PRINCETON UNIVERSITY

jpia JOURNAL OF PUBLIC & INTERNATIONAL AFFAIRS

The Social Credit System: Not Just Another Chinese Idiosyncrasy

By **Eunsun Cho**

Abstract

As the unparalleled ability of big data to capture and process real-time information signals a revolution in public administration, countries around the world have begun to explore the application of the technology to government functions. At the forefront of these efforts is China, which is planning to launch the social credit system (SCS), a data-powered project to monitor, assess, and shape the behavior of all citizens and enterprises. This new frontier of digital surveillance raises questions about how the United States will incorporate data technology into its own politics and economy. This article argues that the U.S. needs a comprehensive nationwide data protection framework that places limits on surveillance by both private business and the government. Without drawing its own baseline for personal data protection, the United States risks missing the already narrowing opportunity to define its balance between democracy, security, and growth.

Introduction

In his widely celebrated book *Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed*, James C. Scott argues that states' blinded attempts to rationalize and simplify society lay at the heart of many mass-scale tragedies in the modern era. Although science and technology have been the drivers of modernization, the valorization of the scientific organization and standardization of human and natural life, coupled with weak civil society and authoritarianism, often unleashed a destructive force that resulted in humanitarian and ecological crises (Scott 1998).

His stern warning from the end of the 20th century about what he calls the "high-modernist" tendency of modern statecraft is no less relevant today in the age of big data. Big data's unparalleled ability to capture and process real-time information brings boundless business opportunities, but also signals a revolution in public administration. Countries around the world have begun to explore the application of big data to government functions (Chandy et al. 2017, 703-13; Poel et al. 2018). At the forefront of these efforts is China, which is planning to launch the social credit system (SCS), a data-powered project to monitor, assess, and shape the behavior of all citizens and enterprises.

While this new frontier of digital surveillance may seem like yet another mass-scale, government-led project possible only in China, the questions that it raises about the role of data technology in society also apply to democratic societies like the United States. With China openly manifesting its high-modernist belief in data technology that elevates order and control over privacy, the United States is faced with a shortening timeline to determine how to integrate data technology into its own politics and economy, and in so doing, what trade-offs it is willing—or unwilling—to make.

The United States should respond by establishing a comprehensive nationwide data protection framework that places limits on surveillance by both private business and the government. Not only because international human rights documents have long recognized the right to privacy, with recent technological developments adding a digital dimension. Rather, it is because personal data protection is an inalienable part of the ability of the United States to simultaneously pursue democracy, security, and growth. Without drawing its own baseline for personal data protection, the United

States risks missing the already narrowing opportunity to define its own balance between these values.

A Brief History of China's Social Credit System

For most of its history, the SCS was meant to be a narrowly scoped market reform initiative. The system was conceived in 1999, when then-Premier Zhu Rongji sought to ease the difficulty of foreign firms in obtaining information on their Chinese partners (Raphael and Xi 2019). For years after the system was mentioned at the 16th Party Congress in 2002 as a part of the effort by the Chinese Communist Party (CCP) to create a "unified, open, competitive and orderly modern market system," it was discussed in official documents only in the context of market reforms (Jiang 2002). In 2007, credit, tax, and contract performance records were suggested as potential elements of one's social credit status (Chorzempa et al. 2018). The Inter-ministerial Conference on Social Credit System Construction (the "Inter-ministerial Conference") was organized, consisting mostly of government bodies in charge of development, commerce, and taxation (中华人民共和国中央人民政府国务院办公厅, 2007).

> When a person engages in a trust-breaking behavior, the name and the social credit code of the individual will be published on the online "blacklist," along with details about the deed and the following legal sanctions; the trust-keeping equivalents will be announced on the online "red list."

This relatively unremarkable market reform initiative evolved into a pan-society digital reform project in 2014, with the announcement of the Plan for the Construction of the Social Credit System (the "2014 Plan"). According to the document, the system will function as a nationwide incentive mechanism, by collecting social credit information from every individual and enterprise to reward trust-keeping and punish trust-breaking behaviors (Creemers 2015). Although the original goal of reducing transaction costs in the market did not change, the scope of the system as outlined in the 2014 Plan was no longer limited to the economy. It was also meant to promote a culture of honesty and sincerity in all corners of society, including the government, the judiciary, private enterprises, and social organizations (Chorzempa et al. 2018, 2). By 2017, the Inter-ministerial Conference included a wide range of government departments, including the Central Propaganda Department, Ministry of Culture and Tourism, and the National Bureau of Statistics (新华财经 2017).

The 2014 Plan lays out a couple of features that differentiate it from previous reform policies. The first is an online disclosure of the identity of punished and rewarded individuals. When a person engages in a trust-breaking behavior, the name and the social credit code of the individual will be published on the online "blacklist," along with details about the deed and the following legal sanctions; the trust-keeping equivalents will be announced on the online "red list" (Engelmann et al. 2019). These black and red lists will be publicly searchable. Second, the system will operate on the principle of joint punishment and reward; once an individual is discovered to have engaged in dishonest behavior, he will face restrictions on a wide range of activities directly and indirectly related to the behavior. For instance, a failure to act upon a court judgment can lead to limitations on not only applications for government subsidies or certain professional licenses, but also sales of assets, operation of businesses, use of transportation, and consumption of luxury items (中华人民共和国中央人民政府 2016). The online identity disclosure and the joint incentive mechanism together seek to stop individuals who violate rules from going unnoticed and evading consequences (Ahmed 2019).

The system is currently designed to function as a data-powered public shaming and interactive propaganda platform. Under the Chinese judicial tradition, the court often announces the sentencing of a criminal in a public venue, symbolically asserting the party's control over public spaces while educating citizens about the cost of breaking the law (Trevaskes 2003, 362-364). The SCS transports this model to the online space by disclosing the identity of individuals, the details about their behaviors, and subsequent punishments. The SCS would also function as a propaganda channel that cuts through both the online and offline worlds. Previously, even if the government publicly denounced an individual in newspapers or film screenings, these announcements often went unnoticed by people who didn't use these mediums (Ahmed 2019). Under the SCS, sanctions and rewards are distributed in a more universal and standardized manner; not everyone who did the same good behaviors will be listed on the red list, but people with similar social credit standings will still be able to access the same benefits. In turn, individuals on the blacklist and the red list facilitate the spread of the government's messages by serving as models from whom others can learn.

> A project like the SCS may spark widespread public resistance in the United States, but thus far the reaction in China has been largely muted.

A project like the SCS may spark widespread public resistance in the United States, but thus far the reaction in China has been largely muted. Part of this response is cultural, as the Chinese notion of privacy differs from Western political and legal thought. Traditional Confucian philosophy values morality over respect for individual rights as the guiding principle for interpersonal relationships and the government of a society (Huang 2014, 7; Wang 2011, 34-53). As the conceptual barrier between each individual is not clear, privacy has traditionally meant family intimacy or shameful secrets (Wang 2011, 34-48). Chinese law, with the exception of instance-specific clauses such as protection against unlawful search or detention, generally treats the right to privacy mostly as a right to preserve one's reputation against insult and libel (Wang 2011, 50-53).

It further helps that Chinese people are no strangers to arbitrary and extended forms of surveillance. Since the Mao era, the Chinese government has kept *dang'an*, a secret dossier, on millions of its urban residents that maintains influence in the public sector to this day (Jacobs 2015; Yang 2011). The information included in the dossier ranges from one's educational and work performance, family background, and records of self-criticism to mental health conditions, but individuals do not have access to their *dang'an* (Ibid.). When a completely opaque system like *dang'an* has been in place for decades, an intrusive program like the SCS may feel less objectionable to the Chinese public.

Big data surveillance is already in place across the country. In Xinjiang, an autonomous region in western China home to Uighur Muslim minority, the government is collecting a vast array of citizens' information—including but not limited to DNA samples, iris scans, voice samples, applications installed on phones, and records of power consumption—in order to search for "suspected criminals." Xinjiang officials are required to respond to perceived abnormal behaviors (Human Rights Watch 2019). In effect, the granular monitoring of citizens' movement and social relations facilitates the arbitrary and indefinite detention of Uighur minorities in political re-education camps and other facilities, where the detained do not have even the most basic physical or procedural protections (Ibid.). The province of Guizhou—an underdeveloped region in the southwest where less than half of the population had been using the internet until a few years ago—has begun to use facial recognition technology to find crime suspects and missing children (Zhang 2018; The Economist 2018). The speed with which data are gathered and enhanced monitoring systems are deployed in a place like Guizhou leaves little room for doubt that it is only a matter of time before a nationwide big data surveillance program can be achieved.

China's High-Modernism

The Western response to the SCS has been a mix of disdain and concern. Some critics refer to the SCS as an "Orwellian" project that signals the rise of a digital totalitarian government, while others have argued that the SCS in its current form is too underdeveloped and disorganized to merit such a title.[1]

In light of the United States and China trade conflict, there is a concern that the SCS will be weaponized against foreign companies.[2]

While these encompass varying perspectives toward the system, they commonly reflect the underlying assumption that the SCS is a distinctly foreign phenomenon that only a country like China can execute.

> With the SCS, China is boldly presenting its ambition to prove the viability of big data surveillance as a substitute for independent and accountable institutions, such as banks, courts, and transparent bureaucracies, that have traditionally been considered to be prerequisites for long-term development.

But looking at the SCS through the lens of China's development trajectory and ambition to become a global technology leader, a different narrative emerges. The SCS represents China's answer to questions about the extent to which states can successfully use science and technology to rationalize and control society. With the SCS, China is boldly presenting its ambition to prove the viability of big data surveillance as a substitute for independent and accountable institutions, such as banks, courts, and transparent bureaucracies, that have traditionally been considered to be prerequisites for long-term development.

Despite its vibrant market economy, China suffers from a lack of trust among market participants that often results in rule-breaking and increased transaction costs. Recurring news of food safety violations, counterfeit goods, and scams are common.[3]
Businesses face risks of fraud with partners, employees, and the research knowledge they consume (Qin 2017; Jacobs 2019). Within supply chains, companies doubt the information provided by contractors, and the culture

of cheating among online sellers to artificially boost their reputation has forced e-commerce platforms to spend considerable resources to detect fraud (Özer et al. 2019; Zhang et al. 2013).

The problem persists partially because the Chinese economy lacks independent institutions that distribute resources based on unbiased judgment. For example, banks typically help spread trust in the economy by distributing credit based on independent assessments of the risk and trustworthiness of borrowers (Berggren and Jordahl 2006, 144-145; Lapavitsas 2007, 416-471). One of the functions of an independent judiciary is to promote trust in society by ensuring that the law is applied in a continuous and consistent manner independent from political uncertainties (ABA 2017; ABA 2020). However, in China, the establishment of these independent institutions cannot take place, as it will undermine single-party authoritarian rule. The Chinese state needs to be able to control the banking system to support state-owned enterprises, many of which enjoy preferential access to loans despite their lack of competitiveness and profitability (Huang 2019). Despite high-level calls from the party leadership to strengthen the rule of law, it does not mean independence of the court; on the contrary, judicial independence is denounced even within the court system (Heath and Zhang 2017).

> The standardized mechanism of the SCS may help reduce the perceived level of arbitrariness of the current legal system in distributing rewards and sanctions.

The SCS seeks to address this problem by allowing for greater information sharing without generating too much political risk. Even if the distribution of credit may not fully reflect the trustworthiness of borrowers or the prospect of high-return on investments, market actors can still perform basic due diligence by referring to the public records of rule-breaking activities by counterparties. The standardized mechanism of the SCS may help reduce the perceived level of arbitrariness of the current legal system in distributing rewards and sanctions.

The SCS is also a measure to discipline CCP members and hold them accountable for bureaucratic dysfunction ranging from loss and theft of important documents to falsification of official statistics (LaFraniere 2009; Holz 2005, 6-10; Chen et al. 2019). In China, navigating bureaucratic hurdles is the single biggest challenge for businesses (Qing 2011). Moreover, corruption in regulatory agencies has contributed to some of the biggest public health and safety scandals in the country (Huang 2013).

The party leadership has long recognized the need to reform the administrative system. But despite public warnings from presidents and premiers about rampant inefficiency and corruption in the government, principal-agent problems have slowed the pace of reform (Jacobs 2012).

The highly decentralized mechanism of designing and implementing policies, in which the central government announces broadly defined objectives and regional governments experiment with detailed policy measures, has encouraged productive competition between officials from different provinces, but also made it difficult for the central government to monitor and supervise local policy implementations (Fewsmith and Gao 2014; Zhong 2015, 138-143). Taking advantage of this information asymmetry, local officials often resist and distort central government guidance and prioritize their interests (Ibid.).

Eliminating administrative dysfunctions and abuses would take transparency and accountability within the party organization, but too many have a stake in maintaining the organizational complexities and the unofficial tradition of exchanging favors that they can exploit (Fewsmith and Gao 2014, 174). The SCS may help address this dilemma by streamlining administrative procedures while allowing the party leadership to retain control over national policies. In fact, since the 1990s, party leadership has shown considerable enthusiasm about the potential of information and communications technologies (ICT) to enhance transparency in the government without undermining its power (Ma et al. 2005; Seifert and Chung 2009, 12). In this context, the 2014 Plan states that a successful management of government affairs is the crux of promoting sincerity in the rest of society and calls for an improvement in the collection and assessment of data to “[enhance] the credibility in government functions” (Creemers 2015).

The SCS still suffers from numerous deficiencies, but the problems occasionally reported in the Western media may only be a temporary problem. The stalwart support that the Chinese government has given to the big data and artificial intelligence industries is bearing fruit. On top of its unparalleled advantage in access to raw data, China is a dominant player in big data and artificial intelligence by many measures, including the numbers of research organizations, scientific publications, and patent filings (WIPO 2019, 59-64). The State Council already announced in 2017 a plan for China to become the international center for big data application to all corners of society, covering industry, agriculture, education, healthcare, finance, court system, and urban planning (Triolo et al. 2018).

China's Wish: Big Data Hegemony

The opportunity to promote a new model of governance abroad while trumpeting its technological capacity has not gone unnoticed by China. China has long been aware of the disadvantage of being a follower of rules in the technology sector and has sought to become a standard-setter in the international market (Bach et al. 2006, 504-505). Recent advances in the domestic ICT industry have pushed the country ever closer to achieving this goal.

> China has long been aware of the disadvantage of being a follower of rules in the technology sector and has sought to become a standard-setter in the international market.

For years, CCP leadership has treated consolidation of its data governance structure as a policy priority. In 2014, President Xi personally took charge of the Central Leading Group for Cybersecurity and Informatization to issue policy guidelines coordinated by the State Council, the top administrative authority (Gierow 2014, 2-4). The 2017 National Intelligence Law requires companies to cooperate with the government's intelligence activities (Tanner 2017). The Cybersecurity Law enacted in 2017 covers a broad range of issues including digital economy, security, data, encryption, content management, and infrastructure (Sacks).

In the same year, the consolidation of data governance architecture progressed to the international stage. Shortly before the 19th Party Congress in 2017, the previously undisclosed Cyberspace Administration of China published an article expounding China's strategy to become a "cyber superpower" (Kania et al. 2017). Recognizing that cyberspace has become a new area of global competition, the article envisions that the Chinese practice of internet governance will become a future "international consensus" (Ibid.).

Photo by: Dong Fang, **https://commons.wikimedia.org/wiki/File:18th_National_Congress_of_the_Co…**
<
https://commons.wikimedia.org/wiki/File:18th_National_Congress_of_the_Communist_Party_of_China.jpg
>

The Chinese cyber governance architecture is already being exported around the world. Tanzania, following its selection as the pilot country for a China-Africa capacity building program, passed laws that limit internet content and blogging activities (Sacks 2018). Officials in other countries, like Vietnam and Uganda, consulted with Chinese authorities before enacting their own restrictive internet laws (Dave 2018). Under the Belt and Road Initiative, China has begun to install data transmitting cross-border optic cables in countries like Belize, Ecuador, and Guinea (Patrick and Feng 2018). Chinese intelligence monitoring systems are already in use in many countries around the world, including but not limited to

Singapore, Malaysia, Pakistan, the United Arab Emirates, Uzbekistan, and Kenya (Polyakova and Meserole 2019, 6; Mozur et al. 2019). Non-Western countries are not the only targets in this effort; Chinese authorities have stepped up pressure on major internet companies, including those banned in China like Google and Facebook, to cooperate with its censorship policies (Mozur 2018). At international industry meetings, government officials attempt to exchange business deals for support of their proposals on technical standards (Beattle 2019).

> Countries that are facing pressing growth targets without strong support for liberal values are seeing the value of big data for its ability to bypass the cumbersome and messy stage of building liberal institutions.

Under the current climate of weakening international consensus on the supremacy of liberalism, the Chinese government's attempt to harness the analytical and predictive power of data technology to supplant independent and accountable institutions may bring serious repercussions. As the market-based bureaucratic reform model of outsourcing government functions to private service providers has been losing its appeal in the developing world, China is demonstrating that economic and political liberalisms do not have to go hand-in-hand. Countries that are facing pressing growth targets without strong support for liberal values are seeing the value of big data for its ability to bypass the cumbersome and messy stage of building liberal institutions.

Weighing the Trade-offs for the United States

The most immediate challenge from these developments for the United States is geopolitical. The wide-ranging applications of the big data industry for commerce and security makes it an area of competition. In many industries, the United States has maintained leadership not just by its advanced research and development capabilities, but also by its ability to set industry standards and protocols. This matters particularly for dual-use technologies, since the dominance of American manufacturers and standards limits the ability of rivals to hamper U.S. access to these technologies (Bach et al. 505). As markets are increasingly defined less by physical borders and more by standards and regulations, the ability to establish and enforce rules has become even more critical for the efficiency and reliability of U.S. technology products and services (Schoff and Ito 2019).

In the long term, however, the challenge posed by China goes beyond the question of who will maintain dominance in the data industry; it asks whether the United States will also choose to test the maximum power of data technology to control and rationalize society. In the United States, a full-hearted embrace of big data would mean trade-offs for the ability of its citizens to exercise civic freedom and demand government oversight and transparency, a foundational element of U.S. political and economic institutions. Instead, the United States should carefully integrate the benefits of big data into its society while minimizing potential risks, and this should be done through a nationwide, comprehensive personal data protection regime.

> Even data that are supposed to be anonymous can easily be de-anonymized and used to reveal characteristics of the subjects, such as their political and religious views.

Not surprisingly, strong arguments have been made on both sides. On the one hand, scholars and rights advocates argue that privacy constitutes an essential element of individual freedom. On the other hand, businesses and security agencies warn that a stringent data protection law would have burdensome regulatory costs and hinder effective law and security enforcement. As the debate continues, the tendency of societal actors has been to test the limits of the collection and use of personal data. Across states, for example, police have considered using some of the newest facial recognition technologies (Harwell 2019; Hill 2020). A new privately developed facial recognition software scrapes every single image of a person that can be found online and hyperlinks to the images. As police departments experiment with the app, the developers can monitor the search activities by the officers (Hill 2020). And a recent investigation by The New York Times demonstrated that a location data company can track senior government and security officials, including the President, through their cell phone pings. When combined with publicly available records, these location data can reveal intimate details of the officials and their families (Thomson and Warzel 2019). Even data that are supposed to be anonymous can easily be de-anonymized and used to reveal characteristics of the subjects, such as their political and religious views (Narayanan and Shmatikov 2006).

The granular monitoring and targeting of individuals that big data technology enables jeopardizes free and open debate in society, even through seemingly innocuous applications. The online mechanism that gives people recommendations for books and movies is also used to personalize the curation of news stories and political messages (O’Neil 2016, 183-185; Illing 2017). Political advertisements are customized to each voter based on information about her racial and ethnic profile, economic status, and political inclinations. It has become possible for next-door neighbors to receive different messages from the same politician and different search results for the same keyword (Pariser 2011).

Photo By: Bill Ingalls, NASA, **https://www.nationalguard.mil/Resources/Image-Gallery/News-Images/igphoto/2000793912/**
< https://www.nationalguard.mil/Resources/Image-Gallery/News-Images/igphoto/2000793912/>

Such targeted messaging can make mass communication more cost-effective, but does not encourage a lively debate based on a common set of facts—it makes debate avoidable and unnecessary. Politicians may be able to convince voters with greater ease, but there are less opportunities for voters to recognize, confront, and reconcile disagreements among them (Illing 2017). It is precisely this kind of micro-level targeting that Russia utilized to interfere with the 2016 U.S. presidential election (United States Congress 2019, 32-42).

> As the micro-targeting and behavior-shaping capability of big data completely lifts the technical barrier that insulates this safe space from external influence, the legal safeguard against potential government abuse of data technology must be strengthened.

The increasingly fragmented and surveilled sphere of one's online presence narrows the space for minority ideas (Shaw 2017). Freedom in a democratic society requires an intellectual safe space where individuals can experiment and discuss controversial ideas without scrutiny, thereby forming ideas in a manner of their own choosing without being pressured into conformity (Richards 2013, 1946-1950; Cohen 2013, 1912). As the micro-targeting and behavior-shaping capability of big data completely lifts the technical barrier that insulates this safe space from external influence, the legal safeguard against potential government abuse of data technology must be strengthened.

History is riddled with too many cautionary tales to overlook the need for additional lines of protection. It was only a few decades ago that the Federal Bureau of Investigation was able to wiretap civil rights leader Martin Luther King, Jr. and distribute misleading reports on his beliefs, or that the Central Intelligence Agency launched domestic surveillance of political dissidents under the guise of a "counter-terrorism" operation (Garrow 2002; Medsger 2014, 203). Even now, more than half a decade after the uproar against the National Security Agency's mass surveillance program, government agencies maintain checkered records of compliance with the Foreign Intelligence Surveillance Act (Goitein 2019).

If the hyper-monitoring ability of big data poses risks to civic freedom, the reliance on algorithmic decision-making renders accountability moot. When the decision-maker is a computer, it is unclear who is to be held accountable when mistakes are made. Big data analysis involves a search for unanticipated correlations and predictions about the future, rather than understanding the nature of existing relationships between data points (Andrejevic and Gates 2014, 190; Devins et al. 2016, 360-362). Thus, growing complexity and variety within the dataset lowers an algorithm's ability to tell which pieces of data contributed to correlation or by how much. If one does not understand the process of analysis, it becomes much more difficult to contest the outcome.

This "black box" problem becomes even more serious when considering the embedded human biases in these algorithms. Numerous cases demonstrate that algorithms are far from the impartial and objective arbiters of truth that they are expected to be. Instead, they make decisions based on the same biases their human designers have—such as against race, gender, and socioeconomic backgrounds—to distribute risks and resources in society, but on a scale much larger than that of any human-made decision (O'Neil 2016). The argument that more data means greater efficiency and accuracy operates on the assumption that data and algorithms are objective and fair, but in reality, human bias is mixed into practically every stage of data collection and analysis.

> The argument that more data means greater efficiency and accuracy operates on the assumption that data and algorithms are objective and fair, but in reality, human bias is mixed into practically every stage of data collection and analysis.

Of course, it is undeniable that big data has enabled a more efficient, precise, and safe delivery of goods and services in many parts of society, and it will be the driver of growth and innovation in the coming years. Some of the newly available data will bring insights into previously inscrutable security matters. There is no question that individuals and society should be able to take advantage of the benefits scientific development brings.

Nonetheless, it should be recognized that on the flip side of great benefits lie immense risks. The data-gathering that exposes all individuals and the data analyses that magnify the reach of existing human biases can potentially be harmful for growth and security in the long term. Once a private enterprise can track almost anyone in the U.S. government, there is no guarantee that this data will stay in the hands of responsible individuals. A telling example from China shows that, without strong legal protections, one person was able to publicize the sensitive information of 346,000 individuals (Yin 2018). The burgeoning digital espionage and cyberwarfare sector is only one of many other reasons to be concerned; even without any illegality involved, the acquisition of data-rich companies by foreigners presents U.S. national security risks.[4]

The U.S. Response: A Federal Data Protection Law

As of now, there is no international consensus on how data technologies should be regulated. Approximately 30 percent of countries do not have national data protection laws, and many countries only have partial laws with limited coverage and broad exemptions (UNCTAD 2016, 8-10). Even though various global and regional organizations have issued privacy guidelines, many of these guidelines have been silent on the issue of government surveillance (UNCTAD 2016, 56-57). The United States, despite being home to the world's largest internet companies and the most sophisticated data technologies, is yet another country that does not have a principal data protection law and instead relies on a flurry of sector-specific or state-level regulations (Chabinsky and Pittman 2019).

To refurbish its current fragmented system, the United States needs to adopt a data protection regime that is nationwide in reach and comprehensive in scope. Its application should encompass the collection, storage, and use of personal data by both businesses and the government. It is possible that government entities may be given a different, possibly more flexible, set of rights and responsibilities from that of private companies. Nonetheless, public authorities should not be left beyond the reach of written rules, and safeguard measures are needed to make sure that temporarily and conditionally granted flexibilities do not turn into an arbitrary relaxation of rules for an indefinite period of time.

> Should it take an approach that allows more room for adaptation, the federal data protection framework should still be able to function as an effective standard of accountability, possibly in combination with sector-specific rules and guidelines.

At the same time that it upholds the values enshrined in the democratic system, the upcoming regime would need to suit the priorities of U.S. society. The European Union’s General Data Protection Regulation provides many useful points of reference, but its relatively rigid, process-oriented enforcement mechanism in certain areas might not be congruent with the particular emphasis that the U.S. places on innovation and a broader understanding of freedom (Kerry 2018). Should it take an approach that allows more room for adaptation, the federal data protection framework should still be able to function as an effective standard of accountability, possibly in combination with sector-specific rules and guidelines (Ibid.).

Greater flexibility will also require more creativity in designing the mechanisms for balancing competing needs. For instance, the most transparent way to audit the algorithms used by public authorities would be to take France's approach of disclosing them to the public. Such method is not without side effects, of course; it may deter productive competition among algorithm designers and give an advantage only to those who are able to understand the math (O'Neil 2018). But this does not mean the black box problem should be left unaddressed. It is possible to come up with alternatives, such as having an independent body of experts regularly verify the fairness and reliability of the algorithms and publish the outcomes of algorithmic decisions used in public administration and law enforcement (The Financial Times Editorial Board 2019).

Lessons from Coronavirus and Managing the Balance

Ultimately, establishing the level of data protection is a political question. Depending on where a society strikes the balance between privacy and other goals, such as growth, order, and security, in their own historical and political contexts, these values can seem either mutually exclusive or reinforcing. In addition, because the notion of privacy itself is socially constructed, what is considered to be sensitive personal information will change across time.

The political nature of privacy protection will become even clearer in upcoming years, not least because of the significant contributions that data technologies are making to the global coronavirus (COVID-19) outbreak response. In China, drones flew around neighborhoods to monitor pedestrians without face masks; in some cities, citizens had to scan their QR codes to enter public places or use public transportation (Wall Street Journal 2020; Mozur et al. 2020). Even though South Korea did not enforce such strict restrictions on citizens' movement, public health authorities extensively used CCTV images, cell phone location data, and credit card histories to track the movements of confirmed patients and identify suspected cases (Sonn 2020). Despite concerns about their privacy and data security practices, video conferencing applications are allowing education and the provision of medical services to continue without the risk of exposure to the virus.

> At the same time, the coronavirus has shown that technology alone, including powerful surveillance systems, is not enough to prevent and contain a large-scale crisis.

At the same time, the coronavirus has shown that technology alone, including powerful surveillance systems, is not enough to prevent and contain a large-scale crisis. The initial outbreak in the city of Wuhan was not due to the CCP's inability to control the movement of its people, but was a direct consequence of the government's misplaced priority on maintaining its political standing over addressing public health concerns. Once the spread of the disease became unstoppable, the availability of medical personnel, equipment, and facilities, and the ability of the government to efficiently coordinate their deployment became the key factors in reducing fatalities. Not all of these resources could be produced overnight with the help of technology; rather, they are parts of the public health infrastructure and the emergency institutional capacity that needed to be maintained during ordinary times. World-class science research capacities could do nothing to assuage the fear of the public when the government failed to provide clear guidance on basic protective measures and reliable information on the status of the outbreak.

In South Korea, certain mishaps in the early period of the outbreak necessitated a quick, aggressive use of surveillance to stop a further downward spiral, but the process of reining in the disease in the country was not that of an enlightened government imposing control over oblivious or unwilling citizens. Rather, the government alerted citizens of the severity of the disease through early recommendations on wearing masks and stay-at-home orders, and provided clear status updates through a speedy roll-out of mass testing. The consistently applied waiver of testing and treatment fees and generous support for quarantined individuals helped relieve citizens' fear and encouraged them to voluntarily report suspected symptoms. It was through the active participation of well-informed citizens practicing proper personal safety measures, and trust in the ability of their society to collectively curb further damage, that the country has been able to reduce the number of new infections without putting a halt to the ordinary course of life.

Whether terrorism, financial crisis, or a pandemic, future global crises will spread through the movement of goods, people and information. The ability of states to balance data technology and privacy with other critical goals will in part determine what the future looks like. In this regard, the SCS is an example of what becomes possible when the decision skews toward an unquestioning prioritization of order and development. Whatever course of action the United States takes, it will become a symbol of how a liberal, innovation-driven society approaches the balancing act. Given the pace of growth in the data industry, simply delaying an answer amounts to supporting more boundary-pushing activities and experiments. The United States' response to the lure of big data should be a personal data protection law that allows society to benefit from technology without sacrificing the values it upholds.

About the Author

Eunsun Cho is a Master's student at the Jackson Institute for Global Affairs at Yale University. She can be reached at **eunsun.cho@yale.edu** < mailto:eunsun.cho@yale.edu>

.

Notes

[1]

For example, see The Economist, 2016 and Fickling, 2019.

[2]

For example, see Stevenson and Mozur, 2019.

[3]

For example, see Government of Canada Trade Commissioner Services, 2019, South China Morning Post, 2016, and Campbell, 2016.

[4]

For example, see Shen and Wang, 2019.

References

Ahmed, Shazeda. “The Messy Truth About Social Credit.” Logic Magazine. May 1, 2019. **https://www.logicmag.io/china/the-messy-truth-about-social-credit/**

< http://www.logicmag.io/china/the-messy-truth-about-social-credit/>

.

American Bar Association (ABA). "Introduction: The Role of Courts in Our Society." American Bar Association. June 2, 2017.

https://www.americanbar.org/groups/crsj/publications/human_rights_magazine_home/2016-17-vol-42/vol-42-no-3/introduction-the-role-of-courts-in-our-society/
< https://www.americanbar.org/groups/crsj/publications/human_rights_magazine_home/2016-17-vol-42/vol-42-no-3/introduction-the-role-of-courts-in-our-society/>

.

ABA. “An Independent Judiciary: The Shield of a Free Society.” American Bar Association. February 18, 2020. **https://www.americanbar.org/groups/judicial/publications/appellate_issues/2020/winter/an-independent-judiciary-the-shield-of-a-free-society/**
< https://www.americanbar.org/groups/judicial/publications/appellate_issues/2020/winter/an-independent-judiciary-the-shield-of-a-free-society/>

.

Andrejevic, Mark and Kelly Gates. “Big Data Surveillance: Introduction.” Surveillance & Society 12, no. 2 (2014).

Bach, David, et al. “The International Implications of China's Fledgling Regulatory State: From Product Maker to Rule Maker.” New Political Economy 11, no. 4 (December 2006). doi: 10.1080/13563460600990731.

Beattle, Alan. “Technology: How the US, EU and China Compete to Set Industry Standards.” Financial Times. July 24, 2019. **https://www.ft.com/content/0c91b884-92bb-11e9-aea1-2b1d33ac3271**
< https://www.ft.com/content/0c91b884-92bb-11e9-aea1-2b1d33ac3271>

.

Berggren, Niclas, and Henrik Jordahl. “Free to Trust: Economic Freedom and Social Capital.” Kyklos 59, no. 2 (2006): 144–145. doi:10.1111/j.1467-6435.2006.00324.x.

Campbell, Charlie. "China Vaccine Scandal Prompts Angry Backlash From Parents and Doctors.” Time. March 22, 2016. **https://time.com/4267266/china-vaccine-scandal/**

< https://time.com/4267266/china-vaccine-scandal/>

.

Chabinsky, Steven and F. Paul Pittman. “USA: Data Protection 2019.” The International Comparative Legal Guides. March 7, 2019. **https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa**

< https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa>

.

Chandy, Rajesh, et al. “Big Data for Good: Insights from Emerging Markets.” Journal of Product Innovation Management 34, no. 5 (September 2017). doi:10.1111/jpim.12406.

Chen, Wei, et al. “A Forensic Examination of China's National Accounts.” Brookings Papers on Economic Activity, Spring 2019, pp. 84–109., doi:10.3386/w25754.

Chorzempa, Martin, et al. China's Social Credit System: A Mark of Progress or a Threat to Privacy? Peterson Institute for International Economics (2018): 3. **https://www.piie.com/system/files/documents/pb18-14.pdf**
< http://www.piie.com/system/files/documents/pb18-14.pdf>

.

Cohen, Julie E. "What Privacy is For." Harvard Law Review 126, no. 7 (May 2013).

Creemers, Rogier. "Planning Outline for the Construction of a Social Credit System (2014-2020)." China Copyright and Media. April 25 2015. **https://www.chinacopyrightandmedia.wordpress.com/2014/06/14/planning-outline-for-the-construction-of-a-social-credit-system-2014-2020/**
< http://www.chinacopyrightandmedia.wordpress.com/2014/06/14/planning-outline-for-the-construction-of-a-social-credit-system-2014-2020/>
. Unofficial translation of 《社会信用体系建设规划纲要（2014—2020年）》.

Dave, Paresh. "China exports its restrictive internet policies to dozens of countries: report." Thomson Reuters. November 1, 2018. **https://www.reuters.com/article/us-global-internet-surveillance/china-exports-its-restrictive-internet-policies-to-dozens-of-countries-report-idUSKCN1N63KE**
< https://www.reuters.com/article/us-global-internet-surveillance/china-exports-its-restrictive-internet-policies-to-dozens-of-countries-report-idUSKCN1N63KE>

.

Devins, Carynm Teppo Felin, et al. “The Law and Big Data.” Cornell Journal of Law and Public Policy 27, issue 2 (2017).

Engelmann, Severin, et al. “Clear Sanctions, Vague Rewards.” Proceedings of the Conference on Fairness, Accountability, and Transparency - FAT* (2019). doi:10.1145/3287560.3287585.

Fewsmith, Joseph, and Xiang Gao. “Local Governance in China: Incentives &amp; Tensions.” Daedalus 143, no. 2 (2014): 171. doi:10.1162/daed_a_00281.

Fickling, David. "China’s Social Credit System Is More Kafka Than Orwell.” Bloomberg. June 19, 2019. **https://www.bloomberg.com/opinion/articles/2019-06-19/china-s-social-credit-system-is-disorganized-and-little-used**

< https://www.bloomberg.com/opinion/articles/2019-06-19/china-s-social-credit-system-is-disorganized-and-little-used>

.

Garrow, David J. “The FBI and Martin Luther King.” The Atlantic (July/August 2002). **https://www.theatlantic.com/magazine/archive/2002/07/the-fbi-and-martin-luther-king/302537/**

< https://www.theatlantic.com/magazine/archive/2002/07/the-fbi-and-martin-luther-king/302537/>

.

Gierow, Hauke J. “Cyber Security in China: New Political Leadership Focuses on Boosting National Security.” China Monitor, no. 20. Mercantor Institute for China Studies. December 9, 2014: 2-4.

Goitein, Eliabeth. “How the FBI Violated the Privacy Rights of Tens of Thousands of Americans.” Brennan Center for Justice. October 22, 2019. **https://www.brennancenter.org/our-work/analysis-opinion/how-fbi-violated-privacy-rights-tens-thousands-americans**

< https://www.brennancenter.org/our-work/analysis-opinion/how-fbi-violated-privacy-rights-tens-thousands-americans>

.

Government of Canada Trade Commissioner Services. “Fraud and Scams in China.” June 20, 2019. **https://www.tradecommissioner.gc.ca/china-chine/market-facts-faits-sur-le-marche/148081.aspx?lang=eng**

< https://www.tradecommissioner.gc.ca/china-chine/market-facts-faits-sur-le-marche/148081.aspx?lang=eng>

.,

Harwell, Drew. “Oregon became a testing ground for Amazon’s facial-recognition policing. But what if Rekognition gets it wrong?” The Washington Post. April 30, 2019. **https://www.washingtonpost.com/technology/2019/04/30/amazons-facial-recognition-technology-is-supercharging-local-police/**

< https://www.washingtonpost.com/technology/2019/04/30/amazons-facial-recognition-technology-is-supercharging-local-police/>

.

Heath, Nicholas and Lusha Zhang. “China's top judge warns courts on judicial independence.” Reuters. January 15, 2017. **https://www.reuters.com/article/us-china-policy-law/chinas-top-judge-warns-courts-on-judicial-independence-idUSKBN14Z07B** < https://www.reuters.com/article/us-china-policy-law/chinas-top-judge-warns-courts-on-judicial-independence-idUSKBN14Z07B>

.

Hill, Kashmir. “The Secretive Company That Might End Privacy as We Know It.” The New York Times. January 18, 2020. **https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html?action=click&module=Top%20Stories&pgtype=Homepage** < https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html?action=click&module=Top%20Stories&pgtype=Homepage>

.

Holz, Carsten A. “OECD — China Governance Project.” OECD Statistics Working Papers, 19 Jan. 2005, pp. 6–10., doi:10.1787/640443218516.

Huang, Philip C. C. “Morality and Law in China, Past and Present.” Modern China 41, no. 1 (2014). doi:10.1177/0097700414553923.

Huang, Tianlei. China Is Only Nibbling at the Problem of "Zombie" State-Owned Enterprises. Peterson Institute for International Economics. 2019. **https://www.piie.com/blogs/china-economic-watch/china-only-nibbling-problem-zombie-state-owned-enterprises**

< https://www.piie.com/blogs/china-economic-watch/china-only-nibbling-problem-zombie-state-owned-enterprises>

.

Huang, Yasheng. "Democratize or Die: Why China's Communists Face Reform or Revolution." Foreign Affairs (January/February 2013). **www.foreignaffairs.com/articles/china/2012-12-03/democratize-or-die**

< http://www.foreignaffairs.com/articles/china/2012-12-03/democratize-or-die>

.

Human Rights Watch. "China's Algorithms of Repression: Reverse Engineering a Xinjiang Police Mass Surveillance App." June 25, 2019. **https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass-surveillance**

< https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass-surveillance>

.

Illing, Sean, "A political scientist explains how big data is transforming politics." Vox. March 16, 2017, **https://www.vox.com/conversations/2017/3/16/14935336/big-data-politics-donald-trump-2016-elections-polarization**

< https://www.vox.com/conversations/2017/3/16/14935336/big-data-politics-donald-trump-2016-elections-polarization>

.

Jacobs, Andrew. " Rampant Fraud Threat to China's Brisk Ascent." The New York Times. October 6, 2019. **https://www.nytimes.com/2010/10/07/world/asia/07fraud.html**

< https://www.nytimes.com/2010/10/07/world/asia/07fraud.html>

.

Jacobs, Andrew. "A Rare Look Into One's Life on File in China." The New York Times. March 15, 2015. **https://sinosphere.blogs.nytimes.com/2015/03/15/a-rare-look-into-ones-life-on-file-in-china/**

< https://sinosphere.blogs.nytimes.com/2015/03/15/a-rare-look-into-ones-life-on-file-in-china/>

.

Jacobs, Andrew. "Chinese Officials Find Misbehavior Now Carries Cost." The New York Times. December 25, 2012. **https://www.nytimes.com/2012/12/26/world/asia/corrupt-chinese-officials-draw-unusual-publicity.html**

< https://www.nytimes.com/2012/12/26/world/asia/corrupt-chinese-officials-draw-unusual-publicity.html>

.

Kania, Elsa, et al. "China's Strategic Thinking on Building Power in Cyberspace." New America. September 25, 2017, **https://www.newamerica.org/cybersecurity-initiative/blog/chinas-strategic-thinking-building-power-cyberspace/**

< https://www.newamerica.org/cybersecurity-initiative/blog/chinas-strategic-thinking-building-power-cyberspace/>

.

Kerry, Cameron F. "Why protecting privacy is a losing game today—and how to change the game." The Brookings Institution. July 12, 2018. **https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/#_edn4** < https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/#_edn4>

.

LaFraniere, Sharon. "Files Vanished, Young Chinese Lose the Future." The New York Times, 26 July 2009, **https://www.nytimes.com/2009/07/27/world/asia/27china.html** < https://www.nytimes.com/2009/07/27/world/asia/27china.html>

.

Lapavitsas, Costas. "Information and Trust as Social Aspects of Credit." Economy and Society 36, no. 3 (2007): 416–417. doi:10.1080/03085140701428381.a.

Ma, Lianjie, et al. "E-Government in China: Bringing Economic Development through Administrative Reform." Government Information Quarterly 22, no. 1 (2005): 20–37. doi:10.1016/j.giq.2004.10.001.

Medsger, Betty. 2014. The Burglary: The Discovery of J. Edgar Hoover's Secret FBI. (New York: Alfred A. Knopf), 203.

Mozur, Paul, et al. "In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags." The New York Times, March 1, 2020,

https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html

< https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html>

.

Mozur, Paul, et al. "Made in China, Exported to the World: The Surveillance State." The New York Times. April 24, 2019. **https://www.nytimes.com/2019/04/24/technology/ecuador-surveillance-cameras-police-government.html**

< https://www.nytimes.com/2019/04/24/technology/ecuador-surveillance-cameras-police-government.html>

.

Mozur, Paul. "China Presses Its Internet Censorship Efforts Across the Globe." The New York Times. March 2, 2018. **https://www.nytimes.com/2018/03/02/technology/china-technology-censorship-borders-expansion.html**

< https://www.nytimes.com/2018/03/02/technology/china-technology-censorship-borders-expansion.html>

.

Narayanan, Arvind and Vitaly Shmatikov. "Robust De-anonymization of Large Sparse Datasets." 2006.

O'Neil, Cathy. 2016. Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. New York: Crown Publishing Group.

O'Neil, Cathy. "Audit the algorithms that are ruling our lives." The Financial Times. July 30, 2018. **https://www.ft.com/content/879d96d6-93db-11e8-95f8-8640db9060a7**

< https://www.ft.com/content/879d96d6-93db-11e8-95f8-8640db9060a7>

.

Özer, Özalp, et al. "Trust, Trustworthiness, and Information Sharing in Supply Chains Bridging China and the U.S." Management Science 60, no. 10 (2014): 2435–2460. doi:10.1287/mnsc.2014.1905.

Pariser, Eli. 2011. "Introduction" in The Filter Bubble: How the New Personalized Web Is Changing What We Read and How We Think. New York: Penguin Books.

Patrick, Stewart M. and Ashley Feng. "Belt and Router: China Aims for Tighter Internet Controls with Digital Silk Road." Council on Foreign Relations. July 2, 2018. **https://www.cfr.org/blog/belt-and-router-china-aims-tighter-internet-controls-digital-silk-road**

< https://www.cfr.org/blog/belt-and-router-china-aims-tighter-internet-controls-digital-silk-road>

.

Poel, Martijn, Eric T. Meyer, and Ralph Schroeder. "Big Data for Policymaking: Great Expectations, but with Limited Progress?" Policy and Internet 10, no. 3 (2018). doi: 10.1002/poi3.176.

Polyakova, Alina, and Chris Meserole. 2019. Exporting Digital Authoritarianism. The Brookings Institution.

Qin, Amy. “Fraud Scandals Sap China’s Dream of Becoming a Science Superpower.” The New York Times. October 13, 2017. **https://www.nytimes.com/2017/10/13/world/asia/china-science-fraud-scandals.html**

< https://www.nytimes.com/2017/10/13/world/asia/china-science-fraud-scandals.html>

.

Qing, Koh Gui. “U.S. firms frustrated by Chinese red tape.” Reuters. March 22, 2011. **https://www.reuters.com/article/us-china-usa-business/u-s-firms-frustrated-by-chinese-red-tape-idUSTRE72L1J420110322**

< https://www.reuters.com/article/us-china-usa-business/u-s-firms-frustrated-by-chinese-red-tape-idUSTRE72L1J420110322>

.

Raphael, René, and Ling Xi. “Discipline and Punish: The Birth of China’s Social-Credit System.” The Nation. 2019. **https://www.thenation.com/article/china-social-credit-system/**

< http://www.thenation.com/article/china-social-credit-system/>

.

Richards, Neil M. “The Danger of Surveillance.” Harvard Law Review 126, no. 7 (May 2013).

Sacks, Samm. "Beijing Wants to Rewrite the Rules of the Internet." The Atlantic. June 18, 2018. **https://www.theatlantic.com/international/archive/2018/06/zte-huawei-china-trump-trade-cyber/563033/**

< https://www.theatlantic.com/international/archive/2018/06/zte-huawei-china-trump-trade-cyber/563033/>

.

Sacks, Samm. "China's Emerging Cyber Governance System." Center for Strategic and International Studies. **https://www.csis.org/chinas-emerging-cyber-governance-system**

< https://www.csis.org/chinas-emerging-cyber-governance-system>

.

Schoff, James L. and Asei Ito. "Competing with China on Technology and Innovation." Carnegie Endowment for International Peace. October 10, 2019. **https://carnegieendowment.org/2019/10/10/competing-with-china-on-technology-and-innovation-pub-80010**

< https://carnegieendowment.org/2019/10/10/competing-with-china-on-technology-and-innovation-pub-80010>

.

Scott, James C. 1998. Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed. New Haven and London: Yale University Press.

Seifert, Jeffrey and Johngpil Chung. "Using E-Government to Reinforce Government–Citizen Relationships." Social Science Computer Review 27, no. 1 (February 2009): 12.

Shaw, Jonathan. "The Watchers: Assaults on Privacy in America." Harvard Magazine (January-February 2017). **https://harvardmagazine.com/2017/01/the-watchers**
< https://harvardmagazine.com/2017/01/the-watchers>
.

Shen, Meg and Echo Wang. "China's Beijing Kunlun to revisit Grindr IPO." Reuters. July 29, 2019, **https://www.reuters.com/article/us-grindr-listing/chinas-beijing-kunlun-to-revisit-grindr-ipo-idUSKCN1UO1PV**
< https://www.reuters.com/article/us-grindr-listing/chinas-beijing-kunlun-to-revisit-grindr-ipo-idUSKCN1UO1PV>
.

Sonn, Jung Won. "Coronavirus: South Korea's success in controlling disease is due to its acceptance of surveillance." The Conversation. March 19, 2020. **http://theconversation.com/coronavirus-south-koreas-success-in-controlling-disease-is-due-to-its-acceptance-of-surveillance-134068**
< http://theconversation.com/coronavirus-south-koreas-success-in-controlling-disease-is-due-to-its-acceptance-of-surveillance-134068>

South China Morning Post. "China's government orders inquiry into sale of counterfeit baby milk formula." April 4, 2016. **https://www.scmp.com/news/china/society/article/1933512/chinas-government-orders-inquiry-sale-counterfeit-baby-milk**

< https://www.scmp.com/news/china/society/article/1933512/chinas-government-orders-inquiry-sale-counterfeit-baby-milk>

.

Stevenson, Alexandra, and Paul Mozur. "China Scores Businesses, and Low Grades Could Be a Trade-War Weapon." The New York Times. September 22, 2019. **https://www.nytimes.com/2019/09/22/business/china-social-credit-business.html**

< https://www.nytimes.com/2019/09/22/business/china-social-credit-business.html>

.

Tanner, Murray S. "Beijing's New National Intelligence Law: From Defense to Offense." Lawfare. July 20, 2017. **https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense**

< https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense>

.

The Economist. "China Invents the Digital Totalitarian State." December 17, 2016. **https://www.economist.com/briefing/2016/12/17/china-invents-the-digital-totalitarian-state**

< https://www.economist.com/briefing/2016/12/17/china-invents-the-digital-totalitarian-state>

.

The Economist. "One of China's Poorest Provinces Wants to Be a Tech Hub." May 31, 2018.

https://www.economist.com/china/2018/05/31/one-of-chinas-poorest-provinces-wants-to-be-a-tech-hub

< https://www.economist.com/china/2018/05/31/one-of-chinas-poorest-provinces-wants-to-be-a-tech-hub>

.

The Financial Times Editorial Board. "AI in law enforcement needs clear oversight." The Financial Times. May 7, 2019. **https://www.ft.com/content/2fb20144-6d94-11e9-a9a5-351eeaef6d84**

< https://www.ft.com/content/2fb20144-6d94-11e9-a9a5-351eeaef6d84>

.

Thompson, Stuart A. and Charlie Warzel. "How to Track President Trump." The New York Times. December 20, 2019. **https://www.nytimes.com/interactive/2019How%20to%20Track%20President%20Trump/12/20/opinion/location-data-national-security.html**

< https://www.nytimes.com/interactive/2019How%20to%20Track%20President%20Trump/12/20/opinion/location-data-national-security.html>

.

Trevaskes, Susan. "Public Sentencing Rallies in China: The Symbolizing of Punishment and Justice in a Socialist State." Crime, Law & Social Change, vol. 39 (2003).

Triolo, Paul, et al. "Translation: Chinese Government Outlines AI Ambitions through 2020." New America. January 26, 2018. **https://www.newamerica.org/cybersecurity-**

initiative/digichina/blog/translation-chinese-government-outlines-ai-ambitions-through-2020/

< http://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinese-government-outlines-ai-ambitions-through-2020/>

.

United Nations Conference on Trade and Development (UNCTAD). 2016. Data Protection Regulations and International Data Flows: Implications for Trade and Development.

United States Congress. Report of the Select Committee on Intelligence United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election: Russia's Use of Social Media with Additional Views. 2019.

Wall Street Journal. "China Deploys Drones, Citizens and Big Data to Tackle Coronavirus." March 5, 2020. **https://www.wsj.com/video/china-deploys-drones-citizens-and-big-data-to-tackle-coronavirus/40590C07-FB56-46CE-8C25-72471A5ECD39.html**

< https://www.wsj.com/video/china-deploys-drones-citizens-and-big-data-to-tackle-coronavirus/40590C07-FB56-46CE-8C25-72471A5ECD39.html>

.

Wang, Hao. Protecting Privacy in China: A Research on China's Privacy Standards and the Possibility of Establishing the Right to Privacy and the Information Privacy Protection Legislation in Modern China. 2011. Springer: 34-53.

World Intellectual Property Organization. 2019. WIPO Technology Trends 2019: Artificial Intelligence. Geneva.

Yang, Jie. “The Politics of the Dangan: Spectralization, Spatialization, and Neoliberal Governmentality in China.” Anthropological Quarterly 84, no. 2 (2011): 508. doi:10.1353/anq.2011.0023.

Yin, Yijun. "Police Shut ‘Privacy Art’ Exhibit for Displaying Personal Data." Sixth Tone. Aptil 11, 2018. **https://www.sixthtone.com/news/1002073/police-shut-privacy-art-exhibit-for-displaying-personal-data**

< https://www.sixthtone.com/news/1002073/police-shut-privacy-art-exhibit-for-displaying-personal-data>

.

Jiang, Zemin. 2002. “Report at 16th Party Congress on Nov 8, 2002.” Ministry of Foreign Affairs of the Republic of China. **https://www.fmprc.gov.cn/mfa_eng/topics_665678/3698_665962/t18872.shtml**

< https://www.fmprc.gov.cn/mfa_eng/topics_665678/3698_665962/t18872.shtml>

.

Zhang, Hui. “Facial Recognition System Leaves Fugitives with No Place to Run, Say Guiyang Police.” Global Times. March 18, 2018, **https://www.globaltimes.cn/content/1093864.shtml**

< http://www.globaltimes.cn/content/1093864.shtml>

.

Zhang, Yu, et al. “Trust Fraud: A Crucial Challenge for China’s e-Commerce Market.” Electronic Commerce Research and Applications 12, no. 5 (2013): 299–308. doi:10.1016/j.elerap.2012.11.005.

Zhong, Yang. 2015. “Policy Implementation at County and Township/Town Levels” In Local Government and Politics in China: Challenges from Below, 138-143. Routledge.

中华人民共和国中央人民政府. “中共中央办公厅 国务院办公厅印发《关于加快推进失信被执行人信用监督、警示和惩戒机制建设的意见》.” September 25, 2016. **https://www.gov.cn/zhengce/2016-09/25/content_5111921.htm**

< http://www.gov.cn/zhengce/2016-09/25/content_5111921.htm>

.

中华人民共和国中央人民政府国务院办公厅. “国务院办公厅关于建立国务院社会信用体系建设部际联席会议制度的通知_2007年第16号国务院公报_中国政府网.” April 18, 2007. **http://www.gov.cn/gongbao/content/2007/content_632090.htm**

< http://www.gov.cn/gongbao/content/2007/content_632090.htm>

.

新华财经. “国务院社会信用体系建设部际联席会议简介.” December 8, 2017. **http://credit.xinhua08.com/a/20171208/1739791.shtml**

< http://credit.xinhua08.com/a/20171208/1739791.shtml>

.