reuters, 23 January 2017, *www.reuters.com/article/us-china-internet/china-cracks-down-on-unauthorized-internet-connections-idUSKBN15715U*.

10. Charles Arthur, “China Tightens ‘Great Firewall’ Internet Control with New Technology,” *Guardian,* 14 December 2012; Leo Zhao and Lulu Xia, “China’s Cybersecurity Law: An Introduction for Foreign Businesspeople,” *China Briefing,* 1 March 2018, *www.china-briefing.com/news/2018/03/01/chinas-cybersecurity-law-an-introduction-for-foreign-businesspeople.html*.

11. “China’s Great Firewall Gets Tougher as Popular VPN Shut Down,” Bloomberg*,* 3 July 2017, *www.bloomberg.com/news/articles/2017-07-03/china-s-great-firewall-gets-tougher-as-popular-vpn-shut-down*; Cate Cadell, “Apple Says It Is Removing VPN Services from China App Store,” Reuters, 29 July 2017, *www.reuters.com/article/us-china-apple-vpn/apple-says-it-is-removing-vpn-services-from-china-app-store-idUSKBN1AE0BQ*; Zhao and Xia, “China’s Cybersecurity Law.”

12. Charles Rollet, “China Public Video Surveillance Guide: From Skynet to Sharp Eyes,” *IPVM,* 14 June 2018, *https://ipvm.com/reports/sharpeyes*.

13. “Zhongguo tianwang jiankong bei you huo qinhai geren yinsi” [China’s Skynet surveillance system raises worries over the possibility of violations of personal privacy], Voice of America, 26 September 2017, *www.voachinese.com/a/news-china-builds-largest-camera-minitoring-system-20170926/4044624.html*; Frank Hersey, “China to Have 626 Million Surveillance Cameras Within 3 Years,” *Technode,* 22 November 2017, *https://technode.com/2017/11/22/china-to-have-626-million-surveillance-cameras-within-3-years*.

14. “China: Voice Biometric Collection Threatens Privacy,” Human Rights Watch, 22 October 2017, *www.hrw.org/news/2017/10/22/china-voice-biometric-collection-threatens-privacy*.

15. Joseph Hincks, “China Is Creating a Database of Its Citizens’ Voices to Boost Its Surveillance Capability: Report,” *TIME,* 23 October 2017.

16. Li Sheng, “Guanyu xia yidai DNA shujuku goujian de sikao” [Thinking about the construction of the next generation DNA database], *Xingshi jishu* 38, no. 1 (2013): 49–51; Wenxin Fan, Natasha Khan, and Liza Lin, “China Snares Innocent and Guilty Alike to Build World’s Biggest DNA Database,” *Wall Street Journal,* 26 December 2017.

17. Fan, Khan, and Lin, “China Snares”; “Privacy Concerns as China Expands DNA Database,” BBC, 17 May 2017, *www.bbc.com/news/world-asia-china-39945220*; “China: Police DNA Database Threatens Privacy,” Human Rights Watch, 15 May 2017, *www.hrw.org/news/2017/05/15/china-police-dna-database-threatens-privacy*.

[18] Megha Rajagopalan, "This Is What a 21st-Century Police State Really Looks Like," *BuzzFeed,* 17 October 2017, *www.buzzfeed.com/meghara/the-police-state-of-the-future-is-already-here?utm_term=.qdqyWxPXgb#.kq33ogJWqN*; Josh Chin and Clément Bürge, "Twelve Days in Xinjiang: How China's Surveillance State Overwhelms Daily Life," *Wall Street Journal,* 19 December 2017.

[19] "China: Passports Arbitrarily Recalled in Xinjiang," Human Rights Watch, 21 November 2016, *www.hrw.org/news/2016/11/21/china-passports-arbitrarily-recalled-xinjiang.*

[20] "China: Minority Region Collects DNA from Millions," Human Rights Watch, 13 December 2017, *www.hrw.org/news/2017/12/13/china-minority-region-collects-dna-millions*; James Griffiths, "China Collecting DNA, Biometrics from Millions in Xinjiang: Report," CNN, 12 December 2017, *www.cnn.com/2017/12/12/asia/china-xinjiang-dna/index.html.*

[21] Mercy A. Kuo, "Uyghur Biodata Collection in China," 28 December 2017, *https://thediplomat.com/2017/12/uyghur-biodata-collection-in-china.*

[22] Mirjam Meissner, "China's Social Credit System," *China Monitor* (Mercator Institute for China Studies), 24 May 2017, *https://www.merics.org/sites/default/files/2017-09/China%20Monitor_39_SOCS_EN.pdf,* 6; Mara Hvistendahl, "Inside China's Vast New Experiment in Social Ranking," *Wired,* 14 December 2017, *www.wired.com/story/age-of-social-credit.*

[23] Cojo, "Sesame Credit: The Dark Side of Gamification," *Artifice,* 2 January 2016, *https://the-artifice.com/sesame-credit-gamification.*

[24] "Shehui xinyong tixi jianshe guihua gangyao (2014–2020 nian) renwu fengong" [Outline of the division of tasks for the Social Credit System construction plan (2014–2020)], *http://www.ndrc.gov.cn/gzdt/201501/W020150105530734502125.pdf.*

[25] "Shehui xinyong tixi jianshe guihua gangyao (2014–2020 nian) renwu fengong."

[26] Martin Chorzempa, Paul Triolo, and Samm Sacks, "China's Social Credit System: A Mark of Progress or a Threat to Privacy?" Peterson Institute for International Economics, June 2018, *https://piie.com/system/files/documents/pb18-14.pdf.*

[27] Harry Cockburn, "China Blacklists Millions of People from Booking Flights as 'Social Credit' System Introduced," *Independent,* 22 November 2018, *https://www.independent.co.uk/news/world/asia/china-social-credit-system-flight-booking-blacklisted-beijing-points-a8646316.html.*

[28] "Big Data, Meet Big Brother: China Invents the Digital Totalitarian State," *Economist,* 17 December 2016.

[29] Anminda, "How Tech Firms Partner with Beijing to Shame Citizens," *China Digital Times,* 17 October 2017.

[30] "Alibaba's Jack Ma Urges China to Use Data to Combat Crime," Bloomberg, 23 October 2016, *www.bloomberg.com/news/articles/2016-10-24/alibaba-s-jack-ma-urges-china-to-use-online-data-to-fight-crime.*

[31] Li Yuan, "Beijing Pushes for a Direct Hand in China's Big Tech Firms," *Wall Street Journal,* 11 October 2017.

[32] Meg Jing Zeng, "Thinking of Taking Up WeChat? Here's What You Need to Know," *The Conversation,* 17 December 2017, *https://theconversation.com/thinking-of-taking-up-wechat-heres-what-you-need-to-know-88787.*

33. Lotus Ruan et al., "One App, Two Systems—How WeChat Uses One Censorship Policy in China and Another Internationally," Citizen Lab, 30 November 2016, *https://citizenlab.ca/2016/11/wechat-china-censorship-one-app-two-systems*.

34. "Government Reportedly Lists 42 Chinese Apps as Dangerous, Including True-Caller, UC Browser, Mi Store: Check If Your Phone Has Any of Them," *Financial Express* (Noida, India), 1 December 2017.

35. Joseph Hincks, "Germany's Intelligence Agency Says China Used Fake LinkedIn Profiles to Spy on Officials," *TIME*, 11 December 2017.

36. Graham Webster et al., "Wang Huning's Speech at the 4th World Internet Conference in Wuzhen," New America, *DigiChina* blog, 13 December 2017, *www.newamerica.org/cybersecurity-initiative/digichina/blog/wang-hunings-speech-4th-world-internet-conference-wuzhen*.

37. "Apple's Tim Cook Says Developers Have Earned $17 Billion from China App Store," Reuters, 2 December 2017, *www.reuters.com/article/us-apple-china/apples-tim-cook-says-developers-have-earned-17-billion-from-china-app-store-idUSKBN1DX04J*.

38. "Zuckerberg Hosts Chinese Internet Regulator, 'Buys Xi Jinping's Book' for Facebook Staff," *South China Morning Post,* 9 December 2014; Charlotte Middlehurst, "Chinese President Snubs Mark Zuckerberg's Request for Baby Name," *Telegraph,* 4 October 2015; Mike Isaac, "Facebook Said to Create Censorship Tool to Get Back into China," *New York Times,* 22 November 2016.

39. Ryan Gallagher, "Google China Prototype Links Searches to Phone Numbers," *Intercept,* 14 September 2018, *https://theintercept.com/2018/09/14/google-china-prototype-links-searches-to-phone-numbers*; Samuel Wade, "Activists Ask Google: What's Changed Since 2010?" *China Digital Times,* 30 August 2018; Samuel Wade, "New iPhones, Google Plans Could Track Chinese Users," *China Digital Times,* 14 September 2018.

40. Zhao and Xia, "China's Cybersecurity Law."

41. Christina Larson, "China's Massive Investment in Artificial Intelligence Has an Insidious Downside," *Science,* 8 February 2018.

42. Paul Mozur, "Beijing Wants A.I. to Be Made in China by 2030," *New York Times*, 20 July 2017.

43. Wade, "New iPhones."

44. "Reinventing Liberalism for the 21st Century," *Economist,* 13 September 2018; "Digital Totalitarian State," *Economist*.