Issue: China’s Big Data Sweep

China’s Big Data Sweep

By: Suzanne Sataline

Pub. Date: April 30, 2018
Access Date: April 25, 2024
DOI: 10.1177/237455680414.n1
Source URL: https://businessresearcher.sagepub.com/sbr-1946-106448-2887399/20180430/chinas-big-data-sweep

Will Beijing push the boundaries of social control?

Executive Summary

The Chinese government is moving beyond its well-developed system of internet censorship – the so-called Great Firewall – to harness technology and data for the purpose of tracking the behavior of individuals and of companies that operate in China. The government is creating a nationwide "social credit" system designed to rate every citizen, based on actions at work and in public as well as on personal financial transactions. The system has generated intense debate among China-watchers, with some calling it an ominous experiment in social control and others saying it is primarily an effort to thwart corruption and regulate corporations. Some experts doubt that the government currently has the capacity to create a mass-surveillance state, given the extensive technological integration needed. Despite such doubts, it seems clear that Chinese authorities are laying the groundwork for a sweeping system of data collection and monitoring.

Some key takeaways:

- China is the world's most restrictive country in limiting online activities, according to the human rights watchdog Freedom House.
- The techniques that the government employs to monitor its citizens include widespread use of surveillance cameras in public places, installation of iris scanners in restive regions and a rapidly expanding DNA database.
- China has made it clear that it expects all companies operating in the country, including foreign corporations, to aid the government by storing data locally and allowing authorities to access that information.

Full Report

Surveillance cameras, like this one atop the Great Hall of the People in Beijing, are part of China's expanding system of monitoring and control. (Photo by Getty Images)

After being sued by another firm over a contract dispute, Xie Wen's advertising company lost in court. He was ordered to pay $127,000, but Xie chose not to do so. Without notice, his name was added to a digital list of debtors, which other companies could access. That debt did not become an issue until Xie was rejected for a bank loan in 2016. Soon after, he was unable to buy a plane ticket online. [1]

"That is when I knew I was blacklisted," Xie said. [2]

Xie's name was included on the Chinese Supreme Court's list of "discredited" persons or entities, a database of nearly 9.6 million people who owe money. [3]

In China's digital world, a citizen's business or personal missteps can ripple with consequences.

China is famed for pioneering the "Great Firewall," a colloquialism for a massive state censorship endeavor that hovers over the country's 731 million online users. [4] Recently, the government has gone further. It now seeks to harness technology and data to track the behavior of companies and citizens in ways that would frighten most people in the West – with the likely intent of preventing social unrest, scholars and activists say. President Xi Jinping routinely preaches the need for stability in China; one of the great fears is that online activism could breed unrest. [5]

Such tactics may be preparing the nation for more systematic scrutiny. The government has indicated it is creating a national "social credit" system that will assign every citizen a rating based on behavior at work, in public and in financial dealings. [6] Some news accounts portray the enterprise as a vast experiment in social engineering to influence behavior and swiftly identify lawbreakers. [7] However, academics such as Jeremy Daum, a senior research scholar at Yale University's Law School, say the goal is to police corporate behavior and crack down on corruption.

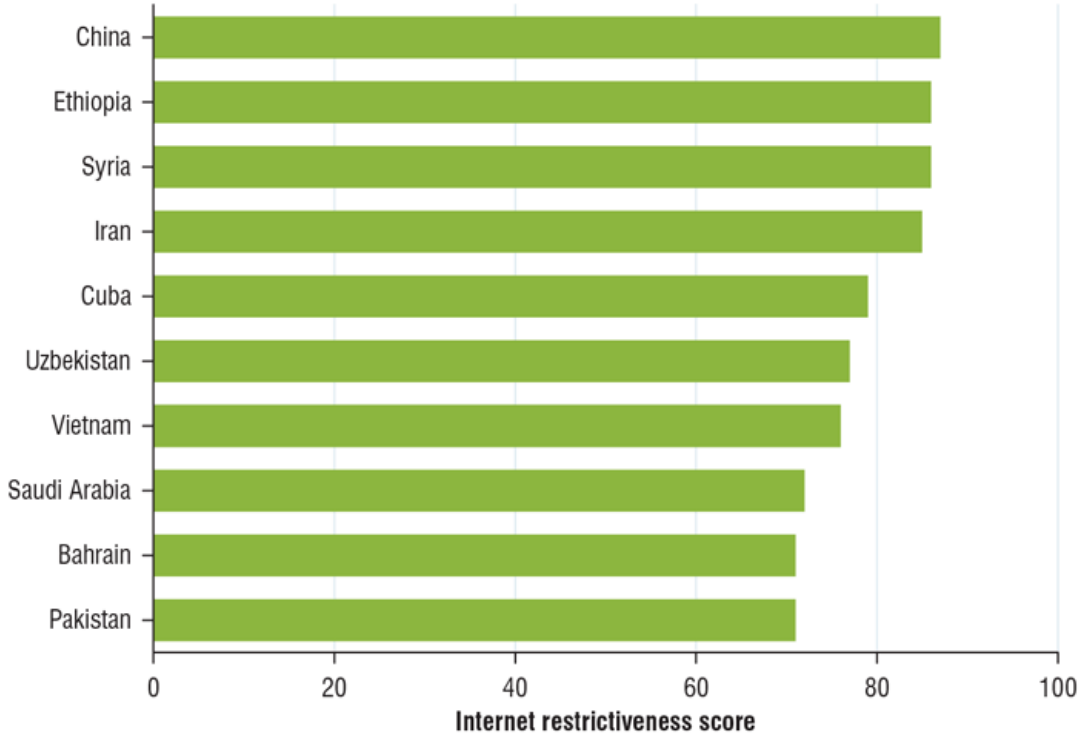
Daum and researcher Maya Wang at Human Rights Watch, a New York-based watchdog group, say they doubt that the government can create a nationwide, mass-surveillance state using technology. [8] And Anil Jain, the head of Michigan State University's Biometrics Research Group, said a world where every person is tracked by his face would require improved algorithms and more sophisticated cameras than what currently exists. [9]

To build the firewall, also dubbed the Golden Shield, more than a decade ago, the Chinese government depended on the technological expertise and investment of Western companies. [10] It no longer requires outside help to take the next step. New technology developed by Chinese companies will be used to monitor both Chinese and Western companies to ensure they comply with the law. [11] A new law instituted in June requires that companies follow strict requirements about data surveillance and storage. [12]

Under Xi, online use has become riskier. Freedom House, another human rights watchdog, says China restricts online activity more than any other country, including Syria, Cuba and Saudi Arabia. [13] In a recent report, the free speech group PEN America documented 80 cases in which police in China targeted citizens for their social media posts, says James Tager, deputy director of free expression research and policy at the New York-based organization.

China Ranked Most Restrictive Online

Countries with least internet freedom, 2017



Note: Scores are based on a scale of 0 (most free) to 100 (least free).

Source: "Freedom on the Net 2017: Table of Country Scores," Freedom House, May 31, 2017, https://tinyurl.com/y8gdpc3m

China is the most restrictive country in limiting internet freedom, followed closely by Ethiopia and Syria, according to a 2017 report by the democracy watchdog organization Freedom House. The group based its scores on an analysis of obstacles to internet access, limits on content and violations of user rights.

It is not completely clear how China's multiple control and monitoring systems fit together, or what they are designed to do. But researchers say some framework for a broad, sweeping system of data collection and surveillance is in place.

"China has historically sought to justify such measures on national security grounds, even though we could characterize them as being disproportionate and an abuse of citizens' human rights," says Jeremy Malcolm, senior global policy analyst at the Electronic Frontier Foundation, a digital rights and advocacy group based in San Francisco. "There are ways to circumvent these controls through strong encryption technologies, but circumvention itself poses risks for companies and foreign nationals working in China."

Even before Xi became president in 2013, members of the ruling Communist Party seemed determined to end the graft and theft that plagued the nation for decades. [14] Xi expanded this cleanup campaign and used it as a springboard to launch a much broader effort to suppress social problems and quash all opposition.

China's fast-growing tech sector gave officials many tools to control the country's population of nearly 1.4 billion. Deploying tech tools to control speech and organizing triggered protests from human rights groups. In 2015, Amnesty International, an international organization that advocates globally for human rights, said Chinese officials "are trying to rewrite the rules of the internet so censorship and surveillance become the norm everywhere. This is an all-out assault on internet freedoms." [15]

Today, there are two broad systems at work in China, according to Yale's Daum. One involves massive data collection and the other centers on pervasive surveillance. Both aim to control behavior and eliminate societal problems.

Data Collection Methods Expand

To maximize data collection, iris scanners have been installed at security checkpoints in restive regions and sophisticated software has been deployed to monitor social media posts. [16] Facial-recognition technology is becoming routine; authorities mine images from constellations of cameras at street corners, subway stations, airports and border crossings. [17] China has used expanded criminal punishments for spreading rumors online and what the government terms "internet speech crime" to prosecute journalists and lawyers. [18]

Human Rights Watch found through tender documents that Chinese police are using software applications to analyze voluminous amounts of online data, including text, video and pictures. [19] Chinese officials said this will help officers predict crime, search for suspects and operate more efficiently. [20] The rights group countered that some systems also will let police gather unprecedented details about ordinary people, including those accused of no wrongdoing. [21]

China's developing social credit system makes full use of this data. The intent is to combine information shared among different regions and departments, much of it public. [22] By rating citizens based on criteria ranging from shopping habits to online comments, the government intends to "manufacture a problem-free society," Wang wrote last year. "Those with low scores will face obstacles in everything from getting government jobs to placing their children in desired schools. It remains unclear exactly who will run the system, whether or how one could dispute scores, or even whether the system is legal." [23]

Daum, however, cautions that many media reports have exaggerated the dangers. He says the system China envisions is the nation's version of a credit report, like Equifax, and not a punitive system that will keep people who commit minor infractions from accumulating credit or traveling.

Another venture, called the "Police Cloud," is run by the Ministry of Public Security. It aims to collect a wide range of information on citizens, ranging from medical histories to supermarket membership and travel records. It is designed to reveal "where individuals have been, who they are with, and what they are doing, as well as make predictions about their future activities," according to Human Rights Watch. [24]

"The ambition to surveil everyone and to get as much data about them using technological means is a nationwide ambition for the Chinese government," says Human Rights Watch's Wang, who is based in Hong Kong. "Most Chinese people don't understand what's going on in China. These programs are secretive.… People cannot research it, they cannot talk about it."

An Amnesty International member protests Chinese internet censorship at a 2008 demonstration in Sydney. (Greg Wood/AFP/Getty Images)

Meanwhile, China is quickly expanding its DNA database. Police have a goal of almost doubling China's current DNA trove to 100 million records by 2020, according to a Wall Street Journal examination of documents from police departments across the country. To do that, they will need to gather almost as many records each year as are in the entire national DNA database the United States has built over two decades. [25] Critics such as Wang see this collection as an invasive form of social control.

In Xinjiang, a western province that is home to many members of China's Muslim minority, authorities require health checks that collect DNA samples and other biometric data from residents. [26]

A government ambition to link DNA profiles with real-time surveillance tactics, such as tools to monitor online use and camera footage used by facial-recognition software, will help China's Communist Party develop an all-encompassing "digital totalitarian state," said Xiao Qiang, adjunct professor at the University of California. Berkeley's School of Information. [27]

Surveillance: Companies Expected to Participate

Recent government moves show that China expects companies, including foreign ones, to join China's expanding surveillance engine. [28] Tech companies have long partnered with the Chinese government – either by censoring problematic content or helping finance new enterprises. [29] Regulations linked to the new cybersecurity law specify how companies must store and share data and detail criminal sanctions for violators. [30] The government is also hard on Chinese companies. It fined tech company Tencent, social media website Sina Weibo and other enterprises for online content that failed to meet "national standards." [31]

Chinese internet companies are required to help the government hunt down criminal suspects and silence political dissent, according to Beijing civil rights activist Hu Jia. [32] Unlike American corporations, which sometimes resist U.S. government requests for information, Chinese firms talk openly about working with authorities. "The political and legal system of the future is inseparable from the internet, inseparable from big data," Jack Ma, co-founder of online retail giant Alibaba, told a Communist Party commission overseeing law enforcement in 2016. [33]

Under President Xi, the government routinely searches online sites for information it considers "false rumors" and removes material it dislikes. [34] Website owners and social media companies are responsible for ensuring that their online content – including comments posted by users – meets government standards, and they censor posts that might violate those standards. [35]

It has become more common for Chinese authorities to investigate and punish people for imprudent comments made in messaging apps, even closed chats that users believed were private, a development that turns ordinary web users into censors. [36] In September,

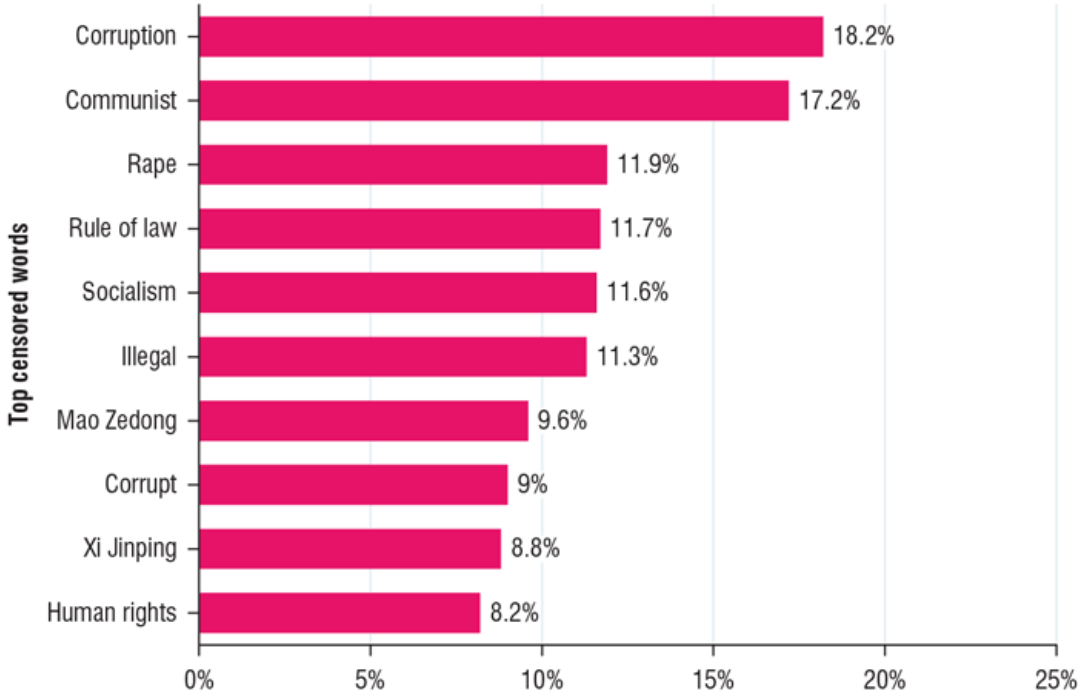
government officials said they would start making the creators of all private chat groups jointly responsible if they fail to police discussions to the authorities' satisfaction. [37] In this way, Chinese social media companies play a direct role in enforcement, one that is likely to expand.

Last September, internet services giant Baidu announced it was developing a system that would allow more than 300 police agencies to monitor and respond to "online rumors," including those appearing on blog posts, microblogs and online forums. [38] Users of social media who voice dissent or expose societal concerns, on topics ranging from labor rights to feminism to environmental issues, are constrained; they either self-censor or overt government actions block discussion of these issues, according to PEN America. [39] The group recommends that foreign social media companies should not enter the Chinese market, because doing so requires that they become an accomplice to human rights violations, including secret detentions and prosecutions. [40]

"There's really no way for foreign social media companies to operate without enabling, facilitating becoming a part of the censorship system," PEN America's Tager says.

China's Most Censored Word: Corruption

Percentage of censored WeChat posts containing certain words



Source: Eva Dou, "Jailed for a Text: China's Censors Are Spying on Mobile Chat Groups," The Wall Street Journal, Dec. 8, 2017, https://tinyurl.com/y8td4enc

The word most likely to trigger Chinese government censorship on the messaging and social media app WeChat was corruption, according to a 2015 report.

This steady government pressure, data collection and analysis have immediate implications for international companies.

China now expects foreign companies to store corporate and customer data in China. Daum says China is doing this to protect its national interests. "When the big war happens and it's a cyberwar, China is going to have a functioning internet and the rest of the world isn't. They've kept all servers at home," he says.

The cybersecurity law that took effect last year directs several government and military offices to build and coordinate a national data regulatory regime with implications for Chinese and foreign companies, said Samm Sacks, a senior fellow in the technology policy program at the Center for Strategic and International Studies, a Washington think tank. [41] The plans call for relying on the help of Chinese internet giants such as Alibaba and Baidu, and industry groups, including those that support greater use of artificial intelligence. [42]

In March, the National People's Congress, China's national legislature, eliminated term limits for Xi and also announced creation of several new agencies, including one tasked with rooting out corruption. [43] This agency, the National Supervision Commission, will have

more investigatory powers in some areas than the ruling Communist Party's Central Commission for Discipline Inspection, China's current top anti-graft agency. The new commission also will investigate public officials, especially administrators and managers who are not Communist Party members. [44]

"Xi Jinping regards these changes as positive because they will give an official fig leaf to a terrifying investigatory/punishment process that until now has been largely practiced by the party against party members," said Jerome A. Cohen, director of New York University's U.S.-Asia Law Institute. [45]

There already are few checks on police power in China. "If [the government] wanted to get into Apple's servers in the U.S., you'd have to get a warrant," Daum says. In China, he says, the request to search is handled by the police, meaning that investigative officers are supervised by their own colleagues.

Foreign companies that provide telecommunications or cloud services in China will be expected to participate more fully in the evolving system. [46]


Samm Sacks of CSIS

Many companies and groups in China routinely use virtual private networks (VPNs) to bypass censors and access services such as Google, which the government blocks. The VPN software also protects communications from hacking and surveillance. [47] The authorities imposed rules that require online traffic to move through channels licensed by Beijing. [48]

In recent months, foreign companies operating in China reported that their custom-built VPNs no longer worked. [49] The Financial Times reported in January that the Ministry of Industry and Information Technology was forcing Chinese and foreign companies to use expensive Chinese software to conduct internal business, which makes their data open to government snooping.

Such procedures have made it increasingly difficult for international companies and organizations to work in China, and many have complained about internet interruptions. [50]

Under orders to comply with government regulations, Apple in February started to store registered users' cloud data at a local company in Guizhou that is owned by the provincial government, giving government officials access to that information. [51]

Apple wasn't the first. China made the storage requirement after it said the nation needed to ensure the privacy of its citizens' data. [52] To comply, Amazon's web services unit sold computing equipment used for its cloud services in China to its local partner. [53]

"The ambition to surveil everyone is a nationwide ambition for the Chinese government."

In August of 2017, Apple also removed several VPN applications that had allowed users to circumvent China's internet censorship; dozens more were taken down in November. [54] The Electronic Frontier Foundation accused the company of aiding the Chinese government's censorship campaign that it said hurts small businesses and university researchers. [55]

After coming under fire from Senators Patrick Leahy, D-Vt., and Ted Cruz, R-Tex., Apple replied that it still offered more than 1.8 million apps in its App Store in China. "We believe that our presence in China helps promote greater openness," wrote Cynthia Hogan, Apple's vice-president for public policy. "We are convinced that Apple can best promote fundamental rights, including the right of free expression, by being engaged even where we may disagree with a particular country's law." [56]

Some companies have reacted to the government's requirements by withdrawing from the Chinese market. Google shut down its Chinese search engine in 2010 after learning that it and other companies had been targeted in a cyberattack originating in China. [57]

As it investigated, the company also learned that the Gmail accounts of several Chinese human-rights activists had been hacked. [58] Google chose not to comply with government requests that it filter its search results. Instead, it directed its Chinese traffic to an uncensored version of its search engine in Hong Kong, leading authorities in Beijing to block most Chinese users from accessing Google. [59]

Facebook has had a more convoluted history in China. Widely blocked in the country since 2009, the company has quietly developed tools that could be used to remove online posts from news feeds in specific geographic areas, or to let a third party – likely a Chinese company – block certain content from appearing on feeds. [60] That might allow the social media company to regain access to the world's biggest social media market, according to The New York Times. But unveiling a new censorship tool in China could subject Facebook to demands by Chinese authorities to suppress content from other countries, the Times said. [61]

The Future: Security Trumps Privacy

Daum says Chinese officials have made it clear "that they are willing to violate privacy and rights for technology and security" and want to convince the world that extensive surveillance and reporting make their society work better. Among many people outside of China, he says, "there's almost a mythos of the incredibly efficient China model. Anyone who lives in China knows that's poppycock."

Malcolm of the Electronic Frontier Foundation cautions that China does not have a monopoly on internet surveillance and restrictions. "The United States does a lot of surveillance," he says. "It's a little hypocritical to set up a binary between free countries and oppressive countries. We can't say it's just Russia and China that are the bad guys."

About the Author

Suzanne Sataline is an independent journalist who lives in Hong Kong and the New York region. As a 2017 fellow at the Alicia Patterson Foundation, she began to research a book about Hong Kong politics. She is a graduate of Columbia University's Masters of Fine Arts program and was a Nieman fellow at Harvard University. She is a regular contributor to Foreign Policy's website and has published in The New York Times, The New Yorker.com, The Economist, The Guardian, The Washington Post, Popular Science and National Geographic. She previously reported for SAGE Business Researcher on China's economic slowdown, Chinese living abroad and Hong Kong's economy.

Chronology

1950-1999	**Post-revolutionary China begins to monitor its citizens.**
1950s	The Chinese government under Mao Zedong compiles a dossier – or *dang'an* – on each worker as a form of social control, recording moves to new jobs, large purchases and foreign friendships. The *hukou*, or household registration, records residency.
1978	Chinese leader Deng Xiaoping adopts economic reforms opening China to the outside world. He creates special economic zones in some cities to attract foreign business and engage in market-orientated trade.
1998	The government begins work on the Golden Shield Project – also known as the Great Firewall of China – to block websites that the Ministry of Public Security deems a threat to Communist rule.
1999	Jack Ma, a former schoolteacher, starts the Alibaba Group, which eventually consists of 25 internet-based businesses that include online marketplaces, retail payment platforms, a shopping search engine and data-centric cloud computing services. Online shopping website TaoBao, an Alibaba subsidiary with 16 million vendors, is managed through Alibaba's proprietary credit scoring model that uses big data to understand client behaviors.
2000-2011	**Foreign tech firms face pressure.**
2000	The government unveils the Golden Shield project and also announces plans to link national, regional and local security agencies in a nationwide digital surveillance network that will have immediate access to records on every citizen in China.… From 2000 to 2006, Beijing's Zhongguancun technology park registers an average of two new firms created each workday by Chinese nationals who earned degrees overseas.… Foreign investors begin pumping millions of dollars into Chinese tech firms.
2003	The government creates a national DNA database as a crime-fighting tool.
2006	Google agrees to censor its search results in China.… A U.S. congressional hearing discusses allegations that Yahoo, Microsoft, Google and Cisco collaborated with China on internet censorship.
2009	Chinese officials block Facebook to suppress information about riots in Xinjiang province that killed 140 people.
2011	After Chinese dissidents discuss online a movement similar to the "Jasmine Revolution," a popular uprising in Tunisia, Chinese officials detain many activists and deploy their massive censorship apparatus to block the word "jasmine" on the internet.… Chinese officials censor online news reports about a high-speed train crash in Wenzhou in eastern China.
2013-Present	**Regulation increases under Xi.**
2013	Xi Jinping becomes China's president.… Residents in Binzhou in eastern China are incensed when police take mouth swabs from about 3,500 students, presumably for DNA samples, while investigating the theft of cellphones and computers on a college campus.

2014 Beijing's regulators reportedly plan to purge foreign technology from government agencies and state-owned enterprises, prompting complaints from companies in the United States and other countries.

2015 A draft of a Communist Party document refers to government plans to build a "social credit system." … Seventeen U.S. trade groups representing most segments of the tech sector ask U.S. officials to press Beijing to reverse new policies that require companies working in China to submit proprietary software source code to Chinese officials.

2016 China announces plans to impose a sweeping cybersecurity law in 2017 that will require all online companies to store internet logs and relevant data in China for at least six months to assist law enforcement.… University of Toronto researchers discover that users of WeChat, the Chinese social media app, are not notified when their messages are censored, a government strategy aimed at quashing political gatherings.

2017 A new regulation holds internet companies accountable for breaches of content rules and requires them to establish credit rating systems for chat group users, among other things.… Apple removes applications from its app store in China that had allowed users to evade internet censorship by Chinese officials. Amazon also capitulates to China's censors when a Chinese company that operates Amazon's cloud services tells local customers to cease using software that would breach China's firewall.

Resources for Further Study

Bibliography

Books

Roberts, Margaret E., "Censored: Distraction and Diversion Inside China's Great Firewall," Princeton University Press, 2018. A scholar uses digital data and propaganda leaks to examine how censorship influences public life in China.

Walton, Greg, "China's Golden Shield: Corporations and the Development of Surveillance Technology in the People's Republic of China," Rights & Democracy, 2001. A cybersecurity expert explains China's massive online surveillance project.

Articles

Chin, Josh, "About to Break the Law? Chinese Police Are Already On To You," The Wall Street Journal, Feb. 27, 2018, https://tinyurl.com/ya5gbh35. A journalist explains how China is amassing data to tamp down ethnic opposition in the Xinjiang region.

Dou, Eva, "Jailed for a Text: China's Censors Are Spying on Mobile Chat Groups," The Wall Street Journal, Dec. 8, 2017, https://tinyurl.com/y8td4enc. Authorities in China today use the internet and other technology to identify behavior and opinions that once were revealed by informants.

Sacks, Samm, Paul Triolo and Graham Webster, "Beyond the Worst Case Assumptions on China's Cybersecurity Law," New America, Oct. 13, 2017, https://tinyurl.com/y8lhtf8y. Technology experts at two Washington think tanks analyze China's latest attempt to regulate online data.

Sacks, Samm, "New China Data Privacy Standard Looks More Far-Reaching than GDPR," Center for Strategic & International Studies, Jan. 29, 2018, https://tinyurl.com/yawzo384. A scholar explains China's new guidelines on information and data protection.

Reports and Studies

"China: Big Data Fuels Crackdown in Minority Region," Human Rights Watch, Feb. 26, 2018, https://tinyurl.com/y9expjdj. An international human rights group details how Chinese authorities are using big data to monitor a largely Muslim population in northwestern China.

"China: Police 'Big Data" Systems Violate Privacy, Target Dissent," Human Rights Watch, Nov. 19, 2017, https://tinyurl.com/y8fkbj6o. The human rights organization examines China's Police Cloud surveillance system.

"Forbidden Feeds: Government Controls on Social Media in China," PEN America, March 13, 2018, https://tinyurl.com/y8ehnypb. The New York-based free speech advocacy group documents instances of social media censorship in China.

"Giving Credit 3: Inputs and Outputs," China Law Translate, Jan. 15, 2018, https://tinyurl.com/yd8e8zgm. Yale scholar Jeremy Daum translates and explains laws and rules governing a social credit system.

Triolo, Paul, et al., "China's Cybersecurity Law One Year On: An Evolving and Interlocking Framework," New America, Nov. 30, 2017, https://tinyurl.com/y7b9nujw. A group of security scholars explain and monitor China's 2017 cybersecurity law.

The Next Step

Facial Recognition

Schmitz, Rob, "Facial Recognition In China Is Big Business As Local Governments Boost Surveillance," NPR, April 3, 2018, https://tinyurl.com/y77pkcws. Increasing demand from local governments for facial recognition technology is rapidly expanding the artificial intelligence industry in China.

Wang, Amy B., "A suspect tried to blend in with 60,000 concertgoers. China's facial-recognition cameras caught him," The Washington Post, April 13, 2018, https://tinyurl.com/yag7yk67. A man wanted by Chinese law enforcement was snapped up in the middle of a massive outdoor concert due to the quickly advancing facial recognition technology used in police surveillance.

Zuo, Mandy, "Chinese public toilets go hi-tech with Wi-fi and facial recognition," South China Morning Post, April 13, 2018, https://tinyurl.com/yava4ybw. Cities in China have started installing new technologies in public bathrooms, including facial recognition, which will dispense a set amount of toilet paper when an individual's face is scanned.

Public Backlash

Liao, Shannon, "China's microblogging platform Weibo reverses its decision to ban all gay content after online protests," The Verge, April 16, 2018, https://tinyurl.com/y8uzcvyv. China's version of Twitter reversed a ban on homosexual content on its platform in response to a vigorous outcry online from users.

Shih, Gerry, "Ethnic Uighurs Protest Chinese Security Crackdown," The Associated Press/U.S. News & World Report, March 15, 2018, https://tinyurl.com/y7dh2v5o. Members of a Chinese ethnic minority gathered worldwide to protest what they called the aggressive surveillance and security policing methods used by the government in China against their people.

Zhao, Christina, "On China's Weibo, It's Forbidden to Disagree With President Xi Jinping's Plan To Rule Forever," Newsweek, Feb. 27, 2018, https://tinyurl.com/ych5efv5. The words and phrases selected for censorship by the Chinese blogging platform Weibo serve as indicators of negative public opinion on the ruling Chinese Communist Party and President Xi Jinping, says the founder of an anti-censorship organization.

Organizations

American Chamber of Commerce in China
Floor 3, Gate 4, Pacific Century Place, 2A Workers' Stadium North Road, Chaoyang District, Beijing, 100027
+(8610) 8519-0800
http://www.amchamchina.org
amcham@amchamchina.org
Trade association representing 900 American businesses operating in China.

Australian Strategic Policy Institute
Level 2, 40 Macquarie St., Barton ACT 2600, Australia
+61 2 6270 5100
www.aspistrategist.org.au
A think tank that provides research and advice to policymakers in Australia, especially on issues related to the Asia-Pacific region.

Center for Strategic and International Studies
1616 Rhode Island Ave., N.W., Washington, DC 20036
1-202-887-0200
www.csis.org
A think tank focusing on economic and international security issues, including cybersecurity and human rights.

Electronic Frontier Foundation
815 Eddy St., San Francisco, CA 94109
1-415-436-9333
www.eff.org
An advocacy group that seeks to preserve privacy, free expression and innovation on the internet through litigation, policy analysis, grassroots activism and technology development.

Human Rights Watch

350 Fifth Ave., 34th Floor, New York, NY 10118-3299
1-212-290-4700
www.hrw.org
A group including lawyers, journalists and academics that researches human rights conditions and advocates for freedom of online expression and against censorship.

New America
740 15th St., N.W., Suite 900, Washington, DC 20005
1-202-986-2700
www.newamerica.org/cybersecurity-initiative
A think tank focused primarily on technology and public policy; its Cybersecurity Initiative explores issues of security, data and digital information through partnerships with scholars and practitioners.

Yale Law School Information Society Project
127 Wall St., New Haven, CT 06511
1-203-432-4992
https://law.yale.edu/isp
A program that hosts interdisciplinary scholars from around the world exploring issues related to law, technology and society.

Notes

[1] Jennifer Pak, "Inside China's 'social credit' system, which blacklists citizens," Marketplace, Feb. 13, 2018, http://tinyurl.com/ya7uwdw7.

[2] Ibid.

[3] Ibid.

[4] "The Great Firewall of China," Bloomberg, Nov. 30, 2017, http://tinyurl.com/yavnjdbo.

[5] Diana Fu, "The End of Activism in China?" Foreign Affairs, Aug. 2, 2017, http://tinyurl.com/ydfpzoem.

[6] Samm Sacks, "New China Data Privacy Standard Looks More Far-Reaching than GDPR," Center for Strategic & International Studies, Jan. 29, 2018, http://tinyurl.com/yawzo384.

[7] Josh Chin and Liza Lin, "China's All-Seeing Surveillance State is Reading Its Citizens' Faces," The Wall Street Journal, June 26, 2017, http://tinyurl.com/ycgv8ov5.

[8] Paul Triolo, et al, "China's Cybersecurity Law One Year On: An Evolving and Interlocking Framework," New America Foundation, Nov. 30, 2017, http://tinyurl.com/y7b9nujw.

[9] Chin and Lin, op. cit.

[10] Greg Walton, "China's Golden Shield: Corporations and the Development of Surveillance Technology in the People's Republic of China," International Centre for Human Rights and Democratic Development, 2001.

[11] Sacks, op. cit.

[12] "China to implement cyber security law from Thursday," Reuters, May 29, 2017, http://tinyurl.com/y8bbksba.

[13] "Manipulating Social Media to Undermine Democracy: Freedom on the Net 2017," Freedom House, last assessed April 23, 2018, http://tinyurl.com/y77gbb7c.

[14] Willy Wo-Lap Lam, "Growing CCDI Power Brings Questions of Politically Motivated Purge," The Jamestown Foundation, Feb. 4, 2015, http://tinyurl.com/yb6fppop.

[15] "Tech Companies Must Reject China's Repressive Internet Rules," Amnesty International, Dec. 15, 2015, http://tinyurl.com/y8c2gm34.

[16] "China: Minority Region Collects Data from Millions," Human Rights Watch, Dec. 13, 2017, https://tinyurl.com/ycg5v9s2.

[17] "China: Big Data Fuels Crackdown in Minority Region," Human Rights Watch, Feb. 26, 2018, http://tinyurl.com/y9expjdj.

[18] Jeremy Daum, "If you don't have anything nice to say…," China Law Translate, June 20, 2014, http://tinyurl.com/ybetj6h3.

[19] "China: Police 'Big Data' Systems Violate Privacy, Target Dissent," Human Rights Watch, Nov. 19, 2017, http://tinyurl.com/y8fkbj6o.

[20] Ibid.

[21] Ibid.

[22] “Giving Credit 3: Inputs and Outputs,” China Law Translate, Jan. 15, 2018, http://tinyurl.com/y83twqan.

[23] Maya Wang, “China’s Chilling ‘Social Credit’ Blacklist,” The Wall Street Journal, Dec. 11, 2017, http://tinyurl.com/yc3dj8ue.

[24] “China: Police ‘Big Data’ Systems Violate Privacy, Target Dissent,” op. cit.

[25] Wenxin Fan, Natasha Khan and Liza Lin, “China Snares Innocent and Guilty Alike to Build World’s Biggest DNA Database,” The Wall Street Journal, Dec. 26, 2017, http://tinyurl.com/y7aju33v.

[26] “China Building DNA Database by Controversial Means,” China Digital Times, Dec. 28, 2017, http://tinyurl.com/y9om3qfx.

[27] Fan, Khan and Lin, op. cit.

[28] Shelly Banjo, “China Protectionism Creates Tech Billionaires Who Protect Xi,” Bloomberg, March 7, 2017, http://tinyurl.com/y89gbeoh.

[29] Ibid.

[30] Ibid.

[31] Ibid.

[32] Liza Lin and Josh Chin, “China’s Tech Giants Have a Second Job: Helping Beijing Spy on Its People,” The Wall Street Journal, Nov. 30, 2017, http://tinyurl.com/ycxuqbcc.

[33] Ibid.

[34] “Forbidden Feeds: Government Controls on Social Media in China,” PEN America, March 13, 2018, http://tinyurl.com/y8ehnypb.

[35] Ibid.

[36] Eva Dou, “Jailed for a Text: China’s Censors Are Spying on Mobile Chat Groups,” The Wall Street Journal, Dec. 8, 2017, http://tinyurl.com/y8td4enc.

[37] “China’s Great Firewall is rising,” The Economist, Jan. 4, 2018, http://tinyurl.com/y9twrbqy.

[38] “Forbidden Feeds: Government Controls on Social Media in China,” op. cit.

[39] Ibid.

[40] “Forbidden Feeds: Government Controls on Social Media in China,” op. cit.

[41] Sacks, op. cit.

[42] Triolo, et al., op. cit.

[43] Chris Buckley and Keith Bradsher, “China Unveils Superagencies to Fight Pollution and Other Threats to Party Rule,” The New York Times, March 13, 2018, http://tinyurl.com/y6vgvxx3.

[44] Ibid.

[45] Ibid.

[46] Triolo, et al., op. cit.

[47] Lucy Hornby, “China’s VPN crackdown is about money as much as censorship,” Financial Times, Jan. 22, 2018, http://tinyurl.com/ybg34ucn.

[48] Ibid.

[49] Ibid.

[50] Yuan Yang, Lucy Hornby and Emily Feng, “China disrupts global companies’ web access as censorship bites,” Financial Times, Jan. 16, 2018, http://tinyurl.com/ycoz3gka.

[51] “Learn more about iCloud in China,” Apple Inc., April 6, 2018, http://tinyurl.com/y7fw7bz9; “Local Firm to Take Over Apple’s iCloud in China,” China Digital Times, Jan. 10, 2018, http://tinyurl.com/ydakhdl5.

[52] Ibid.

[53] “Amazon Sells Hardware to Cloud Partner in China,” The Wall Street Journal, Nov. 14, 2017, http://tinyurl.com/y7lqpt9z.

[54] Tim Bradshaw, “Apple drops hundreds of VPN apps at Beijing’s request,” Financial Times, Nov. 21, 2017, http://tinyurl.com/yayegtfe.

[55] Amul Kalia and Eva Galperin, “Deciphering China’s VPN Ban,” Electronic Frontier Foundation, Aug. 2, 2017, http://tinyurl.com/ydbqp6dy.

[56] Bradshaw, op. cit.

[57] Kaveh Waddell, “Why Google Quit China – and Why It’s Heading Back,” The Atlantic, Jan. 19, 2016, http://tinyurl.com/y75f28ux.

[58] Ibid.

[59] Ibid.

[60] Mike Isaac, “Facebook Said to Create Censorship Tool to Get Back Into China,” The New York Times, Nov. 22, 2016, http://tinyurl.com/y7rjdezy.

[61] Ibid.