The Road to Digital Unfreedom: How Artificial Intelligence is Reshaping Repression

Steven Feldstein

Journal of Democracy, Volume 30, Number 1, January 2019, pp. 40-52 (Article)

Published by Johns Hopkins University Press
DOI: *https://doi.org/10.1353/jod.2019.0003*

The Road to Digital Unfreedom

HOW ARTIFICIAL INTELLIGENCE IS RESHAPING REPRESSION

Steven Feldstein

Steven Feldstein *is associate professor and Frank and Bethine Church Chair of Public Affairs at Boise State University and a nonresident fellow in the Democracy, Conflict, and Governance Program at the Carnegie Endowment. From 2014 to 2017, he was deputy assistant secretary in the U.S. Department of State's Bureau of Democracy, Human Rights, and Labor.*

In early 2018, one of Malaysia's key security forces made a startling announcement. The Auxiliary Force, a branch of the Royal Malaysia Police Cooperative, had entered into a partnership with the Chinese company Yitu Technology to equip the Force's officers with facial-recognition capabilities. Security officials will be able to rapidly compare images caught by live body cameras with images from a central database. The head of the Auxiliary Force explained that this use of artificial intelligence (AI) was a "significant step forward" in efforts to improve public security. He also noted that his agency planned eventually to enhance the body-camera system so as to enable "real-time facial recognition and instant alerts to the presence of persons of interest from criminal watch lists."[1]

Neighboring Singapore soon followed suit, declaring its plans to launch a pilot camera-installation project with the end goal of embedding facial-recognition technology on every public lamppost. The project is ostensibly aimed at facilitating "crowd analytics" and assisting with antiterror operations. Privacy advocates such as the Electronic Frontier Foundation have warned that this technology will enable governments to target political opponents and suppress free expression, but their protests have been to no avail.[2]

Meanwhile in April 2018, AI startup CloudWalk Technology, based in the Chinese city of the Guangzhou, reportedly signed a deal with Zimbabwe's government to provide facial-recognition technology for use by state-security services and to build a national image database. CloudWalk is also known for supplying facial-recognition and identity-verification technology to police forces in China's Xinjiang region,

Journal of Democracy Volume 30, Number 1 January 2019

one of the most heavily repressed regions in the world. Its new African partnership falls under the umbrella of the multicontinental Chinese infrastructure and investment scheme known as the Belt and Road Initiative (BRI).[3] CloudWalk's offerings threaten to exacerbate political repression in Zimbabwe, where authorities recently carried out a violent postelection crackdown.

These are not isolated examples. Around the world, AI systems are showing their potential for abetting repressive regimes and upending the relationship between citizen and state, thereby accelerating a global resurgence of authoritarianism. The People's Republic of China (PRC) is driving the proliferation of AI technology to authoritarian and illiberal regimes, an approach that has become a key component of Chinese geopolitical strategy.

The concept of AI has proven resistant to exact definition. One widespread assertion is that the goal of AI is to "make machines intelligent," a concept often explained with reference to human intelligence.[4] Others, such as Jerry Kaplan, question the usefulness of such analogies. Kaplan maintains that whether machines are "self-aware as people are" is irrelevant. Instead, the essence of AI can be boiled down to a computer's "ability to make appropriate generalizations in a timely fashion based on limited data."[5]

This article does not seek to resolve these disputes. Rather, it focuses on the practical effects of new technologies that are coming into circulation thanks to three major developments: 1) the increased availability of big data from public and private sources; 2) enhanced machine learning and algorithmic approaches; and 3) correspondingly advanced computer processing. (Machine learning, which can be applied to tasks that range from winning Go matches to identifying pathogens, is an iterative statistical process in which an AI system is introduced to a set of data and "tries to derive a rule or procedure that explains the data or can predict future data."[6]) The import of this technology for the world's authoritarians and their democratic opponents alike is growing ever clearer. In recent years, autocracies have achieved new levels of control and manipulation by applying advanced computing systems to the vast quantities of unstructured data now available online and from live video feeds and other sources of monitoring and surveillance. From facial-recognition technologies that cross-check real-time images against massive databases to algorithms that crawl social media for signs of opposition activity, these innovations are a game-changer for authoritarian efforts to shape discourse and crush opposition voices.

AI is not the only category of new technology increasingly being harnessed by autocrats for political gain. Other communications and information technologies, frequently used in tandem with AI, are having equally alarming effects. These include advanced biometrics, state-based cyber hacking, and information-distortion techniques. This article highlights the repressive impact of AI technology for two reasons. First, AI provides a

higher-order capability that integrates and enhances the functions of other technologies in startling new ways. Second, mainstream understanding of the policy impact of AI technology remains limited; policy makers have yet to seriously grapple with AI's repressive implications.

Why AI Is a Boon to Authoritarian Leaders

Although AI has significant potential as a tool for governments everywhere, it offers a number of particular benefits to authoritarian and illiberal regimes. Despite the wide variety of nondemocratic regime types—ranging from single-party dictatorships to hybrid or semiauthoritarian regimes to military dictatorships and personalist autocracies—most of these governments maintain power through a mixture of coercion (threatening and intimidating would-be rivals) and cooptation (bribing or otherwise inducing political actors to join the ruling coalition).

A leader who opts to repress must rely on state-security forces to apply the necessary coercive measures. This brings two attendant problems. First, such repression is labor-intensive and expensive; over time, it requires an increasing amount of resources to sustain. Second, it leads to a principal-agent problem: "the very resources that enable the regime's repressive agents to suppress its opposition also empower them to act against the regime itself."[7] In other words, as a regime increasingly relies on police or soldiers to do its dirty work, it also grows more vulnerable to pressure or even insurrection from those same quarters. Leaders face a fraught choice as to whether the benefits of deploying security forces to crush challenges from without outweigh the potential threat that these forces themselves pose from within.

This is where the advantages of AI technology become apparent. Instead of relying on a dense security-force infrastructure to enable widespread surveillance, harassment, and intimidation of opponents across the state's territory, authoritarian leaders can use AI to cultivate a digital repression capability at a lower cost—and reduce principal-agent concerns.[8] In fact, the most advanced surveillance operations rely on relatively few human agents: Many functions are instead automated through AI. Moreover, in comparison to human operatives with limited reserves of time and attention, AI systems can cast a much wider net. Because of this omnipresence, they can induce changes in behavior and create a significant "chilling effect" even in the absence of sustained physical violence. If citizens know that AI "bots" are monitoring all communications and that algorithms will pick up dissenting messages and report them to the authorities, the public has a powerful motivation to conform. Such is the elegant simplicity of AI repression: It requires considerably fewer human actors than conventional repression, entails less physical harassment, and comes at a lower cost.[9] Yet it may well have a more wide-ranging and systematic impact.

Even before the onset of digital repression, the landscape of contemporary authoritarianism was shifting in noteworthy ways. First, the erosion of democratic institutions and norms has accelerated worldwide. The Varieties of Democracy (V-Dem) 2018 report estimates that around 2.5 billion people now live in countries affected by this "global autocratization trend."[10] In fact, gradual democratic backsliding has become one of the most common routes to authoritarianism.

Second, the manner in which autocrats exit power is also changing. From 1946 to 1988, coups were the most common way for autocrats to leave office, with such events accounting for 48.6 percent of authoritarian exits. But in the post–Cold War era, instances of change from factors external to the regime have overtaken coups. From 1989 to 2017, the most common causes of departure for dictators were popular revolt and electoral defeat. Exits through coups have plummeted, making up only 13 percent of total exits (in fact, leadership exits due to civil war slightly exceeded exits from coups in this period).[11]

This indicates that the gravest threats to authoritarian survival today may be coming not from insider-led rebellions, but from discontented publics on the streets or at the ballot box. The implication for dictators who want to stay in power is clear: redirect resources to keep popular civic movements under control and do a better job of rigging elections. In these areas, AI technology provides a crucial advantage. Rather than relying on security forces to repress their citizenry—with all the resource costs and political risk that this entails—autocratic leaders are embracing digital tactics for monitoring, surveilling, and harassing civil society movements and for distorting elections. A look at three possible scenarios will help to clarify the relevance of AI to some of the most pressing challenges facing contemporary authoritarians.

Scenario 1: Keeping tabs on popular discontent and controlling mass protest. In the first scenario, an incumbent one-party regime faces rising discontent over economic stagnation and political suppression. Spontaneous protests have taken place intermittently over the past year, worrying the political leadership. The regime wants to take assertive steps to forestall mass political mobilization, but its limited resources mean that it cannot afford to rely on mass arrests and imprisonment. It also fears that overt repression of this kind could trigger a popular backlash. Therefore, it has settled on a two-part strategy: 1) identify, monitor, and selectively detain opposition leaders and potential key followers; and 2) closely monitor crowd formations that could turn into mass rallies while keeping security forces on standby to break up protests before they reach scale.

To carry out this strategy, the regime first needs to identify dissident leaders and key followers who are likely to mobilize. It starts with an extensive survey of social-media services and personal communications. Be-

cause certain chat groups rely on privacy settings or encryption to prevent government snooping, authorities may reach out to international malware firms such as FinFisher or NSO Group, which peddle software designed to penetrate these closed groups. Alternatively, the regime could choose a cheaper option and procure the services of an international "hacker-for-hire" or a second-string malware vendor for this task.[12] This survey of online data helps the regime to discern patterns, identify individuals of interest, and home in on relevant conversations. As the surveillance operation builds profiles of political activists and maps civic and opposition networks, it feeds this information into an AI algorithm, which then sifts through multiple datasets using pattern-recognition software to identify individuals with tendencies toward political dissent. The algorithm also helps the regime to monitor issues that are provoking popular dissatisfaction, and it looks out for communications indicating imminent protest. Armed with this information, the regime carries out targeted detentions and preventive arrests to forestall mass disruptions.

If protests do start despite these efforts, AI can help the regime to contain them. One technology already made available by the popular Chinese communications platform WeChat produces "heat maps" that show crowd density and measure foot traffic in specific locations.[13] The regime can embed tracking technology in similar chat platforms, enabling it to know instantaneously when crowds start to form. Alternatively, it can install facial-recognition systems in urban public spaces (along the lines of Singapore's lamppost proposal). AI systems with access to these cameras can monitor crowd density, search for individuals carrying political signage, and keep tabs on the whereabouts of persons of interest. Finally, AI enhances the state's ability to deploy selective censorship and online disinformation to sow confusion and undercut potential protests. This can take the form of denial-of-service attacks against protest campaigns (undercutting the ability of opponents to organize and effectively censoring vital information) or of bot-driven information-distortion campaigns (producing a flurry of misleading posts to blur opponents' messaging and overwhelm information channels with noise).

Scenario 2: Keeping a restive province in check. In this example, an authoritarian regime grapples with potential instability in an outlying province where an ethnic minority makes up the bulk of the population. The regime's legitimacy in this province is historically tenuous, and the region periodically goes through bouts of unrest. Recently, the central government has decided to curb political turbulence through heavy-handed repression that combines traditional tactics with new technology. This scenario closely hews to the current state of affairs in Xinjiang region, and the PRC's ongoing efforts to quell dissent in the region sharply illuminate the vast repressive potential of AI used in conjunction with older coercive tactics.

First, the Chinese government is making widespread use of conventional physical repression. Authorities have set up a sprawling network of reeducation camps believed to house a million or more Muslim detainees, chiefly members of the Uyghur ethnic minority. This represents a sizeable portion of Xinjiang's roughly 21 million people. These work camps involve relentless indoctrination, including self-criticism and the repetition of phrases ("we will oppose extremism, we will oppose separatism, we will oppose terrorism"). Detainees are held in locked rooms in wrenching conditions and face draconian discipline.[14]

Second, PRC authorities are supplementing severe physical coercion with a broader approach that relies on advanced technology. They are implementing "grid-style social management," which entails dividing communities into "geometric zones so that security staff can systematically observe all activities with the aid of new technologies."[15] The state has established police stations every few hundred feet in targeted districts, staffed by tens of thousands of security agents. Moreover, Chinese authorities are equipping this force with advanced surveillance capabilities and systems that can perform big-data analytics.

In particular, the Chinese are building a predictive-policing program that aggregates and analyzes multiple streams of data in order to identify potential threats. Human Rights Watch has reported on the creation by Xinjiang authorities of an "Integrated Joint Operations Platform" (IJOP), which collects information from sources including closed-circuit TV cameras (often equipped with facial-recognition software) and "wifi sniffers" that gather identifying addresses from laptops and smartphones. IJOP gets additional information from license plates and ID cards examined at checkpoints, as well as from health, banking, and legal records.[16] While the degree of integration between IJOP and other PRC data-collection efforts is unknown, it is noteworthy that Chinese authorities are increasingly deploying handheld scanning devices to break into smartphones and extract contacts, social-media communications, emails, photos, and videos. In addition, the PRC recently created a mandatory DNA database with the goal of obtaining samples from all Xinjiang residents aged 12 to 65.[17]

Once the relevant information is fed into IJOP computers, algorithms sift through reams of data looking for patterns that could signify threatening behavior. It is unclear what confidence thresholds Chinese authorities are using to run these tests, but the algorithms are probably generating significant numbers of false matches due to system errors. Once the machine flags an individual, that person may be picked up by security forces and detained for an indefinite period.

Developing this system has not been cheap. The sum budgeted by Xinjiang authorities for "security-related investment projects" reportedly rose from just US$27 million in 2015 to more than $1 billion in the first quarter of 2017.[18] Yet this is a low figure compared to the amount

the state would have to spend to build a comparable system of surveillance and repression without using AI technology.

Scenario 3: Using disinformation to delegitimize opponents. In the third scenario, an autocratic regime is organizing national elections required by its constitution. It plans to engage in the usual election rigging, ballot-stuffing, and voter suppression, but it is also seeking out new strategies that will help to fully guarantee a victory over the opposition. AI technology can assist in several ways, particularly on the disinformation front.

First, AI can manipulate available information and push out key regime messages. For example, social-media platforms use content-curation algorithms to drive users toward certain articles—and keep them addicted to their social-media feeds. State authorities can exploit such algorithms to push out proregime messaging using bot and troll armies for hire. AI can help to identify key social-media "influencers," whom the authorities can then coopt into spreading disinformation. Emerging AI technology can also facilitate the deployment via social-media platforms of automated, hyperpersonalized disinformation campaigns—targeted at specific individuals or groups—much along the lines of Russian influence efforts in the 2016 U.S. election or Saudi troll armies targeting dissidents such as the slain journalist Jamal Khashoggi. In recent years, there has been a growing trend of political actors spreading disinformation by these and other means in order to energize supporters or disorient opponents.

Second, AI technology is increasingly able to produce realistic video and audio forgeries. One new technique whose disinformation potential especially worries policy makers is the use of generative adversarial networks, which pits competing AI systems against each another.[19] Essentially, the first machine generates forgeries that the second machine tries to uncover. The feedback from the second system then helps the first system to design increasingly realistic examples. Ultimately, this can result in sophisticated forgeries that even advanced AI systems may be unable to detect. For authoritarian leaders, deep-fake technology offers a means of discrediting would-be challengers, who may become the subjects of doctored videos that falsely depict them making inflammatory remarks or engaging in vile acts.

Key Policy Challenges

The proliferation of AI technology and the rise of digital repression pose serious policy challenges to liberal democracies. A key question is whether powerful AI tools will cause these democracies themselves to become more repressive. In particular, will the temptation to take advantage of AI's surveillance potential ultimately corrode democratic safeguards?

History suggests that citizens should be wary. In 1975, shocking al-

legations of U.S. intelligence-community misconduct prompted the U.S. Senate to authorize the establishment of what came to be known as the Church Committee. The CIA was reportedly running assassination attempts against foreign leaders, and other agencies had set up expansive domestic-surveillance networks to monitor and harass civil rights activists, political protesters, and Native American organizations.[20] In its final report, the Church Committee warned: "Too often, constitutional principles were subordinated to a pragmatic course of permitting desired ends to dictate and justify improper means."[21] Despite a long tradition in the United States of protecting individual rights and placing checks on governmental authority, the potential for state overreach remained vast.

As AI proves its repressive value for the autocracies now pioneering new technologies, copycat behavior by other governments is likely to follow.

Intentional abuse by state-security agencies is not the only civil-liberties issue accompanying the rise of AI. Implicit bias and reinforced discrimination in algorithms are also causes for concern. AI learning used in policing or healthcare, for example, can reinforce inequality and produce or perpetuate discriminatory practices. One notorious example of implicit bias was a 2015 incident in which Google's photo-indexing system described pictures of African Americans as "gorillas." The major culprit was the "training data" used to "teach" the algorithm to identify faces, which skewed predominantly toward Caucasian faces. It likely did not help that only 2 percent of Google's "professional" workforce is African American, which may have prevented the team from recognizing this issue sooner.[22] Subsequent research has shown that human prejudice has a profound effect on the workings of AI systems. A 2017 article in *Science* documented how machine-learning programs acquire biases from textual data: The tested program came to associate family-related descriptions such as "parents" with female names, whereas it linked male names with terms such as "professional."[23]

The criminal-justice sector has been an early adopter of AI-based predictive analysis, but studies reveal that the programs involved frequently rely on biased data. For instance, crime statistics indicate that African Americans are far likelier to be arrested by the police than Caucasian counterparts. But machine algorithms rarely consider that police bias may be the reason for disproportionate African American arrests. Instead, the default algorithmic assumption is that African Americans are more prone to commit crimes. This dubious conclusion forms the basis for the subsequent predictions produced by these algorithms, underscoring a vital principle: AI machines are only as good as the data with which they are trained.

In 2018, it is not difficult to imagine liberal-democratic governments ex-

ploiting AI technology in ways that infringe on citizens' rights. Fortunately, citizens in advanced democracies have successfully combatted government surveillance abuses in the past, and robust checks and balances exist that can push back against state overreach. While there is no guarantee that AI will not weaken democratic political systems, the risk there is less acute.

The danger is much greater for fragile democracies or countries with authoritarian tendencies. In backsliding regimes such as Poland, Hungary, or the Philippines, the repressive potential of AI may lead to even steeper deterioration. Illiberal governments that face prospective popular challenges have a natural interest in technology that could help them to weather mass discontent. Even in political systems that are ostensibly democratic, governments have a high incentive to arm security forces with intrusive technology, monitor the activities of political opponents and civil society, and take preemptive action against potential challenges to their authority. States also closely track one another's actions. As AI proves its repressive value for the autocracies now pioneering new technologies, copycat behavior by other governments is likely to follow.

The United States and China lead the world in AI technology, but they offer vastly different visions for its use. For China, AI is an essential component of the broader system of control that underpins Communist Party rule. Moreover, supplying new AI capabilities to bolster fellow authoritarians serves to further the regime's grand strategic aims, particularly "undermining the Western liberal order while reaching for PRC hegemony in Asia and the expansion of Chinese influence worldwide."[24]

Consequently, the Chinese are both aggressively working to develop new AI capabilities and vigorously peddling their new products abroad. Of the three central components of AI—training data for machine learning, computing power, and strong algorithms—China has training data in abundance and its algorithms are improving, but its industrial chip capacity lags far behind that of the United States. In contrast, the United States possesses the world's most advanced microchips, and its algorithms also lead the world in sophistication and complexity. But the United States is increasingly trailing China in terms of the digital data available to AI companies. This matters because data increasingly "make all the difference" when it comes to building AI-driven companies that can outperform competitors.[25] Under the flagship initiative "Made in China 2025," the PRC is seeking to transform its chip-manufacturing capacity through investment and intellectual-property theft in order to dominate a core set of high-tech industries. Experts caution that this campaign signals an aspiration "not so much to join the ranks of hi-tech economies like Germany, the United States, South Korea, and Japan, as much as replace them altogether."[26] The rapid advance of the AI startup Yitu is emblematic of China's push.

Yitu was founded by two Chinese AI experts in 2012, and in only six years it has passed several remarkable milestones. Its "Dragonfly Eye"

image platform already contains more than 1.8 billion photographs, and Yitu claims that the system requires only three seconds to identify an individual within its database. This dataset includes images from the PRC's national database, as well as an estimated 320 million entry and exit photos taken at the country's borders. Yitu's value reached an estimated $2.4 billion in 2018, and the company now employs more than five-hundred people spread across Shanghai, Singapore, and Silicon Valley. Most importantly, its algorithms work: Yitu's facial-recognition technologies have won top awards from the U.S. National Institute of Standards and Technology and the U.S. intelligence community's Intelligence Advanced Research Projects Activity (IARPA) program.

As China develops a robust AI sector, it is using the BRI to spread this sophisticated technology to governments worldwide. Illustrative projects range from constructing a network of "safe cities" in Pakistan (such cities feature extensive monitoring technology built directly into the infrastructure) to providing Argentine authorities with AI and facial-recognition software that will enhance public surveillance. The PRC shrewdly assumes that the more it can bring other countries' models of governance into line with China's own, the less those countries pose a threat to Chinese hegemony. Furthermore, as governments become dependent on advanced Chinese technology to control their populations, they will feel increasing pressure to align their policies with the PRC's strategic interests. In fact, China's AI strategy is blunt about the technology's perceived benefits: "It [AI] will become a new impetus for advancing supply-side structural reforms, a new opportunity for rejuvenating the real economy, and a new engine for building China into both a manufacturing and cyber superpower."[27]

Policy Responses

In the years ahead, AI will have a major impact on global politics. While no single unified policy response can adequately address an issue so complex and multifaceted, there are several important implications for democratic states.

In general, advanced democracies should more explicitly recognize how big a threat AI technology poses to open political systems. China's efforts to build sophisticated AI capabilities, along with its proliferation of such technology to other authoritarian regimes, present serious long-term risks. Western policy makers should afford a much higher priority to opposing these efforts, both externally and at home.

The misuse of AI technology is not limited to authoritarian regimes. As democratic governments acquire new technologies that dramatically increase their monitoring and surveillance capabilities, they need to determine acceptable limits to the use of these technologies. Democracies must look inward and take the lead in developing domestic regulatory

frameworks. Such a process will be messy; technological innovation often leapfrogs the ability of regulators to devise reasonable standards and guidelines. Nonetheless, advanced democracies are in the best position to consider how to regulate private companies and prevent abuses.

Domestic efforts should complement international action to create clearer frameworks for AI use. Initiatives such as the UN Guiding Principles on Business and Human Rights offer a useful template. Working out international guidelines on AI technology will require a multistakeholder process that is inclusive in nature; flexible enough to reflect new technological advances; and resistant to capture by China or other authoritarian governments. A much more extensive normative discussion is also needed. The international community has yet to tackle scores of issues related to algorithmic bias, implicit discrimination, and privacy.

Finally, democracies should consider ways to strengthen the capacity of civil society to withstand AI-fueled repression and to participate in shaping guidelines for AI use. Local civil society organizations (CSOs) operating in repressive environments will require more resources, training, and technological support. Many such groups have migrated online, but they are failing to use widely available digital-security tools, such as encryption services. As a result, they face significant risks of cyber hacking, intrusion, monitoring, and surveillance. For CSOs operating in democracies, the big challenge is to comprehensively monitor proposed regulations, spotlight violations stemming from the misuse of AI, and assume an overall watchdog role. Investigations such as ProPublica's uncovering of algorithmic implicit bias in the U.S. criminal-justice system are making an appreciable difference in how governments use AI technology. As more and more governments adopt AI platforms, there will be an increasing demand for such work. Internationally, it is vital that civil society stakeholders have a strong voice in conversations about how to properly regulate AI.

AI technology is "dual-use": It can be deployed for beneficial purposes as well as exploited for military and repressive ends. But this technology cannot be neatly separated into "beneficial" and "harmful" buckets. The functions that gain value from automation can just as easily be used by authoritarians for malicious purposes as by democratic or commercial actors for beneficial ones. To help ensure that AI is used responsibly, enhancing the connections linking the policy community to engineers and researchers will be key. In other words, those responsible for designing, programming, and implementing AI systems also should share responsibility for applying and upholding human-rights standards. Policy experts should be in regular, open dialogue with engineers and technologists so that all sides are aware of potential misuses of AI and can develop appropriate responses at an early stage.

The world's autocracies, with China in the lead, are increasingly demonstrating the dangers that lie at the intersection of cutting-edge AI

technology, broader innovations in the information and communications spheres, and authoritarian projects of coercion and control. To counter not only the spread of high-tech repression abroad, but also potential abuses within their own borders, policy makers in democratic states must think seriously about how to mitigate harm and to shape better practices. From Pakistan to Zimbabwe, a dangerous authoritarian vision of the future of AI is taking shape. The time has come for democratic actors to mount a serious response.

NOTES

1. Li Tao, "Malaysian Police Wear Chinese Start-Up's AI Camera to Identify Suspected Criminals," *South China Morning Post,* 20 April 2018.

2. Aradhana Aravindan and John Geddie, "Singapore to Test Facial Recognition on Lampposts, Stoking Privacy Fears," *Reuters*, 13 April 2018.

3. Amy Hawkins, "Beijing's Big Brother Tech Needs African Faces," *Foreign Policy*, 24 July 2018.

4. Nils J. Nilsson, *The Quest for Artificial Intelligence: A History of Ideas and Achievements* (Cambridge: Cambridge University Press, 2010).

5. Jerry Kaplan, *Artificial Intelligence: What Everyone Needs to Know* (New York: Oxford University Press, 2016), 5–6.

6. Executive Office of the President, National Science and Technology Council, Committee on Technology,"Preparing for the Future of Artificial Intelligence," October 2016, *https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf,* 8.

7. Milan W. Svolik, *The Politics of Authoritarian Rule* (Cambridge: Cambridge University Press, 2012), 124.

8. Lucan A. Way and Steven Levitsky, "The Dynamics of Autocratic Coercion After the Cold War," *Communist and Post-Communist Studies* 39 (September 2006): 387–410.

9. In comparison, for example, East Germany's Stasi security service relied upon an informant network equivalent to 1 percent of the country's total population leading to sizeable and persistent economic costs. See Andreas Lichter, Max Löffler, and Sebastian Siegloch, "The Long-Term Costs of Government Surveillance: Insights from Stasi Spying in East Germany," SOEPpapers on Multidisciplinary Panel Data Research No. 865, Deutsches Institut für Wirtschaftsforschung, Berlin, 2016, *www.econstor.eu/bitstream/10419/146890/1/869045423.pdf.*

10. V-Dem Institute, *Democracy for All? V-Dem Annual Democracy Report 2018,* 2018, *www.v-dem.net/en/news/democracy-all-v-dem-annual-democracy-report-2018,* 19. See also Erica Frantz and Andrea Kendall-Taylor, "The Evolution of Autocracy: Why Authoritarianism Is Becoming More Formidable," *Survival* 59 (October–November 2017): 57–68.

11. The statistics and classification system used to make these determinations are based on data for 1946 to 2010 from Barbara Geddes, Joseph Wright, and Erica Frantz, "Autocratic Breakdown and Regime Transitions: A New Data Set," *Perspectives on Politics* 12 (June 2014): 313–31. Data for the period 2010–17 has been updated by the author with assistance from Erica Frantz.

12. Collin Anderson, "The Hollowing Middle of the Surveillance Malware Market," *Motherboard,* 14 December 2017, *https://motherboard.vice.com/en_us/article/595dkd/the-hollowing-middle-of-the-surveillance-malware-market*.

13. Josh Horwitz, "WeChat's New Heat Map Feature Lets Users—and Chinese Authorities—See Where Crowds Are Forming," *Quartz,* 7 October 2015, *https://qz.com/518908/wechats-new-heat-map-feature-lets-users-and-chinese-authorities-see-where-crowds-are-forming*.

14. Gerry Shih, "China's Mass Indoctrination Camps Evoke Cultural Revolution," AP, 18 May 2018.

15. Adrian Zenz and James Leibold, "Chen Quanguo: The Strongman Behind Beijing's Securitization Strategy in Tibet and Xinjiang," Jamestown Foundation, *China Brief,* 21 September 2017.

16. Human Rights Watch, "China: Big Data Fuels Crackdown in Minority Region," 26 February 2018, *www.hrw.org/news/2018/02/26/china-big-data-fuels-crackdown-minority-region.*

17. Cate Cadell, "From Laboratory in Far West, China's Surveillance State Spreads Quietly," Reuters, 14 August 2018; Human Rights Watch, "China: Minority Region Collects DNA from Millions," 13 December 2017, *www.hrw.org/news/2017/12/13/china-minority-region-collects-dna-millions*.

18. Josh Chin and Clément Bürge, "Twelve Days in Xinjiang: How China's Surveillance State Overwhelms Daily Life," *Wall Street Journal,* 19 December 2017.

19. Will Knight, "The US Military Is Funding an Effort to Catch Deepfakes and Other AI Trickery," *MIT Technology Review*, 23 May 2018.

20. See LeRoy Ashby and Rod Gramer, *Fighting the Odds: The Life of Senator Frank Church* (Pullman, Wash.: Washington State University Press, 1994), 478.

21. *Intelligence Activities and the Rights of Americans: Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities, United States Senate,* Book II (Washington, D.C.: U.S. Government Printing Office, 1976), *www.intelligence.senate.gov/sites/default/files/94755_II.pdf,* III.

22. Wendy Lee, "How Tech's Lack of Diversity Leads to Racist Software," *SFGATE,* 22 July 2015.

23. Princeton University, Engineering School, "Biased Bots: Human Prejudices Sneak into Artificial Intelligence Systems," *ScienceDaily*, 13 April 2017.

24. Minxin Pei, "China in Xi's 'New Era': A Play for Global Leadership," *Journal of Democracy* 29 (April 2018): 38.

25. Kai-Fu Lee, *AI Superpowers: China, Silicon Valley, and the New World Order* (New York: Houghton Mifflin Harcourt, 2018), 56.

26. Lorand Laskai, "Why Does Everyone Hate Made in China 2025?" Council on Foreign Relations*, Net Politics,* 28 March 2018, *www.cfr.org/blog/why-does-everyone-hate-made-china-2025*.

27. Paul Triolo, Elsa Kania, and Graham Webster, "Translation: Chinese Government Outlines AI Ambitions Through 2020," New America, *DigiChina,* 26 January 2018, *www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinese-government-outlines-ai-ambitions-through-2020*.