

Flygtningenævnets baggrundsmateriale

Bilagsnr.:	633
Land:	Kina
Kilde:	Freedom House
Titel:	Freedom on the Net 2021- China
Udgivet:	21. september 2021
Optaget på baggrundsmaterialet:	25. februar 2022

Document #2060883

Freedom House

Freedom on the Net 2021 - China

- NOT FREE

10

/ 100

A [Obstacles to Access](#) 8 / 25B [Limits on Content](#) 2 / 35C [Violations of User Rights](#) 0 / 40

LAST YEAR'S SCORE & STATUS

10 / 100 Not Free

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

Overview

Conditions for internet users in China remained profoundly oppressive, and confirmed the country's status as the world's worst abuser of internet freedom for the seventh consecutive year. During the coverage period, authorities censored calls for an independent investigation into the origins of the COVID-19 pandemic and criticism of Chinese-produced vaccines. Ordinary users continued to face severe legal repercussions for activities like sharing news stories, talking about their religious beliefs, or communicating with family members and others overseas. Separately, authorities yielded their immense power over the tech industry through new legislation, regulatory investigations, and administrative fines for alleged misuse of data. Despite the tighter constraints and risk of criminal penalties, investigative journalists, activists, bloggers, and ordinary internet users took courageous action calling for redress for government abuses, criticizing the authorities' response to the pandemic, and sharing information about other sensitive topics.

China's authoritarian regime has become increasingly repressive in recent years. The ruling Chinese Communist Party (CCP) is tightening its control over the state bureaucracy, the media, online speech, religious groups, universities, businesses, and civil society associations, and it has undermined its own already modest rule-of-law reforms. The CCP leader and state president, Xi Jinping, has consolidated personal power to a degree not seen in China for decades, but his actions have also triggered rising discontent among elites within and outside the party. The country's human rights movements continue to seek avenues for protecting basic liberties despite a multiyear crackdown.

Editor's Note: Tibet and Hong Kong are not covered in this report. Certain territories that are assessed separately in Freedom House's Freedom in the World report are excluded from the relevant country reports in Freedom on the Net, as conditions in such territories differ significantly from those in the rest of the country.

Key Developments, June 1, 2020 – May 31, 2021

- More mobile apps were blocked during the coverage period, including the encrypted communication platform Signal and the audio app Clubhouse. Authorities also intensified an ongoing crackdown on unapproved virtual private networks (VPNs), often prosecuting activists who provide access to them. These developments further restricted Chinese users' ability to communicate with people abroad via a secure medium (see B1, B2, and C3).
- Authorities censored calls for an independent investigation into the origin of the coronavirus, as well as criticism of Chinese-produced COVID-19 vaccines; continued prosecuting journalists and activists for reporting on the pandemic; and harassed family members of those who died of the virus for speaking up (see B2, B5, and C3).
- In January 2021, new restrictions on online self-publishing took effect. They require administrators of independently operated social media accounts to obtain a permit and to refrain from commenting on a list of restricted topics, and their enforcement has led to the removal of several accounts (see B2 and B6).

- As a result of intensifying controls, the online presence of independent civil society, human rights documentation, and prodemocracy viewpoints declined. Encouraged by authorities, the volume and aggressiveness of nationalistic voices continue to increase, contributing to more self-censorship (see B4 and B5).
- New legislation criminalized those who infringe on the reputation of “heroes and martyrs” and members of the armed forces, further restricting the scope of permitted speech. Violations can result in up to three years’ imprisonment (see C2).
- The ruling party launched a crackdown on entrepreneurs who refused to toe the party line. Prominent entrepreneur and anticorruption activist Li Huaqing was sentenced to 20 years in prison for “inciting subversion of state power,” with evidence including a handful of Li’s WeChat posts and private messages. In July 2020, property tycoon and party member Ren Zhiqiang was sentenced to 18 years in prison for corruption after publishing an online critique of Xi’s response to the pandemic (see C3).
- The government passed new rules and laws that more strictly regulate the ways that Chinese tech companies collect, store, and share users’ data, including the Personal Information Protection Law and the Data Security Law. Several companies were also investigated for allegedly misusing personal information (see C6).

A Obstacles to Access

A1 0-6 pts

Do infrastructural limitations restrict access to the internet or the speed and quality of internet connections? 6

According to the government’s China Internet Network Information Center (CNNIC), there were 989 million internet users in China—representing 70.4 percent of the population—as of December 2020.¹ That figure represents an increase of 85.4 million since March 2020. The number of users reaching the internet via mobile devices grew from 897 million to 986 million between March 2020 and December 2020; 99.7 percent of users access the internet via mobile devices.²

Internet speeds in China ranked below global averages in 2020. The country had a mean download speed of 2.09 Mbps, according to tests conducted by Cable.co.uk, earning it a rank of 200 among the 221 countries tested,³ although Chinese government sources reported significantly higher broadband speeds. In May 2020, the Ministry of Industry and Information Technology (MIIT) reported 93 percent of internet users in the country have access to fiber optics.⁴ Connection speeds in China are slowed by the government’s extensive censorship apparatus (see B1), which filters all cross-border traffic and makes the loading of content from foreign-hosted websites sluggish.⁵ Internet speeds vary significantly in different parts of the country. According to government data, the fastest available connections were in Shanghai,⁶ while the slowest were in less prosperous and more heavily censored regions such as Xinjiang.⁷

Chinese companies have been at the forefront of building and deploying 5G networks. In December 2020, the Ministry of Industry and Information Technology (MIIT) announced plans to build at least 600,000 more 5G base stations in 2021. As of March 2021, China had 910,000 5G base stations and 365 million devices connected to 5G networks.⁸

A2 0-3 pts

Is access to the internet prohibitively expensive or beyond the reach of certain segments of the population for geographical, social, or other reasons? 3

Internet access is relatively affordable for the average user, but other digital divides limit access for certain populations.

According to the China Academy of Information and Communication Technology (CAICT), the average monthly broadband expense in the fourth quarter of 2020 was 36.3 renminbi (\$5.60), and the average rate for mobile users was 3.75 renminbi (\$0.58) per GB.⁹

The digital divide between urban and rural areas narrowed during the coverage period: 68.7 percent of users were based in cities in December 2020, comparing with 71.8 percent in March 2020, according to government figures.¹⁰ As of December 2020, 416 million people did not have access to the internet, and 62.7 percent of those lived in rural areas.¹¹

A3 0-6 pts

Does the government exercise technical or legal control over internet infrastructure for the purposes of restricting connectivity? 6

The Chinese government maintains control over China’s gateways to the global internet, giving authorities the ability to cut off cross-border information requests in order to restrict connectivity or access to content hosted on servers outside the country.¹² This arrangement is the foundation for the “Great Firewall,” as the country’s comprehensive internet censorship system is informally known. All service providers must subscribe via the gateway operators, which are overseen by the MIIT. In June 2020, new Cybersecurity

Review Measures came into effect.¹³ Under these rules,¹⁴ all critical information-infrastructure operators must submit purchases of network products and services to a thorough national security review conducted by a government agency.¹⁵

The government has shut down access to entire communications systems in response to specific events. The most dramatic example occurred in 2009, when authorities imposed a 10-month internet blackout in Xinjiang—home to 22 million people—after ethnic violence in the regional capital, Urumqi.¹⁶ Since then, the practice has continued sporadically on a smaller scale.

Human rights activists and their families are sometimes subject to targeted network disconnections. For instance, in June 2020, police in Yunnan Province cut the internet and mobile services of the family of activist Wang Zang, preventing them from speaking out against the detention of Wang.¹⁷ In October 2020, authorities cut the internet connection as well as mobile service of Xin Na and her family in Hohhot after they protested the government’s policy to replace Mongolian as the medium of instruction in elementary and middle schools in the region of Inner Mongolia.¹⁸

Network shutdowns are often explained as national security precautions. The cybersecurity law and Article 84 of a 2015 antiterrorism law introduced fines and detentions of up to 15 days for telecommunications firms and internet service providers (ISP), as well as relevant personnel, who fail to restrict certain forms of content including “shut[ting] down related services” (see B3 and C2).¹⁹

A4 0-6 pts

Are there legal, regulatory, or economic obstacles that restrict the diversity of service providers? 1 / 6

State-owned China Mobile, China Telecom, and China Unicom dominate the mobile market,²⁰ though the government has authorized new players to enter the sector over the past few years.²¹ In January 2019, BT (formerly British Telecom) became the first foreign telecommunications company to receive permission to provide internet services across the country.²² In September 2020, the State Council approved a plan allowing foreign firms to own up to 50 percent in joint ventures providing virtual private network services for foreign companies in Beijing.²³

Authorities exercise tight control over cybercafés and other public access points, which are licensed by the Ministry of Culture in cooperation with other state entities.²⁴ Overall, internet cafés are no longer as popular as they once were, although many remain gathering venues for video gamers. The total number of cybercafés was estimated to be approximately 125,000 in February 2021. In 2020, just under 13,000 cybercafés were closed, partly due to restrictions implemented in response to the COVID-19 outbreak.²⁵

A5 0-4 pts

Do national regulatory bodies that oversee service providers and digital technology fail to 0 / operate in a free, fair, and independent manner? 4

Several government and CCP agencies are responsible for internet regulation at the local and national levels, but the system has been consolidated during Xi Jinping’s tenure.

The Cyberspace Administration of China (CAC)²⁶ and the CCP’s Central Cyberspace Affairs Commission oversee the telecommunications sector and regulate internet content.²⁷ The cybersecurity law in effect since 2017 identifies the CAC as the principle agency responsible for implementing many of its provisions.²⁸ The CAC reports to the Central Cyberspace Affairs Commission, a party entity that is headed directly by Xi Jinping, making it the highest authority on internet policy in China.²⁹ Since 2014, the commission has also overseen the CNNIC, an administrative agency under the MIIT that issues digital certificates to websites.³⁰

The CCP has exerted even greater control over the press, film, radio, and television industries in recent years, including online video and streaming services. Since administrative restructuring occurred in March 2018, more agencies involved in media regulation, including online content, have been directly subordinated to the CCP’s Central Propaganda Department, although several continue to report to the State Council. Regardless, the Central Propaganda Department plays a leading role with regard to enforcing CCP’s political and ideological priorities through online regulation.

Zhuang Rongwen has served as director of the CAC since mid-2018³¹ and continued in that position during the coverage period, while simultaneously serving as deputy director of the CCP’s Central Propaganda Department.³² Both entities frequently issue rules and instructions regarding technical, legal, administrative, or content dimensions of internet activity in China and in ensuring party control over online content.

B Limits on Content

B1 0-6 pts

Does the state block or filter, or compel service providers to block or filter, internet content, 0 / particularly material that is protected by international human rights standards? 6

The Chinese government’s Great Firewall is the world’s most sophisticated internet censorship apparatus. The content targeted for blocking, including major social media platforms, usually contains criticism of individuals, policies, or events that are considered integral to the one-party system. The breadth of the affected content is constantly growing, leaving Chinese users with access only to a highly censored, monitored, and manipulated version of the internet.

Drawing on Chinese government documents and websites, a January 2021 report by Ryan Fedasiuk of Georgetown University in the Jamestown Foundation’s China Brief estimated that China’s Cyberspace Affairs Commissions and Public Security Bureaus have spent \$6.6 billion on internet censorship since 2018, with \$5.75 billion of that being spent at the county or municipal level.³³

According to GreatFire.org—an anticensorship group that tracks filtering in China—as of mid-2021, at least 165 out of the top 1,000 most visited websites and social media platforms around the world were blocked in China.³⁴ Many international news outlets and their Chinese-language websites are blocked, such as those of the *New York Times*, Reuters, the *Wall Street Journal*, the Australian Broadcasting Corporation, and the British Broadcasting Corporation (BBC). The websites of independent Chinese-language news services from Taiwan, Hong Kong, and the Chinese diaspora—such as *Liberty Times* (Taiwan), *Apple Daily* (Hong Kong/Taiwan), *Initium* (Hong Kong), China Digital Times (United States), and New Tang Dynasty TV (United States)—were also blocked during the coverage period. In June 2020, amid tensions between China and India following clashes along the countries’ disputed border, the *Times of India* reported that China had blocked a number of Indian news websites.³⁵ The move seems to have come prior to the Indian government’s decision to ban dozens of Chinese apps, including TikTok, on national security grounds.³⁶

A wide range of other websites that might provide information critical of the Chinese government are also blocked, including those of human rights groups such as Amnesty International, Human Rights Watch (HRW), and Freedom House. In April 2021, authorities blocked the website of Centre for Strategic and International studies (CSIS), a Washington-based think tank.³⁷

Most international social media and messaging platforms are blocked in China, including Facebook, WhatsApp, Twitter, Instagram, YouTube, Telegram, Snapchat, Line, and Pinterest, among others.³⁸ In February 2021, authorities blocked the newly emerged mobile audio app Clubhouse, after thousands of users in China had flocked to the app to discuss detention camps in Xinjiang.³⁹ In March 2021, the government blocked the encrypted messaging app Signal.⁴⁰ The popular discussion forum Reddit was blocked in August 2018,⁴¹ while all languages of Wikipedia were blocked in late April 2019, probably as part of the censorship sweep associated with the Tiananmen Square crackdown anniversary.⁴² Previously, only the Chinese-language version of Wikipedia and individual pages on sensitive topics were inaccessible.⁴³ A number of Google services—including Maps, Translate, Calendar, Scholar, and Analytics—remained blocked in 2021. The long-standing blocks on international communications platforms have helped to enable the exponential growth of local services such as Tencent’s WeChat and Sina Weibo, which are subject to the government’s strict censorship demands (see B2).

Blocks on global search engines also severely limit the content available on the Chinese internet. Google’s search engine has been blocked since 2012,⁴⁴ while the Yahoo search function was blocked in September 2018.⁴⁵ Microsoft’s Bing has generally remained accessible due to its compliance with the government’s censorship requirements.⁴⁶ Nevertheless, Bing accounts for only 2.6 percent of the search engine market in China, which is dominated by the Chinese companies Baidu and Sogou, with their market share as of March 2021 being 75.5 percent and 15.3 percent respectively.⁴⁷ In October 2020, the Chinese internet security company Qihoo 360 released Tuber, an Android app that allowed China-based users to access some websites blocked in China. It required real-name registration and simultaneously censored searches for sensitive terms like “Tiananmen Square” and “Xi Jinping.” Despite these controls, government authorities took the app offline within days of its release, after over 5 million downloads.⁴⁸ Similarly, in November 2019, web browser Kuniao, which allowed China-based users to partially bypass internet censorship, was similarly taken offline within days of its release.⁴⁹

A minority of Chinese internet users (albeit tens of millions of users) are able to access blocked websites with circumvention tools, such as VPNs (see B7). However, the government has intensified its restrictions on these tools since 2017, when MIIT issued a ban on the use of unlicensed VPNs.⁵⁰ Service providers are barred from setting up VPNs without government approval, and illegal VPN operations have been increasingly targeted for closure or blocking (see C3).⁵¹ Blocks on VPNs typically escalate ahead of high-profile events, such as the annual plenary sessions of China’s legislature.⁵² VPN providers have noted that a growing technical sophistication of Chinese authorities has been reflected in VPN blocking incidents.⁵³

B2 0-4 pts

Do state or nonstate actors employ legal, administrative, or other means to force publishers, content hosts, or digital platforms to delete content, particularly material that is protected by international human rights standards?

The government requires locally hosted websites, social media platforms, and other tech companies to proactively monitor content, remove significant amounts of banned material, and close user accounts. They can face severe punishment for failure to comply. The scale of content removals, website closures, and social media account deletions continued to expand over the past year, reaching new types of platforms and

extending to topics that were previously uncensored. Content censored includes information recognized internationally as problematic, but also political, religious, cultural, and social issues deemed undesirable by the regime.

In March 2021, China’s National Radio and Television Administration published draft amendments to the Radio and Television Law that expand it to cover online video broadcasters and platforms.⁵⁴ It specifies nine types of banned content, including content that “endangers security,” “slanders Chinese culture,” or does not help youth “establish the correct world view.”⁵⁵

The cyberspace administration of China (CAC) regularly launches “rectification” and “clean-up” campaigns to pressure websites and social media platforms to more effectively police content. Separately, in 2020, Baidu reported deleting over 51.6 billion items deemed “harmful information,” a slight decrease from 53.2 billion in 2019.⁵⁶ According to a CAC report covering the second quarter of 2020, in addition to targeting “socially harmful content,” such as pornography and gambling, the CAC also targeted content that “endangers national security,” or is “politically harmful.” During this period, it suspended 281 websites, and shut down 2,686 websites and 31,000 accounts. In August, CAC shut down an additional 179,000 social media accounts.⁵⁷ In December 2020, the government pulled the travel app TripAdvisor from mobile app stores after it launched a new round of “clean-up” the internet campaign.⁵⁸

In November, the National Radio and Television Administration released new regulations for the country’s massive live-streaming industry, which features some 560 million users. The regulations include requirements that platforms notify authorities ahead of time of celebrity and foreigner appearances, and that they promote accounts that embody core socialist values. The administration also said that it would enforce the new regulations during a clean-up campaign in December, during which it would shut down platforms that do not comply.⁵⁹

Censors increasingly target “self-media,” a category that includes independent writers, bloggers, and social media celebrities (see B6). Overall, tens of thousands of these accounts have been shut down, delivering a major blow to one of the few remaining avenues for independent and critical news and analysis.⁶⁰

The authorities apply pressure to Chinese internet companies to tightly enforce censorship regulations or risk suspensions, fines, blacklisting, closure, or even criminal prosecution of relevant personnel. Such pressure has intensified under the cybersecurity law that took effect in 2017. During the coverage period, several major news and online portals were subject to short-term punitive suspensions, leading them to intensify their own efforts to control content. From June 10 to 17, 2020, the CAC imposed a suspension of the trending topics list for the popular Sina Weibo microblogging service, saying messages on the platform had been “disrupting online communication order” and “spreading illegal information.”⁶¹ In March 2021, the CAC reportedly ordered Microsoft’s LinkedIn to suspend new sign-ups for 30 days and undergo a self-evaluation for not censoring enough content during the annual legislative meetings in March.⁶² The company issued a statement on March 9 that it was “work[ing] to ensure we remain in compliance with local law.”⁶³

Faced with increasing state demands, major content-hosting companies have hired more human censors to purge “illegal” material and avoid penalties. Entire departments are often dedicated to content moderation and removals, with personnel controlling content on major apps—like the microblogging platforms Sina Weibo,⁶⁴ China’s top news app Jinri Toutiao,⁶⁵ and live-streaming app Kuaishou⁶⁶—numbering in the thousands.⁶⁷

As the number of smartphone users in China has skyrocketed in recent years, mobile phone apps have increasingly become a focus for censorship, content deletion, and forced removals, often at the behest of authorities. In October 2020, the CAC ordered companies operating mobile browsers to conduct a “self examination,” by November 9 to remove sensational headlines, rumors, and content that does not follow “socialist values,” or risk being shut down. The CAC specifically instructed companies to pay special attention to “self-media” accounts. Companies that received the order include Huawei, Alibaba, Xiaomi, and Tencent.⁶⁸ In March 2021, internet companies pulled Alibaba’s web browser, UC Browser, from Chinese Android app stores following a call by Xi Jinping on March 15 for regulators to “step up” regulation of the country’s growing technology companies.⁶⁹ In July 2021, after the coverage period, WeChat permanently suspended the accounts of over a dozen college LGBT+ groups.⁷⁰

Apple had since 2017 been blocking a list of sites generated by Tencent on its iPhone browser, restricting websites deemed politically sensitive by the CCP in much the same manner as it would combat malware or phishing content internationally.⁷¹ In June 2020, the Guardian reported that Apple had removed the podcast apps Pocket Casts and Castro from its Chinese app store after the creators refused to comply with government censorship directives.⁷² In March 2021, Apple’s China App store removed the viral face animator app Avatarify, which produced “deep-fakes” in which a person’s face is altered or replaced.⁷³ While Chinese state media reported that the app was removed due to privacy concerns, some netizens suspect that the real reason was the spoofs created of CCP politicians. In May 2021, *the New York Times* reported that since 2017, roughly 55,000 active apps have disappeared from Apple’s App Store in China, including hundreds of virtual private network (VPN) services.⁷⁴ As of August 2021, a website run by the anticensorship group Greatfire.org, which tracks the availability of apps in different countries, had identified 7,032 apps that were unavailable in Apple’s China store compared to other app stores, including over 170 news apps, as well as entertainment, gaming, sports, weather, and travel apps.⁷⁵

In June 2020, as Chinese activists around the world sought to use Zoom to commemorate the 1989 Tiananmen Square massacre, the company, following instructions from one of its employees who was secretly tied to the Chinese government, terminated sessions or accounts of organizers in the United States at the behest of the Chinese government.^{[76](#)}

Security officials have increasingly resorted to harassing and coercing users to delete content, particularly from Twitter, which is blocked in China. A small but savvy community of internet users access Twitter via circumvention tools, enabling participation in the types of conversations that are heavily censored within the Great Firewall. Official media outlets like the *People's Daily*, China Global Television Network (CGTN), and Xinhua News Agency actively use Twitter to reach global audiences, as do a growing number of Chinese diplomats and government spokespeople, even as most Chinese internet users are unable to access the platform. Over the past three years, numerous users faced reprisals for their Twitter activities including prison time, with many forced to delete their posts en masse (see C3 and C7).^{[77](#)}

Censored topics often involve breaking news related to the reputation of the party or officials, official wrongdoing, foreign affairs, health and safety, and civil society activism.^{[78](#)} Any negative or unauthorized content related to President Xi and the CCP is heavily censored. There is also consistent and systematic censorship of content that violates long-standing taboos on subjects such as the June 4, 1989, Tiananmen massacre; Taiwanese independence; and repression of ethnic minorities in Xinjiang and Tibet or of banned religious groups like Falun Gong in other parts of China. The CCP's Propaganda Department and its local subsidiaries issue almost daily instructions to news websites and social media platforms on what content to restrict.^{[79](#)}

In October 2020, the CAC issued a specific list of censorship instructions to social media and news platforms in preparation for the Fifth Plenum 19th Party Congress, asking that they “strengthen management” to find and delete banned content. Off-limits topics include speculation about power struggles and factions among CCP elite, critical coverage of China in foreign news outlets, comments that conflate stock market fluctuations with politics, and general negative commentary about CCP leadership and the PRC government system. It also instructed platforms to not prominently display news of violence or celebrity gossip, to strengthen publicity for important government speeches, and to seek approval before republishing any foreign information.^{[80](#)} Also in October, the CAC instructed broadcasters to only use official tapings of events covering the 70th anniversary of the Korean War, and to monitor comments sections.^{[81](#)}

In April 2021, censors deleted from WeChat and other websites an article written by former premier Wen Jiabao, with state news outlet refusing to publish it, likely due to its implicit criticism of Xi Jinping. The article provided rare insight into Wen's personal thoughts, with him writing, “China, in my vision, should be a country of justice and fairness.”^{[82](#)}

Content that criticizes the government's repression of free speech was also censored. In February 2021, censors deleted an article by Gao Yu, the deputy editor in chief at Caixin, that criticized how journalists trying to independently report information are targeted by both authorities and nationalistic “keyboard warriors.”^{[83](#)} In March, WeChat blocked an article from being shared that was posted by the British embassy and defended the international press. China's Foreign Ministry also summoned its author, Ambassador Caroline Wilson, for a meeting.^{[84](#)}

The COVID-19 pandemic, which first emerged in the city of Wuhan in Hubei province in late 2019, continue to be one of the most censored topics during the coverage period. In the run-up to the anniversary of the January 23 lockdown in Wuhan, censors deleted posts critical of the government's initial handling of the outbreak, including ones with terms like “first anniversary” and “whistleblower.”^{[85](#)} A Citizen Lab report found that over 2,100 keywords related to the virus were censored on WeChat between January and May of 2020, affecting tens of millions of posts. Banned keywords related to the virus itself, international criticism of the government's response to the pandemic, conspiracy theories concerning the virus' origin, and US domestic politics. ^{[86](#)}

Content related to marginalized ethnic, religious, and linguistic groups is also restricted. Keywords related to the persecuted Falun Gong spiritual group consistently appear on leaked lists of prohibited terms. Reference to the banned Church of the Almighty God spiritual groups are also reportedly marked as politically sensitive by censors employed by mobile phone services, with users facing account deactivation for sharing religious information.^{[87](#)} Following the coronavirus outbreak in January 2020, reports emerged of Christian congregations being prevented from conducting live-streamed meetings and of individual parishioners being compelled to delete religious imagery from their social media accounts.^{[88](#)} Many Cantonese live streamers using ByteDance's popular Douyin app (the Chinese version of TikTok, which has 400 million daily active users)^{[89](#)} have been banned for not broadcasting in Mandarin.^{[90](#)}

LGBT+ content has been heavily restricted on China's internet since 2017, when the China Netcasting Services Association labelled homosexuality as “abnormal sexual behavior.”^{[91](#)} The courts have upheld the restrictions in response to multiple legal challenges.^{[92](#)}

In July 2020, a music game by Taiwanese company Rayark was suspended from China’s app stores after it was discovered that Rayark’s musical director had published on SoundCloud a song with an oblique reference to Hong Kong’s protest movement.⁹³ In September 2020, the Ministry of Culture and Tourism released new guidelines for tighter control of artistic performances, including reviewing the content of performances and procedures for seeking approval.⁹⁴

Automation is also playing an increasingly important role in censorship. The University of Toronto-based research group Citizen Lab in August 2019 revealed image-filtering capabilities on the popular social media platform WeChat that targeted users’ creative efforts to circumvent text-based censorship through image-based commentary.⁹⁵ People.cn, the online version of the official CCP newspaper *People’s Daily*, has been improving its artificial intelligence-assisted censorship capabilities.⁹⁶ As of March 2020, Alibaba and Tencent had also emerged as industry leaders in content moderation and censorship technologies that intentionally target political content, selling the systems to other Chinese companies as well as foreign clients. The systems reportedly err on the side of caution for potentially politically sensitive content, sometimes removing even positive references to Xi Jinping.⁹⁷

After women spoke out in solidarity with feminist Xiao Meili, Weibo reportedly deleted her account and those of around 20 other women after they were doxed or otherwise attacked for defending Xiao (see B8). One of the women targeted, New York-based Liang Xiaomen, sued Weibo under China’s new Civil Code for deleting her account without providing an explanation or evidence of wrongdoing. Social media site Douban also deleted over 10 feminist groups on its platform, including groups tied to the 6b4t women’s empowerment movement that began in South Korea, and refers to women who choose to be single, refrain from sex, or decline to have children, among other things.⁹⁸

B3 0-4 pts

Do restrictions on the internet and digital content lack transparency, proportionality to the 0 / stated aims, or an independent appeals process? 4

Censorship decisions are arbitrary, opaque, and inconsistent, due to weak rule of law in China’s political system and because so many individuals and processes are involved. Regulations issued by government and CCP agencies establish censorship guidelines. The impact of content restrictions may vary depending on factors like timing, technology, and geographic region. ISPs reportedly install filtering devices differently, including in the internet backbone or even in provincial-level internal networks.⁹⁹ Lists of prohibited websites and sweeping censorship directives are closely held secrets, but are periodically leaked. There are no formal avenues for appeal and they cannot be challenged in the courts. Criticism of censorship is itself censored.¹⁰⁰ There is also no transparency surrounding private companies’ day-to-day censorship in China, and users similarly lack avenues for appeal.

Article 84 of a 2015 antiterrorism law introduced fines and detentions of up to 15 days for telecommunications firms and internet service providers, as well as relevant personnel, who fail to “stop transmission” of terrorist or extremist content, “shut down related services,” or implement “network security” measures to prevent the transmission of such content (see C2).¹⁰¹ The cybersecurity law in effect since 2017 also provides legal grounds for officials to instruct network operators to stop transmission of certain content to protect public security, among other restrictions (see A3).

The CAC and other bodies routinely introduce new rules and guidelines to further refine online restrictions, with an increasing focus on user-generated content (see B2).

B4 0-4 pts

Do online journalists, commentators, and ordinary users practice self-censorship? 0 / 4

Self-censorship among ordinary users and journalists is common, and takes place amid an increasing risk of account closures, real-world reprisals, and legal penalties for online commentary (see B2, C3, and C7). Various forms of online intimidation and verbal abuse by nationalistic netizens against government critics or others perceived to have harmed the reputation of China also contributed to self-censorship during the coverage period.

There is evidence that WeChat users are increasingly self-censoring to preempt the closure of their accounts or other penalties (see B2).¹⁰² With over a billion daily active users, WeChat is relied on for messaging, banking, ride hailing, ordering food, booking travel, and more.¹⁰³ The app’s critical role in daily life in China, alongside platform moderators’ growing propensity to close accounts rather than delete objectionable posts, has increased pressure on users to self-censor.

Self-censorship is pervasive among members of persecuted groups, especially Uyghurs, whose WeChat activities are closely monitored. Many block their own family members living abroad to avoid being detained for their foreign contacts.¹⁰⁴ In addition to encouraging pervasive self-censorship, this blunt form of punishment has narrowed avenues for civic mobilization and further suppressed online activism (see B8).

Despite these pressures, various examples emerged during the coverage period of internet users speaking out on sensitive topics. On June 4, 2020, users commented on the last post of late COVID-19 whistle-blower Li Wenliang on Weibo to obliquely commemorate the Tiananmen massacre. Since his death in February 2020,

Dr. Li’s final Weibo post has a place for frustrated citizens to express themselves.^{[105](#)} In September 2020, users criticized a ceremony honoring those who contributed to the fight against the coronavirus because it failed to recognize Li Wenliang.^{[106](#)}

B5 0-4 pts

Are online sources of information controlled or manipulated by the government or other 0 / powerful actors to advance a particular political interest? **4**

The government has significant control over digital news media and other information sources. Online discussion is subject to extensive manipulation, and user-generated content is highly regulated. Websites and social media accounts, other than those operated by official news outlets, are not legally allowed to produce news content, though the definition of what constitutes “news” is unclear. Propaganda officials systematically instruct internet outlets to amplify content from state media and downplay news that might generate public criticism of the government.^{[107](#)}

In March 2020, new rules called the Provisions on the Governance of the Online Information Content Ecosystem came into effect.^{[108](#)} These provisions place online content in three categories: encouraged positive content, discouraged negative content, and illegal content. Encouraged material includes “spreading party doctrine,” while negative categories include “excessive celebrity gossip” and sensationalist headlines. The illegal category includes terrorist and obscene content, as well as information “harming the nation’s honor and interests,” “subverting” the CCP regime, or challenging the government’s social, ethnic, religious, or economic policies.^{[109](#)} According to the rules, the encouraged content must be actively promoted in prominent online locations such as on web portal home pages, pop-up windows, hot topic lists, default search results, and other “key areas that can easily attract attention.”^{[110](#)} They also call for the use of algorithms by online content providers to promote officially approved “mainstream values.”^{[111](#)} Most actions required by the provisions have already been occurring for many years, but the new regulations consolidate them into a single set of rules.^{[112](#)}

Paid web commentators, known informally as the 50 Cent Party, are employed to post progovernment remarks and influence online discussions.^{[113](#)} Such commentators are known for reporting users who post offending statements, deliberately muddying the facts of particular incidents,^{[114](#)} and coordinating smear campaigns against government critics.^{[115](#)} According to a report released in December 2020, a robust government-funded industry of automated online commenting has emerged to flood social media platforms with desired posts, even under the direction of small local agencies.^{[116](#)}

Since 2017, content manipulation and disinformation campaigns have increasingly extended even to platforms that are blocked in China, demonstrating an ability to influence online discourse internationally.^{[117](#)} The Oxford Internet Institute reported that in 2019, the Chinese government displayed “new-found interest in aggressively using Facebook, Twitter, and YouTube” to spread propaganda and disinformation.^{[118](#)}

In addition to paid commentators, local authorities have mobilized *ziganwu*—volunteer commentators motivated by ideology rather than money—to promote the government’s image online.^{[119](#)} Their activity is part of a propaganda strategy to “spread positive energy among society.”^{[120](#)} A document leaked in 2015 revealed hundreds of thousands of “youth league online commentators” in China’s higher education institutions, tasked with turning students against supposed “Western” democratic values.^{[121](#)} In 2016, a handful of *ziganwu* were appointed to a social media division of the Communist Youth League.^{[122](#)} The league’s new media working group uses Weibo, WeChat, and other social media platforms to tailor political messages for younger audiences.^{[123](#)} In March 2021, sparked by a viral Weibo post from the Communist Youth League, a widespread campaign emerged supporting cotton from Xinjiang and denouncing international brands like Swedish clothing company H&M that pledged not to use it over forced labor concerns.^{[124](#)}

The government encourages Chinese tech companies to engage in “party-building” efforts to strengthen the “ideological security” of their firms.^{[125](#)} Alibaba, Weibo, Jingdong, Baidu, Sohu, Qihoo 360, and LeTV have had CCP branches within their companies since at least 2016, and many smaller enterprises have followed suit.^{[126](#)} Some tech leaders, including the founders of Tencent, Baidu, and Xiaomi, are delegates of China’s National People’s Congress and Chinese People’s Political Consultative Conference.^{[127](#)}

B6 0-3 pts

Are there economic or regulatory constraints that negatively affect users’ ability to publish 0 / content online? **3**

Growing censorship demands, licensing requirements, and data-localization mandates have made it more expensive to run an internet-specific company in China. While large companies have been able to absorb the rising operational costs, it is increasingly difficult for new and smaller players to enter and stay in the market. Arbitrary regulatory decisions have also contributed to an unstable investment climate for China’s technology sector.^{[128](#)}

Independent news media have been hit especially hard. Under CAC regulations on managing internet news and information services that came into effect in 2017,^{[129](#)} only traditional media or state-controlled enterprises may obtain a license to gather or disseminate news in any online format.^{[130](#)} Regulations in effect

since 2016 place restrictions on foreign investment in online publishing and require at least eight full-time editorial or publishing staff members.¹³¹ In addition, CAC rules have made it harder for both independent media and individual bloggers, journalists, and writers to sustain themselves financially.¹³² Commercial media outlets such as Caixin, known for relatively aggressive and investigative reporting, have suffered from falling profits due to censorship and ad hoc directives requiring major news portals and other aggregators to favor state media. Caixin was forced to introduce a paywall in 2017.¹³³

In January 2021, the CAC instituted a new set of restrictions on online self-publishing, requiring independently operated accounts to obtain a permit and prohibiting them from commenting on a list of restricted topics (see B2).¹³⁴

B7 0-4 pts

Does the online information landscape lack diversity and reliability? 1 / 4

China’s online information landscape is significantly less diverse than it had been before Xi Jinping came to power due to increasing censorship—especially of content produced by civil society activists, investigative journalists, and “self-media.” The strict censorship of critical viewpoints and foreign information sources has also empowered nationalist and conservative voices, contributing to their being disproportionately represented in Chinese cyberspace.¹³⁵ Nevertheless, the internet still provides narrow avenues for critical discussion and enables the sharing of information on some important social and political issues, particularly when users devise creative workarounds.

The stringent penalization of groups perceived as a political threat—including organizations, websites, and social media accounts that address human rights and social subjects such as labor activism, public health, and gender equality—has effectively diminished the space for civil society in recent years.¹³⁶ While groups that work on less sensitive issues have a vigorous online presence, organizations and topics that were tolerated in previous years—such as feminist groups—have faced increasing scrutiny. In some cases, netizens have been able to evade censorship through the use of wordplay to disguise discussion and expressions of support for activists, such as the prodemocracy protesters in Hong Kong.¹³⁷

Many members of marginalized ethnic, religious, and linguistic groups attempt to use the internet to disseminate banned content, but these views remain underrepresented online and those who post them risk severe reprisals, including imprisonment and torture, if they are identified as the source of content deemed politically sensitive. Amid the human rights crisis in Xinjiang, for example, Uyghur-language content and relevant news reporting have been heavily censored and many ordinary Uyghur users detained (see B2 and C3), while Islamophobic commentary is permitted to circulate widely.¹³⁸ Other, mostly Han Chinese religious and linguistic minority populations are also disproportionately silenced or restricted, limiting the diversity of content online (see B2).

Despite the tight censorship system, tens of millions of internet users—including from among persecuted minorities—bypass censorship with circumvention technology or creative workarounds. Although hundreds of VPN services have been banned since 2017 or removed from Apple’s iPhone App Store in China,¹³⁹ various options remain available in the country.¹⁴⁰

Within the Great Firewall, netizens deploy humorous neologisms, homonyms, and cryptic allusions to substitute for banned keywords, forcing censors to filter seemingly innocuous terms like “rice bunny,” which is pronounced “mi tu” in Mandarin and has become a well-known alternative for the intermittently censored #MeToo hashtag.¹⁴¹ The cartoon character Winnie the Pooh has also been systematically censored since it became a meme used to caricature Xi Jinping.¹⁴² For the past several years, the word “Xinjiang” and the human rights abuses documented across the region had been taboo on the Chinese internet. Netizens thus used “XJ” and “new jiang” (“xin” means new in Chinese) to try to circumvent censorship.¹⁴³

Although tolerance of investigative journalism has declined dramatically over the past decade,¹⁴⁴ some intrepid reporters continue to expose wrongdoing by companies and officials, focusing on topics that are less likely to draw censorship online and occasionally triggering national conversations. In July 2020, Guyu Story Lab, Tencent’s nonfiction media, published a story of a Tibetan woman who was burned to death by her ex-husband despite calling the police multiple times prior to her death; police had refused to intervene. The story exposed the long-standing problem of domestic violence and authorities’ lack of enforcement of anti-domestic violence laws. In September 2020, *People* magazine published a report shedding light on the lack of labor protections facing China’s delivery drivers. The story put a critical spotlight on two of China’s biggest online food delivery companies.¹⁴⁵

B8 0-6 pts

Do conditions impede users’ ability to mobilize, form communities, and campaign, particularly 1 / on political and social issues? 6

The role of social media in providing a vibrant space for activism in China has waned significantly due to stricter internet controls under Xi Jinping.¹⁴⁶ Growing censorship of popular apolitical platforms such as dating, video-sharing, live streaming, and blockchain applications in recent years has effectively closed avenues users had exploited to disseminate information and mobilize around topics that could not be discussed elsewhere.

Article 35 of the constitution guarantees free assembly and association, although they are not protected in practice. A November 2018 CAC regulation requires internet companies “of public-opinion nature” or which have “the capacity for social mobilization” to undergo “voluntary” assessments of how effective they are at preventing “security risks.”¹⁴⁷ Under the regulation, which includes a mechanism for on-site inspections, companies are obliged to keep detailed records of user data, such as real names, internet protocol (IP) addresses, activity logs, and the type of device used (see C6).¹⁴⁸

Activists continue to face harassment, arrest, and mistreatment in detention at the hands of the police (see C3 and C7).¹⁴⁹ Yet while overt activism on political issues is exceedingly rare, China's #MeToo movement continues to demonstrate that citizens can organize around select social causes, and that their efforts sometimes have a real-world impact. Despite heavy censorship of the global campaign, #MeToo encouraged a number of Chinese students to speak out online about their experiences with sexual harassment (see B7), leading to a few instances of positive change. China's new Civil Code, released in June 2020, bans sexual harassment,¹⁵⁰ a move seen as a response to numerous cases of professors harassing female students on college campuses across China.¹⁵¹ In December 2020, a court in Beijing heard a landmark case involving Zhou Xiaoxuan, who sued a prominent television-show host for sexually harassing her. Around 100 people gathered outside the court to support Zhou, after first learning about the case on Chinese social media.¹⁵²

In March and April 2021, women spoke out in solidarity with feminist Xiao Meili after her post on Weibo led to a stream of nationalistic and misogynistic trolling, ultimately resulting in Weibo deleting her account in late March (see B2).

Nascent attempts to advocate for labor rights and push for collective action against e-commerce companies took place during the coverage period. The efforts were led by delivery driver Chen Guojian, who recorded videos and set up WeChat groups to organize delivery drivers, who work with few protections.¹⁵³ However, Chen's disappearance in February and arrest in March 2021 seems to have quelled digital activism on the issue (see C3).

C Violations of User Rights

C1 0-6 pts

Do the constitution or other laws fail to protect rights such as freedom of expression, access to information, and press freedom, including on the internet, and are they enforced by a judiciary that lacks independence? 0 / 6

Article 35 of the constitution guarantees freedoms of speech and publication, but such rights are subordinated to the CCP's status as the ruling party. The constitution cannot be invoked in courts as a legal basis for asserting rights. The judiciary is not independent and closely follows party directives, particularly in politically sensitive cases involving freedom of expression.

C2 0-4 pts

Are there laws that assign criminal penalties or civil liability for online activities, particularly those that are protected under international human rights standards? 0 / 4

Numerous laws and regulations place strict limits on the activities of internet users and the companies that provide information and communication technology services. Prosecutors exploit vague provisions in China's criminal code; antiterrorism laws; laws governing printing and publications, subversion, and separatism; and state-secrets legislation to imprison citizens for online activity. Trials and hearings typically lack due process. It can take years for cases to move through the court system, with bail routinely denied and pretrial detention often long-lasting.

Laws prohibiting offenses including defamation, creating disturbances, illegal commercial activities, and extortion have implication for online speech.¹⁵⁴ Defamation has been interpreted to include “online rumors,” content deemed false, or online expression that “seriously harms” public order or state interests.¹⁵⁵ It carries a possible three-year prison sentence under “serious” circumstance, defined to apply when the content in question receives more than 5,000 views or is reposted more than 500 times.¹⁵⁶ Online messages deemed to incite unrest or protests are subject to criminal penalties under provisions punishing citizens for “picking quarrels and provoking trouble.”

Crimes such as “subversion” and “separatism”—as well as inciting such actions—can draw sentences as severe as life in prison, with members of religious and ethnic minorities periodically receiving life sentences when charged.¹⁵⁷ Article 300 of the criminal code punishes “using heterodox religion to undermine implementation of the law” and is often invoked against members of banned religious groups such as Falun Gong, whose members exercise their right to free expression and access to information online.¹⁵⁸ A 2015 amendment to the criminal code increased the maximum penalties from 15 years to life imprisonment.¹⁵⁹ The same 2015 legislation introduced penalties of up to seven years in prison for the dissemination of misinformation on social media.¹⁶⁰

An amendment to the criminal code that went into effect in March 2021 added a provision stipulating that those who “insult, slander, or infringe the reputation and honor of heroes and martyrs” can be held criminally liable and punished with up to three years' imprisonment.¹⁶¹ A law in June 2021 was introduced to ban “slander” of members of the armed forces.¹⁶²

Separately, the 2015 antiterrorism law bars social media users from sharing information about acts of terrorism or spreading “inhuman” images that could encourage copycat attacks (see B3 and C5).¹⁶³ The sweeping cybersecurity law that took effect in 2017 also increased censorship requirements (see C4 and C6).¹⁶⁴

In February 2020, amid the coronavirus outbreak, China’s top judicial and law enforcement agencies released new guidelines for judges, prosecutors, and others working in the legal system urging strong action against crimes seen as weakening disease-control efforts and undermining the CCP’s authority during the pandemic. Among the ten categories of crimes listed for tighter enforcement was “spreading false information and rumors online.” Besides false information related to the virus itself, the provisions also covered speech deemed to be “disrupting social order, especially maliciously attacking the party and government, taking the opportunity to incite subversion of state power, or overthrow of the socialist system.”¹⁶⁵ In addition to calling for punishment of individual users for proscribed speech under relevant provisions of the Criminal Law, the guidelines also warn that network service providers who refuse regulator demands to stop the spread of “false” or other “illegal” information should be prosecuted under the criminal code for not performing “the obligation of information network security management.”¹⁶⁶

Some detentions do not require approval by a court.¹⁶⁷ One form of administrative detention known as “reeducation through labor” was abolished in 2013 in response to domestic and international calls for reform,¹⁶⁸ but individuals can be detained without trial under similarly poor conditions in drug rehabilitation.¹⁶⁹ Chinese law also contains a form of criminal detention termed “residential surveillance at a designated location”¹⁷⁰ where police may hold individuals in secret locations without informing their families or legal counsel for up to six months.¹⁷¹

C3 0-6 pts

Are individuals penalized for online activities, particularly those that are protected under 0 / international human rights standards? **6**

Chinese citizens are regularly jailed for their online activities, including advocates of political reform, human rights workers, members of ethnic and religious minority groups, and ordinary users who express dissent or mock or criticize CCP leaders, particularly Xi Jinping. Chinese citizens’ risk of being detained or imprisoned for accessing or sharing information online or via smartphone has increased considerably over the past several years. Rapid advances in surveillance technology and growing police access to user data have helped facilitate the rise in arrests and prosecutions (see C5 and C6).¹⁷²

During the coverage period, authorities continued to detain or prosecute people for their speech related to the COVID-19 pandemic. The anonymous Twitter account @SpeechFreedomCN has tracked over 663 arrests for COVID-19-related speech between January 2020 and June 2021.¹⁷³ In September 2020, Hubei user Zhang Wenfang was sentenced to a six-month prison term for “picking quarrels and provoking trouble” for a poem she posted on Weibo about the pandemic.¹⁷⁴ In March 2021, retired professor Chen Zhaozhi went on trial in Beijing on charges of “picking quarrels and provoking trouble” for posting online that the “Wuhan pneumonia is not a Chinese virus, but Chinese Communist Party virus.” Prosecutors recommended a two-and-a-half-year sentence, but the trial ended without a verdict being pronounced.

Professional and citizen journalists in China are frequently imprisoned for their work and online writings or video posts, including those who reported on the pandemic and lockdown in Wuhan. According to the Committee to Protect Journalists (CPJ), at least 47 journalists were behind bars in China as of December 2020.¹⁷⁵ In December 2020, a Shanghai court sentenced lawyer turned citizen journalist Zhang Zhan to four years in prison for “picking quarrels and provoking trouble.” Zhang had covered the COVID-19 outbreak in Wuhan and had uploaded more than 120 videos to YouTube prior to her arrest in May 2020. While in detention, Zhang went on a hunger strike and was reportedly force fed by police.¹⁷⁶ As of August 2021, Chen Mei and Cai Wei, Beijing-based activists who were detained in April 2020 for archiving censored COVID-19 stories on GitHub, remained in detention awaiting trial.¹⁷⁷ The whereabouts of Wuhan businessman and citizen journalist Fang Bin, who was detained in early 2019 for reporting on the pandemic, remained unknown as of August 2021. In April 2020, in an unusually harsh sentence for an ethnic Chinese journalist, Chen Jieren was sentenced to 15 years in prison for publishing material critical of the Communist Party and exposing corruption in Hunan Province on WeChat.¹⁷⁸

Criticism or questioning the authority of Xi Jinping remains a particularly dangerous online activity. During the coverage period, several activists and lawyers faced detention or prosecution for overt or veiled critiques of Xi’s leadership. In July 2020, property tycoon and party member Ren Zhiqiang was sentenced to 18 years in prison on corruption charges after publishing an online critique of Xi’s response to the pandemic; many experts interpreted the punishment as a warning to Xi’s many critics within the party not to challenge his authority.¹⁷⁹ In December 2020, 24 teens and young adults were convicted of “picking quarrels and provoking disturbances” and “infringing on citizens’ personal information,” for posting political memes and leaking personal information about Xi Jinping’s family on the websites zhina wiki and esu.wiki. Niu Tengyu, 21, was accused of being the “main culprit,” and sentenced to 14 years in prison and fined 130,000 renminbi (\$19,800). He claims that he was tortured while in detention and forced to confess.¹⁸⁰

In February 2021, Rights Defense Network reported that it suspected that Dong Yaoqiong, known for live streaming herself splashing ink on a portrait of Xi Jinping in 2018, had been held in a psychiatric hospital after she posted to Twitter about government surveillance to which she was subjected.¹⁸¹ In December 2020, activist Ou Biaofeng was placed under “residential surveillance” in an undisclosed location after he posted one of Dong’s videos about her surveillance on Twitter.¹⁸² In July, Ou was formally arrested on charge of “inciting subversion.”¹⁸³

Activists and human rights lawyers were prosecuted for advocating for democracy, exposing police abuses, unionizing efforts, and other activities. In June 2020, a court in Jiangsu Province sentenced human rights lawyer Yu Wensheng to four years in prison and barred him from publishing publicly and serving in public positions for three years for “inciting subversion” (see C7).¹⁸⁴ Yu had been detained in January 2018 after posting online a call for constitutional reforms and democratic elections. In January 2021, authorities upgraded the charges against prominent rights lawyer Xu Zhiyong to “subversion of state power,” which carries a potential life sentence.¹⁸⁵ Xu was detained in February 2020 after he attended a dinner meeting of activists, but the nationwide effort to track him down appeared to accelerate after he published online a scathing letter¹⁸⁶ calling for Xi to step down over the government’s mishandling of the coronavirus. The case continued at the end of the coverage period. In February, Shandong police detained Xu’s partner, activist Li Qiaochu, for “inciting subversion.”¹⁸⁷

In April 2021, Beijing police arrested delivery worker Chen Guojian on charges of “picking quarrels and provoking trouble” for his labor-unionizing efforts.¹⁸⁸ Guo had recorded videos and set up WeChat groups to organize delivery drivers (see B8). His case remained pending at the end of the coverage period. In the same month, Shaanxi police charged human rights lawyer Chang Weiping with “subversion of state power,” which carries a potential life sentence. Chang had released a YouTube video detailing torture he reported suffering when detained in January 2020.¹⁸⁹

The CCP also launched a crackdown on prominent entrepreneurs who refused to toe the party line. In November 2020, a Chongqing Court sentenced entrepreneur and anticorruption activist Li Huaqing to 20 years in prison for “inciting subversion of state power.” The evidence cited was a handful of Li’s WeChat posts and private messages.¹⁹⁰ In July 2021, after the coverage period, a court in Hebei province sentenced billionaire Sun Dawu, head of Dawu Agricultural and Animal Husbandry Group, to 18 years in prison on charges including “picking quarrels and provoking trouble” and assembling a crowd to attack state agencies. Sun had openly accused the government of covering up a swine flu outbreak in 2019,¹⁹¹ and had previously supported detained activist Xu Zhiyong and praised the work of lawyers representing people who have criticized the ruling party, including online.¹⁹² He was first detained in November, along with his family and 20 executives for “picking quarrels and provoking trouble.”

Even members of the ruling party have been prosecuted for online posts critical of the government. In October 2020, Zhejiang Province official Ye Fuxing was expelled from the CCP and prosecuted for posting articles online that “vilified and slandered national leaders.”¹⁹³

An increasing number of internet users were detained for “unpatriotic” speech. At least seven people were detained in February 2021 for their online comments related to the release of the names of the Chinese soldiers who died in a border clash with India.¹⁹⁴ Former journalist Qiu Ziming was sentenced to a maximum three-year prison term for suggesting to his 2.5 million Weibo followers that the real death toll was higher than what was officially reported.¹⁹⁵

Users sharing information from or with foreigners were also penalized. In January 2021, a court in Guizhou province sentenced former journalist Zhang Jialong to one-and-a-half years in prison for “picking quarrels and provoking trouble” after he liked and retweeted messages critical of the CCP. (In 2014, in a meeting with US Secretary of State John Kerry, Zhang urged the US to help “tear down” the Great Firewall.¹⁹⁶) In July 2020, Chen Zong from Guangzhou was reportedly sentenced to 15 months in prison on charges of “picking quarrels” after he set up WeChat groups to share information he had collected from blocked overseas websites;¹⁹⁷ Chen had been detained in August 2019.

Authorities selectively enforce the ban on unapproved VPNs, often prosecuting activists who provide access to them—some who do so as a form of anticensorship activism. In June 2020, Chen Yuzhen was detained for “providing programs and tools for hacking computer network illegally” and “illegal controlling computer networks” after he shared his VPN login information with his friends.¹⁹⁸ In May 2020, a man was fined by local police in the city of Ankang, Shaanxi Province, for using a VPN to access content blocked by Chinese censors.¹⁹⁹

Authorities continued to selectively punish users for accessing or sharing information blocked by the Great Firewall. In July 2020, a court in Guangdong province sentenced Chen Zong to fifteen months in prison for “picking quarrels” after he set up WeChat groups to share information he had collected from blocked websites using a VPN.²⁰⁰ In November 2020, a Beijing court sentenced activist Zhang Baocheng to three-and-a-half years in prison for “picking quarrels and provoking trouble” and “promoting terrorism.” Prosecutors accused Zhang of using Twitter to defame the CCP.²⁰¹ In August 2021, a court in Anhui province sentenced Zhou Weilin to three-and-a-half years in prison. Zhou was convicted of “picking quarrels and provoking trouble” due to comments he made on Twitter and articles on human rights he produced for the Rights Defense Network website.²⁰²

A January 2021 *Wall Street Journal* investigation found that over the past three years, 58 Chinese users had been sentenced to prison for between six months and four years over posts on Twitter, Facebook, or YouTube.²⁰³ In December 2019, a man with 27 followers on Twitter was sentenced to 13 months in prison after he tweeted “glory to Hong Kong, shame on Communist bandits.”²⁰⁴

Members of persecuted religious and ethnic minority groups face particularly harsh treatment for their online activities. Since early 2017, a systematic Chinese government campaign has been underway to repress Xinjiang’s roughly 13 million Muslims through mass arbitrary detentions, intrusive surveillance, and torture.²⁰⁵ An estimated one million people are being held in political reeducation camps or forced labor facilities,²⁰⁶ some of whom were targeted for their online activities, including communication with relatives living abroad via WeChat.²⁰⁷

During the previous coverage period, reports emerged of prison sentences being imposed on some of these detainees. A leaked Chinese government document with details of dozens of Uyghurs and other Muslims jailed or taken away for reeducation in Xinjiang that was made public in February 2020 included in its list someone who was friends on WeChat with a Uyghur in Turkey, an individual who accidentally clicked on an overseas website on their phone, and a woman sentenced in August 2017 to 15 years in prison for making contact online with Uyghurs outside the country.²⁰⁸ There are also reports that ethnic Hui Muslims inside and outside Xinjiang have come under greater state surveillance and experience periodic detention.²⁰⁹ In January 2020, Cui Haoxin, a Hui Muslim poet, was detained by police in the city of Jinan, Shandong Province, for tweeting about repression in Xinjiang and charged with “picking quarrels and provoking trouble.”²¹⁰ That same month the *Washington Post* reported on the case of a Hui woman who was held at a reeducation camp for five months after she used a VPN to submit homework to the University of Washington when visiting her father in Xinjiang.²¹¹

Tibetans living outside the Tibetan Autonomous Region have also been targeted for sharing information on Chinese social media or overseas websites. In March 2021, police in Sichuan informed the family of Rinchen Tsultrim, a Tibetan monk, that he had been sentenced to four-and-a-half years in prison for “inciting separatism” over his WeChat remarks about Tibet and for speaking with Tibetans in exile.²¹²

People in Tibet, which is not factored in to this report’s scores (see Overview), also face prison terms for their online speech. In February 2021, Tibetan Kunchok Jinpa died in a Lhasa hospital while serving a 21-year prison sentence for “leaking state secrets” after being detained in 2013 for providing information to overseas websites about protests in Tibet.²¹³ In September 2020, four monks were tried in secret by the Shigatse Intermediate People’s Court and found guilty for, according to Human Rights Watch, one of three offenses: communicating online with Tibetans abroad, possessing images or literature related to the Dalai Lama, or sending money abroad.²¹⁴ Choegyal Wangpo was convicted to 20 years, Lobsang Jinpa to 19 years, Ngawang Yeshe to 5 years, and Norbu Dondrub, who also was critically beaten by police, to 17 years in prison.

Members of other religious minority groups are also prosecuted for their online and digital activities. Many Falun Gong practitioners have been jailed in recent years for posting messages about the spiritual group or human rights abuses on social media, accessing banned websites, and possessing or sharing prohibited VPN technology.²¹⁵

C4 0-4 pts

Does the government place restrictions on anonymous communication or encryption? 0 / 4

Under data-privacy legislation in effect since 2012 and additional rules that were implemented in 2017,²¹⁶ web service companies are required to register users under their real names and national ID numbers, compromising anonymity and placing communications at risk of direct government surveillance.²¹⁷ Chinese authorities introduced guidelines for online gamers in November 2019, requiring all players to register using their name and phone number.²¹⁸ In June 2020, the government also implemented real-name registration for online literature platforms, where many novelists have turned to discuss sensitive subjects in recent years.²¹⁹

Mobile phone registration requirements also greatly infringe on user anonymity, especially given that the majority of internet services require registration with a mobile phone number.²²⁰ The authorities justify real-name registration as a means to prevent cybercrime, but uploaded identity documents are vulnerable to theft or misuse.²²¹ In December 2019, new regulations took effect that require mobile phone users (which make up the vast majority of internet users in China) to have their faces scanned when registering for mobile phone services.²²²

The government’s tightening restrictions on VPN use and controls over available services has further reduced the options for user anonymity, while raising concerns that government approved VPN services would share user data with authorities.

Authorities in some areas have instructed public Wi-Fi providers to comply with user registration requirements.²²³ Cybercafés check photo identification, record user activities, and at times require facial scans, sometimes in cooperation with law enforcement. However, cybercafés are no longer as popular as they once were due to expanding broadband and mobile phone internet access, and are used mostly by gamers.

Laws also undermine encryption technology. The 2015 antiterrorism law requires companies to offer technical support to decrypt information at the request of law enforcement agencies, among other provisions.²²⁴ Regulations for the Administration of Commercial Encryption dating to 1999, and related rules from 2006, separately require a government regulator to approve encryption products used by foreign and domestic companies.²²⁵ In January 2020, a new Encryption Law took effect which requires critical information-infrastructure providers to apply for a review by the CAC if their use of encryption technologies is viewed as potentially impacting national security.²²⁶

In May 2021, the *New York Times* reported that Apple abandoned the encryption technology it typically uses when storing user data in China after the Chinese government prohibited the technology’s use (see C6).²²⁷

Measures that erode privacy disproportionately target groups that are perceived as threats to the regime. In Xinjiang, Uyghurs have been required since 2015 to register with their real names when purchasing electronic devices with storage, communication, and broadcast features. Stores selling such equipment are also required to install software that provides police with real-time electronic records on transactions.²²⁸

C5 0-6 pts

Does state surveillance of internet activities infringe on users’ right to privacy? 0 / 6

Direct surveillance of internet and mobile phone communications is pervasive and highly sophisticated, and privacy protections under Chinese law are minimal. In recent years, the Chinese government has increasingly moved toward big-data integration with the help of private companies, essentially consolidating in various databases a wide array of information on individuals, including their internet and mobile phone activities.

A new October 2020 study by ChinaFile provided clarity on the extent to which local officials have purchased intrusive surveillance technology.²²⁹ Through an examination of more than 76,000 local government procurement documents published between 2004 and May 2020, the study found that in 2019 alone authorities in one third of Chinese counties purchased surveillance equipment, including facial-recognition –enabled cameras, databases for storing citizen information and images, and Wi-Fi sniffers. Much of the equipment is connected to Project Sharp Eyes, which aims to cover all key public spaces in China by video surveillance.

In April 2021, users criticized a new app developed by the Ministry of Public Security designed to warn users of scam calls, texts, and apps, and voiced objections that they were forced to download the app in order to enter their residence buildings or to receive vaccinations by staff members. Though the app claims not to collect user data, users are required when registering to submit their name, national ID number, biometric facial data, address, and phone number, and must approve 29 access permissions including to cameras and microphones.²³⁰

When conducting investigations, the authorities have unfettered access to user communications and data on certain popular platforms, as indicated by reports of users being punished for their presumably private conversations, particularly on WeChat. In February 2020, authorities detained Chen Geng after he mentioned Falun Gong in a private message on WeChat.²³¹

Residents of Xinjiang are subject to severely invasive surveillance tactics. A leaked list of Uyghur detainees examined in a December 2020 report by Human Rights Watch showed how Chinese authorities are using big-data technology to arbitrarily detain Muslims in Xinjiang. Dated from late 2018, the list from Xinjiang’s Aksu Prefecture names 2,000 people flagged by the police’s Integrated Joint Operations Platform (IJOP) for surveillance and detention. Despite Chinese government claims that technologies like IJOP are only used against criminals, the research showed that the vast majority of the people on the list were targeted by police for nonviolent and mundane behavior like owning multiple cell phones, receiving phone calls from relatives in foreign “sensitive countries,” wearing religious clothing, using Skype, or studying the Quran. Some of the punished actions appear to have taken place years or even decades ago—such as studying the Quran in the mid-1980s, or staying overnight in another part of Xinjiang in 2013.²³²

Surveillance technologies and policies deployed in one part of China are often later expanded to other parts of the country, with Xinjiang emerging as a particularly important testing ground.²³³ Chinese border police are reported to have installed surveillance apps on the phones of tourists traveling in Xinjiang, which grant authorities the ability to extract user data and identify politically and culturally sensitive material stored on the person’s phone.²³⁴ In August 2019, reports emerged that Chinese border officers were beginning to check the photographs, messages, and apps on the phones of anyone arriving in China from Hong Kong for evidence of support for the prodemocracy protest movement in the city.²³⁵

Existing, albeit geographically disparate, data sets assembled through surveillance efforts could feed into “social credit” systems that create an assessment of individuals’ online activities and other personal data; a few municipalities are currently testing such systems,²³⁶ which have been subject to criticism within and outside China due to privacy and other concerns. Although a 2014 document referred to the full implementation of a vaguely defined “social credit” system by 2020,²³⁷ a fully integrated national social credit system does not yet exist and questions have been raised about how widespread and effective local pilot efforts have been.²³⁸ Nevertheless, being listed as problematic by municipal or provincial authorities under such systems can result in restrictions on movement, education, and financial transactions. By contrast, those

highly rated in Alibaba’s Sesame Credit scoring system or in municipal ratings of local governments like Xiamen and Fuzhou can win privileged access to private services, deposit waivers, free library book borrowing, or shorter lines at airport security.²³⁹

C6 0-6 pts

Does monitoring and collection of user data by service providers and other technology companies 0 / infringe on users’ right to privacy? 6

Internet-specific companies are required under numerous laws and regulations to assist the government in monitoring users’ online activities. Recent regulations include a September 2018 rule that provides security authorities with broad powers to enter the premises of all internet service companies to inspect and copy any information deemed important to cybersecurity.²⁴⁰ That rule formed part of the Provisions on Internet Security Supervision and Inspection by Public Security Organs, published by the Ministry of Public Security, which allows officials to supervise and inspect the “network security” of ISPs. The new regulatory package complemented the 2017 cybersecurity law’s requirement that network operators assist police and security agencies with criminal investigations or national security operations.²⁴¹ Inspections under the new rules began immediately.²⁴²

Other surveillance laws include a 2013 amendment to the criminal procedure code that lays out a vague review process for allowing police monitoring of suspects’ electronic communications, which the Ministry of Public Security permits in many types of criminal investigations.²⁴³ The State Secrets Law obliges telecommunications companies to cooperate with authorities investigating leaked state secrets, or risk losing their licenses.²⁴⁴

Individuals or entities that refuse to comply with government requests for surveillance assistance risk detention or criminal punishment. A National Intelligence Law adopted in 2017 states that those deemed to be obstructing national intelligence work can be subject to 15 days of administrative detention and further criminal charges.²⁴⁵

Various regulations outline requirements for companies to retain user data, which they must make available to officials.²⁴⁶ CAC rules issued in 2016 oblige Chinese app providers to register users and keep user activity logs for 60 days.²⁴⁷ Other ISPs are required to retain user information for 60 days and submit it to the authorities upon request, without judicial oversight or transparency.²⁴⁸

Tencent—the parent company of WeChat and QQ, two of the world’s most widely used social media platforms—directly assists the Chinese government with surveillance. Research by the University of Toronto’s Citizen Lab found in early 2020 that WeChat was monitoring messages and images sent by users registered outside of China, scanning them for politically sensitive key words and retaining the relevant conversations in order to train the platform’s censorship system.²⁴⁹

The e-commerce giant Alibaba also helps the government with surveillance. In October 2019, research published by the Open Technology Fund revealed evidence that the government’s Study the Great Nation app, which was designed by Alibaba to promote the CCP’s ideology and encourage the study of “Xi Jinping thought” in particular, was built with a back door that could grant the authorities access to users’ internet browsing histories, text messages, photos, and other personal information.²⁵⁰

Such private-government partnerships and apparent backdoors in effectively mandatory apps continued after the coronavirus struck, as regional officials partnered with major Chinese tech firms Alibaba and Tencent to develop “health code” apps. The prevailing software assigns individuals a QR code and low (green), medium (amber), or high (red) risk ratings depending on factors such as their location history and self-reported symptoms, although neither authorities nor the companies provide further information on how the risk levels are calculated. A green code is required to access certain public spaces and office buildings. Although there are variations among the dozens of apps used in each province or municipality, an analysis by the law firm Norton Rose Fulbright found that the privacy policy of Beijing’s app did not incorporate strong privacy-by-design principles or state any time limit on the retention of data.²⁵¹ A *New York Times* investigation showed that the Alipay Health Code app automatically shared data with the police.²⁵² As the initial outbreak was brought under control in China, certain health code apps were rolled back in cities like Shanghai. In March 2021, a new vaccine passport was launched on WeChat to track the health, testing, and vaccination records of Chinese citizens entering and exiting China.²⁵³ The use of a vaccine passport on WeChat is concerning in light of the app’s links to the government’s censorship and surveillance apparatus.

The 2017 cybersecurity law mandates that internet companies store the data of Chinese residents on servers based in the country, a practice that makes it easier for the government to access user information. Apple quickly complied with the requirement.²⁵⁴ In February 2018, Apple’s iCloud began storing the data of its Chinese users in partnership with Guizhou-Cloud Big Data, a state-run company.²⁵⁵ and a second data center is expected to open in Inner Mongolia.²⁵⁶ Apple has also complied with other obligations that facilitate government surveillance: in September 2018, it changed the hardware specifications of new iPhones for the Chinese market to comply with real-name registration rules and improve authorities’ ability to track user identities.²⁵⁷ A May 2021 report from the *New York Times* further clarified how Chinese government workers operate Apple-owned data centers in the country, detailing their physical control of computers and administration of other technology. The company also created a new legal agreement that allows it to bypass US law in order to share data with Chinese officials (see C4).²⁵⁸

In November 2020, the *Wall Street Journal* reported that a leading American executive for Airbnb resigned in late 2019 over concerns the company was sharing user data with Chinese authorities.²⁵⁹ The report revealed that, in the paperwork for Airbnb’s December initial public offering (IPO), the company stated that compliance with data requests from the Chinese government could result in its inability to operate in the country as well as harm to its reputation.

The government also seeks to proactively counter efforts to evade surveillance. In March 2021, the CAC announced that it started talks with 11 social media platforms, including ByteDance, Tencent, Alibaba, Xiaomi, and Kuaishou, to explore how to counteract deepfake technologies and voice-changing software, which is often used by activists to elude identification by government authorities.²⁶⁰ The platforms were instructed to report back with security assessments and improved risk-prevention and control measures for voice-based social media software, as well as deepfake technologies.

Several new government efforts were aimed to regulate how Chinese tech companies collect, share, and store users’ data. In August 2021, after this report’s coverage period, the Personal Information Protection Law (PIPL) was passed, with drafts released for public consultation in April 2021 and October 2020.²⁶¹ The law, which will apply to all organizations and individuals in China or seeking to access Chinese citizens’ data, is the country’s first comprehensive piece of legislation about the protection of personal information.²⁶² While some of its provisions come in response to Chinese users’ demands for greater protections, experts have criticized the law for not restraining the state surveillance system.²⁶³ It is set to go in effect in November 2021.

In March 2021, the CAC issued the Provisions on the Scope of Necessary Personal Information for Common Used Mobile Internet Applications, defining what constitutes “necessary personal information” that mobile internet applications can require consumers to provide.²⁶⁴ Regulators subsequently alleged that over 100 apps—including those from Chinese tech giants Tencent and Baidu—violated the rules.²⁶⁵ Separately, in July 2021, after the coverage period, authorities asserted that the ride-hailing app Didi illegally collected users’ personal information and the app was pulled from China-based app stores.²⁶⁶ In April 2021, regulators also fined Alibaba a record \$2.8 billion for using its algorithms and unfair access to data to further entrench its market position.²⁶⁷

In May 2020, the National People’s Congress passed the country’s first Civil Code, which included a provision that requires an individual’s consent for private companies to collect, share, or disclose their digital and biometric data. The provisions came amid growing public concern in China over data collection, hacking, and potential leaks by private companies.²⁶⁸

In June 2021, after the coverage period, the Standing Committee of the National People’s Congress passed the new Data Security Law,²⁶⁹ which will take effect in September 2021. The law imposes extensive data security obligations for businesses—not only regulating data processing and management activities within China, but also those outside of China that would purportedly harm China’s national security or public interest of Chinese citizens or organizations. It requires companies to obtain approval from the state prior to sharing data with a foreign judicial or law enforcement entity.

Chinese companies consistently ranked in the bottom half of the Rating Digital Rights evaluation of major tech companies’ policies around privacy.²⁷⁰ In its 2020 index, which covered 14 major digital platforms, Tencent, owner of WeChat, ranked 12th for privacy protections; Alibaba, affiliated with Ant Financial, ranked 9th; and Baidu ranked 8th.

C7 0-5 pts

Are individuals subject to extralegal intimidation or physical violence by state authorities or any other actor in relation to their online activities? **0 / 5**

Cases of extralegal intimidation and violence involving internet users are widespread. During the coverage period, instances including intimidation, aggressive interrogation, beatings, disappearances, and deaths from abuse in custody were reported.

Law enforcement officials frequently summon individuals for questioning in relation to online activity, an intimidation tactic referred to euphemistically as being “invited to tea.”²⁷¹ This includes activists who expressed opposition to the Chinese government’s attempts to exercise greater political control over Hong Kong.²⁷² Chinese users of Twitter and Line also encountered harassment and intimidation during the coverage period.

Activists have also been forced to travel within the country during sensitive political events, effectively keeping them away from their normal online activities.²⁷³ In June 2021, in the run up to the 32nd Anniversary of the Tiananmen Massacre, police forced activists across the country, including journalist Lu Yuyu, writer Zha Jianguo, activist Ji Feng, and academic Yang Shaozheng, to leave their residences for guarded “vacations,” barring them from communicating with others.²⁷⁴ Some activists have gone into hiding to avoid arrest. In August 2018, a young Uyghur man, Miradil Hesen, went into hiding after authorities noticed he had downloaded the blocked app Instagram to his cell phone. In September 2020, police in Jiangsu Province detained him after he also posted YouTube videos relaying the harassment, detention, and forced sterilization of his family members.²⁷⁵

According to Human Rights Watch, detainees in ordinary criminal cases face “physical and psychological torture during police interrogations, including being hung by the wrists, being beaten with police batons or other objects, and prolonged sleep deprivation.” In February 2020, Chinese Human Rights Defenders reported that “torture and cruel, inhuman and degrading treatment remained rampant in China in 2019.”²⁷⁶ Political and religious prisoners often experience even worse treatment.²⁷⁷ In August 2020, the lawyer of detained lawyer Yu Wensheng said Yu was tortured in detention and his health deteriorated drastically, including loss of his teeth and severe tremors leaving him unable to write with his right hand.²⁷⁸

Members of marginalized religious and ethnic minority groups are among the internet users most vulnerable to extralegal detention, torture, and killing. In Xinjiang, some of the estimated one million Uyghurs and other Muslims were taken to reeducation camps as a result of their online activities, such as downloading WhatsApp, possessing the contact information of prominent Uyghur scholars, or simply clicking on links on their mobile phones.²⁷⁹ Those detained or imprisoned typically suffer harsh conditions and often torture,²⁸⁰ resulting in long-term health problems and sometimes death.

People in Tibet, which is not covered by this report (see Overview), also face physical violence for their online activity. For example, Human Rights Watch reported in July 2021, after the coverage period, that Tibetan monk Choegyal Wangpo had been arrested and severely beaten in 2019 after police found his phone at a café, which contained WeChat messages to other monks in Nepal. The police then raided his village and detained approximately 20 other monks.²⁸¹

Online commentators expressing views critical of the Chinese government or deemed to harm China’s international reputation have in recent years faced increased bullying, harassment, and other real-world repercussions from nationalistic online users. For example, in July 2020, after the Chinese government ordered the US consulate in Chengdu to close, online trolls harassed Tzu-I Chuang, the wife of the then US consul general, who had a large following on Chinese social media.²⁸² In April 2021, Xu Xiuzhong, a China-born researcher who had published reports on repression in Xinjiang, became the target of an online harassment campaign.²⁸³

C8 0-3 pts

Are websites, governmental and private entities, service providers, or individual users subject to 0 / widespread hacking and other forms of cyberattack? 3

Hackers employ a variety of methods to interrupt or intercept online content. China remains a top source of global cyberattacks,²⁸⁴ though those with commercial targets have declined or become harder to trace.²⁸⁵ Attacks known to have originated in China can rarely be linked directly to the state, and much of the activity appears decentralized and uncoordinated. However, many attacks employ sophisticated technology, and experts believe that Chinese military and intelligence agencies either sponsor or condone technical attacks on political targets both within and outside China.

Websites associated with the persecuted Uyghur minority group have faced frequent cyberattacks in recent years, while China-based hackers have deployed various phishing campaigns to infiltrate these communities in exile and collect information about them. In May 2021, cybersecurity firms Check Point and Kaspersky reported that hackers were employing malicious Microsoft Word file purporting to be from the UN Human Rights Council, detailing rights violations to Uyghurs. The document would introduce malware onto a target’s electronic device if opened. The companies alleged that the likely goal of the attack was to introduce malware on a target’s electronic device, particularly prominent Uyghurs, including in China.²⁸⁶

In March 2021, Facebook announced that it had disrupted the actions of hacker groups using malware links on its platform to surveil Uyghurs, with targets mainly based in Turkey, Kazakhstan, the United States, Syria, Australia, and Canada. Targeted users were sent look-alike domains for popular Uyghur and Turkish news sites. Parts of this campaign closely resemble activity associated with Evil Eye, a previously identified threat actor that also targeted Uyghurs.²⁸⁷

In April 2019, the human rights group Charter 08 reported that the contents of its online forum had been deleted and its Google blog removed. The organization also noted that its Twitter account had been hacked several times in recent months.²⁸⁸ Chinese Twitter users have also been hacked, apparently as part of the government’s crackdown on the platform (see B2). One activist, Wang Aizhong, had 3,000 tweets deleted from his account in December 2018, which he attributed to state-sponsored hacking.²⁸⁹

Footnotes

- ¹China Internet Network Information Center (CNNIC), “The 47th Statistical Report on China’s Internet Development,” February 2021, <https://www.cnnic.com.cn/IDR/ReportDownloads/202104/P020210420557302172...>. Zhang Jun, “三大运营商2020年成绩单：5G用户超2.5亿 移动独大联通严峻 [Report card of the three major operators in 2020: 5G users exceed 250 million, China mobile dominates and China Unicom is in a grave situation],” Sina.com, January 25, 2021, <https://finance.sina.com.cn/tech/2021-01-25/doc-ikftssap0653914.shtml> ; <https://finance.sina.com.cn/tech/2021-01-25/doc-ikftssap0653914.shtml>
- ²China Internet Network Information Center (CNNIC), “The 47th Statistical Report on China’s Internet Development,” February 2021, <https://www.cnnic.com.cn/IDR/ReportDownloads/202104/P020210420557302172...>

- [3](#)The ranking is based largely on the amount of time taken to download a 5GB HD movie. Cable.co.uk, “Worldwide broadband speed league 2020,” September 2, 2020, <https://www.cable.co.uk/broadband/speed/worldwide-speed-league/>.
- [4](#)199IT, “工信部：2020年中国光纤用户渗透率已达93%[Ministry of Industry and Information Technology: China’s optic fiber user rate reached 93% in 2020],” May 18, 2020, <http://www.199it.com/archives/1051057.html#:~:text=%E5%B7%A5%E4%BF%A1%E...>
- [5](#)Charlotte Gao, “China’s Great Firewall: A Serious Pain in the Neck for European and US Companies,” The Diplomat, June 21, 2018, <https://thediplomat.com/2018/06/chinas-great-firewall-a-serious-pain-in-...>
- [6](#)China Law Translate, “Cybersecurity Law,” July 4, 2016, <http://www.chinalawtranslate.com/cybersecurity2/?lang=en>
- [7](#)China Power Team, “How web-connected is China?,” China Power, April 18, 2019, <https://chinapower.csis.org/web-connectedness/>.
- [8](#)Juan Pedro Tomas, “Chinese operators have already deployed 916,000 5G base stations: Report” RCR Wireless News, July 13, 2021, <https://www.rcrwireless.com/20210713/5g/chinese-operators-already-deplo...>
- [9](#)China News, “中国宽带资费水平报告：中国在全球处偏低水平[China’s broadband tariff level report: China is at a low level globally],” April 16, 2021, <https://www.chinanews.com/cj/2021/04-16/9456738.shtml>.
- [10](#)China Internet Network Information Center (CNNIC), “The 47th Statistical Report on China’s Internet Development,” February 2021, <https://www.cnnic.com.cn/IDR/ReportDownloads/202104/P020210420557302172....>
- [11](#)China Internet Network Information Center (CNNIC), “The 47th Statistical Report on China’s Internet Development,” February 2021, <https://www.cnnic.com.cn/IDR/ReportDownloads/202104/P020210420557302172....>
- [12](#)Qin Chem, “Inkstone Explains: How China engineers an alternative internet for its people,” Inkstone news, Jun 11, 2020, <https://www.inkstonenews.com/tech/inkstone-explains-how-china-engineers...>
- [13](#)Ouyang Shijia and Ma Si, “Cybersecurity rule to take effect June 1,” China Daily, April 28, 2020, <https://global.chinadaily.com.cn/a/202004/28/WS5ea78912a310a8b241152323...>
- [14](#)CAC, “网络安全审查办法[Cyber Security Review Measures],” CAC, April 27, 2020, http://www.cac.gov.cn/2020-04/27/c_1589535450769077.htm
- [15](#)China Law Translate, “Cybersecurity Review Measures,” China Law Translate, May 7, 2020, <https://www.chinalawtranslate.com/en/cyber-security-review/>
- [16](#)Alexa Olesen, “Welcome to the Uighur Web,” Foreign Policy, April 21, 2014, <http://atfp.co/1jmlCYH>
- [17](#)王丽Wang Li, @0530wlq, “王臧失踪第十四天 [the 14th days since Wang Zang’s disappearance] ...,” Tweet, June 12, 2020, 1271302871112282112
- [18](#)Chinese Human Rights Defenders (CHRD), “新娜：断网至今 我现终于可以出来在外面蹭网了! [Xin na: Until today I was disconnected, now I can go out and use someone else’s internet connection],” October 21, 2020, https://wqw2010.blogspot.com/2020/10/blog-post_51.html.
- [19](#)Drew Foerster, “China’s Legislature Gears Up to Pass a Sweepingly Vague Cybersecurity Law,” American Bar Association, May 2, 2016, http://www.americanbar.org/publications/blt/2016/05/02_foerster.html; China Law Translate, “Counter-Terrorism Law (2015),” China Law Translate, December 27, 2015, <https://www.chinalawtranslate.com/en/counter-terrorism-law-2015/>
- [20](#)Alan Weissberger, “China’s big 3 mobile operators have 9 Million 5G subscribers in advance of the service; Barron’s: China to lead in 5G deployments,” Techblog, October 7, 2019, <https://techblog.comsoc.org/2019/10/07/chinas-big-3-mobile-operators-ha...>
- [21](#)Lan Xinzhen, “Full-Pricing Autonomy,” Beijing Review, May 26, 2014, http://www.bjreview.com.cn/business/txt/2014-05/26/content_621017.htm; Paul Mozur and Lorraine Luk, “China to Liberalize Telecommunications Pricing,” Wall Street Journal, May 9, 2014, <http://on.wsj.com/1NFam3s>; 毛启盈, “工信部支持民资进入转售业务 打破垄断发文还不够 [MIIT supports private capital entering network leasing business, more antimonopoly policy is needed],” 搜狐Sohu, December 30, 2015, <http://it.sohu.com/20151230/n432995626.shtml>.
- [22](#)Global Services, BT, “First global telco to receive domestic telecoms licenses in China,” January 24, 2019, <https://www.globalservices.bt.com/en/aboutus/news-press/bt-first-global...>
- [23](#)Global Times, “China opens up VPN joint venture to foreign investors,” September 07, 2020, <https://www.globaltimes.cn/content/1200193.shtml>.
- [24](#)These include the Public Security Bureau and the State Administration for Industry and Commerce. “一看就明白全程图解网吧牌照申请流程图” [A look at an illustration of the whole course of the

- cybercafe license application process],” Detail.Zol.com, http://detail.zol.com.cn/picture_index_100/index997401.shtml.
- [25](#)Dahe News, “2020年全国网吧共倒闭12888家 网吧行业急需解锁新技能 [In 2020, 12,888 internet cafés will close across the country. The internet café industry urgently needs to unlock new skills],” Sina.com, March 26, 2021, <https://finance.sina.com.cn/chanjing/cywxw/2021-03-26/doc-iknscsk174792...>.
 - [26](#)Central Cyberspace Affairs Commission website, accessed June 28, 2021, <http://www.cac.gov.cn/>.
 - [27](#)David Feng, “Chinese Cyber Administration Office Goes Online,” Tech Blog 86, December 31, 2014, <https://web.archive.org/web/20150112152942/http://www.techblog86.com/20...>; National Law Review, “More Officials Appointed to Lead Film and Media Authorities in China,” National Law Review, July 31, 2018, <https://www.natlawreview.com/article/more-officials-appointed-to-lead-f...>.
 - [28](#)Drew Foerster, American Bar Association, “China’s Legislature Gears Up to Pass a Sweepingly Vague Cybersecurity Law,” May 2, 2016, http://www.americanbar.org/publications/blt/2016/05/02_foerster.html.
 - [29](#)Paul Mozur, “In China, Internet Czar Is Taking a Blunt Tone,” Bits (blog), New York Times, October 31, 2014, <http://nyti.ms/1GELosY>; Shannon Tiezzi, “Xi Jinping Leads China’s New Internet Security Group,” Diplomat, February 28, 2014, <https://thediplomat.com/2014/02/xi-jinping-leads-chinas-new-internet-se...>.
 - [30](#)Kathleen Wilson, “Revoking Trust in one CNNIC Intermediate Certificate,” Mozilla Security Blog, March 23, 2015, <https://blog.mozilla.org/security/2015/03/23/revoking-trust-in-one-cnni...>.
 - [31](#)Timothy P. Stratford, Jason Goldberg and Christopher Adams, “More Officials Appointed to Lead Film and Media Authorities in China,” Global Policy Watch, July 31 2018, <https://www.globalpolicywatch.com/2018/07/more-officials-appointed-to-l...>.
 - [32](#)Xinhua, “Senior CPC official stresses united front work in Internet sector,” Xinhua Net, November 28, 2019, http://www.xinhuanet.com/english/2019-11/28/e_138590257.htm.
 - [33](#)Ryan Fedasiuk, “Buying Silence: The Price of Internet Censorship in China,” The Jamestown Foundation, January 12, 2021, <https://jamestown.org/program/buying-silence-the-price-of-internet-cens...>; <https://freedomhouse.org/report/china-media-bulletin/2021/legal-pushbac...>.
 - [34](#)“Censorship of Alexa Top 1000 Domains in China,” GreatFireChina, <https://en.greatfire.org/search/alexa-top-1000-domains>.
 - [35](#)The Times of India, “Indian newspapers, websites not accessible in China,” updated June 30, 2020, <https://timesofindia.indiatimes.com/world/china/indian-newspapers-websi....>.
 - [36](#)The Economic Times, “India to permanently ban 59 Chinese apps, including TikTok,” updated January 26, 2021, <https://economictimes.indiatimes.com/tech/technology/india-to-permanent...>.
 - [37](#)Mark Magnier, “China blocks US think tank Centre for Strategic and International Studies website following critique on sanctions,” SCMP, April 17, 2021, <https://www.scmp.com/news/china/diplomacy/article/3129932/china-blocks-...>.
 - [38](#)GreatFire, “Censorship of Alexa Top 1000 Domains in China,” GreatFireChina, <https://en.greatfire.org/search/alexa-top-1000-domains>; Sherisse Pham, “China adds Pinterest to list of banned sites,” CNN, March 17, 2017, <http://money.cnn.com/2017/03/17/technology/pinterest-banned-china/>.
 - [39](#)Amy Chang Chien and Amy Qin, “In China, an App Offered Space for Debate. Then the Censors Came,” The New York Times, February 08, 2021, <https://www.nytimes.com/2021/02/08/world/asia/china-clubhouse-blocked.h...>.
 - [40](#)Stephanie Yang, “China Appears to Block Popular Encrypted Messaging App Signal,” The Wall Street Journal, March 16 2021, <https://www.wsj.com/articles/china-appears-to-block-signal-one-of-last-...>.
 - [41](#)Chauncey Jung, “Reddit Blocked In China,” Supchina, August 12, 2018, <https://supchina.com/2018/08/12/reddit-blocked-in-china/>.
 - [42](#)“Wikipedia blocked in China in all languages,” BBC, May 14, 2019: <https://www.bbc.com/news/technology-48269608>.
 - [43](#)Hillary Leung, “Wikipedia Is Now Banned in China in All Languages,” Time, May 15, 2019, <https://time.com/5589439/china-wikipedia-online-censorship/>.
 - [44](#)Michael Kan, “Google blocked in China by censors, unclear how long it will last,” Info World, November 9, 2012, <https://www.infoworld.com/article/2615782/google-blocked-in-china-by-ce...>.
 - [45](#)Rachel Mok, “Yahoo search is now blocked in China,” Startup Living China, August 31, 2018, <https://startuplivingchina.com/yahoo-search-now-blocked-china/>.
 - [46](#)“China blocks Microsoft’s Bing search engine for one day,” Guardian, January 24, 2019, <https://www.theguardian.com/world/2019/jan/24/china-blocks-microsofts-b...>.

- [47](#)MarketMeChina, “Baidu Search Engine Market Share in China Mar 2021,” April 08, 2021, <https://www.marketmechina.com/baidu-search-engine-market-share-in-china...>
- [48](#)Arjun Kharpal, “An app that let Chinese users bypass the Great Firewall and access Google, Facebook has disappeared,” CNBC, October 11, 2020, <https://www.cnbc.com/2020/10/12/chinese-app-that-let-users-access-googl...>
- [49](#)Tracy Qu and Minghe Hu, “China web browser Kuniao that offered access beyond Great Firewall disappears from domestic internet,” SCMP, November 18, 2019, <https://www.scmp.com/tech/apps-social/article/3038232/china-web-browser...>
- [50](#)BBC, “中国打击代理服务器‘非法经营’ 网民忧无法翻墙 [China cracks down on ‘illegal operation’ of proxy servers],” January 23, 2017, <https://www.bbc.com/zhongwen/simp/chinese-news-38714639>
- [51](#)Jingjing Ma, “New regulations set rules for Internet access services sector: experts,” Global Times, January 22, 2017, <http://www.globaltimes.cn/content/1030188.shtml>
- [52](#)Wong Siu-san and Sing Man, “China Mobilizes The ‘Masses’ to Join Nationwide Security Ops Ahead of Oct. 1,” RFA, September 25, 2019. <https://www.rfa.org/english/news/china/anniversary-surveillance-0925201...>
- [53](#)Sophia Yan, “China blocks internet searches abroad as Xi under pressure ahead of major speech,” The Telegraph, March 5, 2019, <https://www.telegraph.co.uk/news/2019/03/05/china-blocks-internet-searc...>
- [54](#)Huaxia, “China’s broadcasting watchdog solicits public opinion for legislation,” Xinhua, March 17, 2021, http://www.xinhuanet.com/english/2021-03/17/c_139817258.htm.
- [55](#)National Radio and Television Administration, “中华人民共和国广播电视法 征求意见稿 [Radio and Television Law of the People’s Republic of China – Draft for comments],” March 16, 2021, <http://www.nrta.gov.cn/module/download/downfile.jsp?spm=checkydwncf.0.0...> 中华人民共和国广播电视法(征求意见稿).pdf&filename=f2a2331b46d7441581fc09a74323cfd6.pdf.
- [56](#)Sohu, “百度发布2020年信息安全治理年报 [Baidu release 2020 annual report on information security governance],” Sohu, February 9, 2021, https://www.sohu.com/a/449673757_161795
- [57](#)Cyberspace Administration of China, “二季度全国网信行政执法工作扎实推进 [The nationwide cybersecurity and information administrative law enforcement advanced in the second quarter],” July 18, 2020, http://www.cac.gov.cn/2020-07/21/c_1596879319813780.htm; Qiao Long, “中国二季度关闭两千多家网站 再掀大规模网络整治风暴 [In another large-scale network renovation storm, China shut down more than 2,000 website in the second quarter],” Radio Free Asia, July 24, 2020, <https://www.rfa.org/mandarin/yataibaodao/meiti/ql1-07242020062431.html>.
- [58](#)Michelle Toh, “Tripadvisor’s app, and more than 100 others, have just been blocked in China,” CNN, December 9, 2020, <https://www.cnn.com/2020/12/08/tech/tripadvisor-china-apps-intl-hnk/ind...>
- [59](#)Xinhua, “广电总局：网络直播平台“打赏”用户实行实名制管理 [National Radio, Film and Television Administration: Real-name management of users on the webcast platform ‘ticketing’],” November 23, 2020, http://www.xinhuanet.com/politics/2020-11/23/c_1126776466.htm; Karen Chiu, “China orders live streamers and gift-giving fans to register with real names,” SCMP, November 24, 2020, <https://www.scmp.com/tech/policy/article/3111177/china-orders-live-stre...>
- [60](#)赫海威, “中国“标题党女王”的倒下：咪蒙为何被封杀 [Why China Silenced a Clickbait Queen in Its Battle for Information Control],” New York Times Chinese, March 19, 2019, <https://cn.nytimes.com/china/20190319/china-bloggers-internet/dual/>
- [61](#)Wendy Huang, “When Weibo Stopped Updating Its Trending Topics List...,” Whats on Weibo, June 17, 2020, <https://www.whatsonweibo.com/when-weibo-stopped-updating-its-trending-t...>
- [62](#)Paul Mozur, Raymond Zhong, and Steve Lohr, “China Punishes Microsoft’s LinkedIn Over Lax Censorship,” The New York Times, March 18, 2021, <https://www.nytimes.com/2021/03/18/technology/china-linkedin-censorship...>
- [63](#)LinkedIn, “An update on LinkedIn China,” March 09, 2021, <https://news.linkedin.com/2021/march/an-update-on-linkedin-china>; Arjun Kharpal, “China’s Xi Jinping says regulations need to close ‘loopholes’,” CNBC, March 2016, 2021, <https://www.cnbc.com/2021/03/16/chinas-xi-calls-accelerating-regulation...>
- [64](#)Elliott Zaagman, “Cat videos meet Big Brother,” The Interpreter, September 11, 2019, <https://www.lowyinstitute.org/the-interpreter/cat-videos-meet-big-broth...>
- [65](#)“Under Pressure From Cyberspace Administration, China’s Top News App Will Hire 2,000 More Content Reviewers,” Global Voices, January 5, 2018, <https://globalvoices.org/2018/01/05/under-pressure-from-cyberspace-admi...>
- [66](#)Emma Lee, “Kuaishou is hiring more people to filter content after crackdown on ‘vulgar’ content,” Tech Node, April 8, 2018, <https://technode.com/2018/04/08/kuaishou-content-patrols/>
- [67](#)Yuan Li, “Learning China’s Forbidden History, So They Can Censor It,” New York Times, January 2, 2019, <https://www.nytimes.com/2019/01/02/business/china-internet->

- [censor.html](#); <https://beyondsoft.com/interview-with-beyondsoft-ceo/> Matt Field, “Censorship 101: China’s young censors first have to learn about forbidden topics,” Bulletin of the Atomic Scientists, January 3, 2019, <https://thebulletin.org/2019/01/censorship-101-chinas-young-censors-fir...>
- [68](#)Reuters, “China launches crackdown on mobile web browsers, decries ‘chaos’ of information,” October 26, 2020, <https://www.reuters.com/article/uk-china-censorship-browsers/china-laun...>
 - [69](#)Reuters, “Alibaba’s browser removed from Chinese Android app stores,” March 16, 2021, <https://www.reuters.com/technology/alibabas-uc-browser-removed-chinese-....>
 - [70](#)Shawn Yuan, “LGBTQ in China lament ‘dark day’ after social media crackdown,” Al Jazeera, July 13, 2021, <https://www.aljazeera.com/news/2021/7/13/china-lgbtq>
 - [71](#)Jane Li & Matthew De Silva, “This is the blacklist Apple uses to censor the internet in China,” Quartz, October 31, 2019, <https://qz.com/1737232/apple-and-tencent-use-this-blacklist-to-censor-s...>
 - [72](#)Alex Hern, “Apple removes two podcast apps from China store after censorship demands,” The Guardian, June 12, 2020, <https://www.theguardian.com/technology/2020/jun/12/apple-removes-two-po...>
 - [73](#)Global Times, “Apple removes AI face-changing app amid privacy concerns,” March 08, 2021, <https://www.globaltimes.cn/page/202103/1217755.shtml>.
 - [74](#)Jack Nicas, Raymond Zhong & Daisuke Wakabayashi, “Censorship, Surveillance and Profits: A Hard Bargain for Apple in China,” The New York Times, May 17, 2021, <https://www.nytimes.com/2021/05/17/technology/apple-china-censorship-da...>
 - [75](#)Great Fire, “3636 apps are unavailable in the China (mainland) App Store,” Apple Censorship, <https://applecensorship.com/na/CN?!=en>
 - [76](#)Paul Mozur, “Zoom Blocks Activist in U.S. After China Objects to Tiananmen Vigil,” New York Times, June 11, 2020, <https://www.nytimes.com/2020/06/11/technology/zoom-china-tiananmen-squa...>; Drew Harwell and Ellen Nakashima, “Federal prosecutors accuse Zoom executive of working with Chinese government to surveil users and suppress video calls,” The Washington Post, December 18, 2020, <https://www.washingtonpost.com/technology/2020/12/18/zoom-helped-china-....>
 - [77](#)Paul Mozur, “Twitter Users in China Face Detention and Threats in New Beijing Crackdown,” New York Times, January 10, 2019, <https://www.nytimes.com/2019/01/10/business/china-twitter-censorship-on-...>; Yaxue Cao, “China Steps up Nationwide Crackdown to Silence Twitter Users – the Unmediated Story,” China Change, December 5, 2018, <https://chinachange.org/2018/12/05/china-steps-up-nationwide-crackdown-...>
 - [78](#)Sarah Cook, “The News China Didn’t Want Reported in 2017,” Diplomat, January 27, 2018, <https://thediplomat.com/2018/01/the-news-china-didnt-want-reported-in-2...>
 - [79](#)“Directives from the Ministry of Truth,” China Digital Times, accessed October 8, 2020, <https://chinadigitaltimes.net/china/directives-from-the-ministry-of-tru...>
 - [80](#)Samuel Wade, “Minitrue: Propaganda directives for the Fifth Plenum,” China Digital Times, October 22, 2020, <https://chinadigitaltimes.net/2020/10/minitrue-propaganda-directives-fo...>
 - [81](#)Joseph Brouwer, “Minitrue: Commemorating the 70th Anniversary of the War to Resist America and Aid Korea,” China Digital Times, October 22, 2020, <https://chinadigitaltimes.net/2020/10/minitrue-commemorating-the-70th-a-....>
 - [82](#)China Digital Times, “学人SCHOLAR | 温家宝深情撰文：我的母亲 [Scholar - Wen Jiabao’s Affectionate Writing: My Mother],” April 17, 2021, <https://chinadigitaltimes.net/chinese/664996.html>.
 - [83](#)David Bandurski, “Thoughts on a Dark Year,” China Media Project, February 24, 2021, <https://chinamediaproject.org/2021/02/24/thoughts-on-a-dark-year/>; China Digital Times, “财新副主编高昱年终总结：‘三十年启蒙失败了’ [Caixin Deputy Editor-in-chief Gao Yu’s year-end summary: ‘Thirty years of enlightenment failed’],” February 21, 2021, <https://chinadigitaltimes.net/chinese/662858.html>.
 - [84](#)Reuters, “China summons British ambassador over ‘inappropriate’ article,” March 09, 2021, <https://www.reuters.com/article/us-china-britain-diplomat/china-summons...>; Caroline Wilson, @CWilson_FCDO, “I stand by my article. No doubt the outgoing Chinese Ambassador to the UK stands by the 170+ pieces he was free to place in mainstream British media...,” Tweet, March 09, 2021, https://twitter.com/CWilson_FCDO/status/1369296012519612418.
 - [85](#)Amy Qin and Javier C. Hernandez, “A year after Wuhan, China tells a tale of triumph (and no mistakes),” The New York Times, January 10, 2021, <https://www.nytimes.com/2021/01/10/world/asia/wuhan-china-coronavirus.h...>
 - [86](#)Masashi Crete-Nishihata, Jakub Dalek, Jeffrey Knockel, Nicola Lawford, Caroline Wesley, and Mari Zhou, “Censored Contagion II - A Timeline of Information Control on Chinese Social Media During COVID-19,” The Citizen Lab, August 25, 2020, <https://citizenlab.ca/2020/08/censored-contagion-ii-a-timeline-of-infor...> <https://freedomhouse.org/report/china-media-bulletin/2020/xi-legitimacy...>

- [87](#)Li Changshan, “For Mobile Users in China, One ‘Wrong’ Word Means Punishment,” Bitter Winter, October 6, 2020, <https://bitterwinter.org/for-mobile-users-in-china-one-wrong-word-means...>
- [88](#)Wan Zixin, “Religious Activities Online Banned or Censored During Pandemic,” Bitter Winter, October 7, 2020, <https://bitterwinter.org/religious-activities-online-banned-or-censored...>
- [89](#)Manish Singh, “Douyin, TikTok app in China, hits 400 million daily active users,” Tech Crunch, January 7, 2020, <https://techcrunch.com/2020/01/06/douyin-tiktok-app-in-china-hits-400-m...>
- [90](#)David Paulk, “THREAD about how Douyin, the Chinese version of #TikTok, is banning livestreamers for speaking Cantonese instead of Mandarin,” Thread Reader, April 1, 2020, <https://threadreaderapp.com/thread/1245299840944201729.html>
- [91](#)Rik Glauert, “EXCLUSIVE: China throws out court challenge against gay online content ban,” Gay Star News, October 26, 2018, <https://www.gaystarnews.com/article/exclusive-china-throws-out-court-ch...>
- [92](#)Rik Glauert, “Court challenge of China’s LGBTI content ban loses appeal,” Gay Star News, April 15, 2019, <https://www.gaystarnews.com/article/court-challenge-of-chinas-lgbti-con...>
- [93](#)Helen Davison, “Cytus II game removed in China over links to pro-Hong Kong morse code message,” The Guardian, July 21, 2020, <https://www.theguardian.com/world/2020/jul/22/cytus-ii-game-removed-in-...>
- [94](#)Ministry of Culture and Tourism, “文化和旅游局关于深化“放管服”改革促进演出市场繁荣发展的通知 [Ministry of Culture and Tourism Notice on Deepening the Reform of ‘Decentralization, Administration, and Service,’ to Promote the Prosperity of the Performance Market],” September 14, 2020, http://www.gov.cn/zhengce/zhengceku/2020-09/16/content_5544020.htm, <https://freedomhouse.org/report/china-media-bulletin/2020/xi-legitimacy...>
- [95](#)Jeffrey Knockel, Lotus Ruan, Masashi Crete-Nishihata, and Ron Deibert, “(Can’t) Picture This,” The Citizen Lab, August 14, 2018, <https://citizenlab.ca/2018/08/cant-picture-this-an-analysis-of-image-fi...>
- [96](#)Lusha Zhang and Ryan Woo, “Censorship pays: China’s state newspaper expands lucrative online scrubbing business,” Reuters, March 28, 2019, <https://www.reuters.com/article/us-china-censorship/censorship-pays-chi...>
- [97](#)Shan Li, “Made-in-China Censorship for Sale,” Wall Street Journal, March 6, 2020, <https://www.wsj.com/articles/made-in-china-censorship-for-sale-11583448...>
- [98](#)William Yang, “China feminists face clampdown, closure of online accounts,” Deutsche Welle, April 21, 2021, <https://www.dw.com/en/china-feminism-free-speech/a-57277438>; Ryan Woo and Colin Qian, “Closure of online feminist groups in China sparks call for women to ‘stick together’,” Reuters, April 14, 2021, <https://www.reuters.com/world/china/closure-online-feminist-groups-chin...>
- [99](#)Xueyang Xu, Z. Morely Mao, and J. Alex Halderman, “Internet Censorship in China: Where Does the Filtering Occur?,” Passive and Active Measurement, (2011): 133–142, <https://web.eecs.umich.edu/~zmao/Papers/china-censorship-pam11.pdf>
- [100](#)Gary King, Jennifer Pan, and Margaret E. Roberts, “How Censorship in China Allows Government Criticism But Silences Collective Expression,” American Political Science Review 107, no. 2, May 2013, 1–18, <http://j.mp/2nxNUhk>
- [101](#)Drew Foerster, “China’s Legislature Gears Up to Pass a Sweepingly Vague Cybersecurity Law,” American Bar Association, May 2, 2016, http://www.americanbar.org/publications/blt/2016/05/02_foerster.html; China Law Translate, “Counter-Terrorism Law (2015),” China Law Translate, December 27, 2015, <https://www.chinalawtranslate.com/en/counter-terrorism-law-2015/>
- [102](#)Viola Zhou, “Locked out of an online life,” Ink Stone, July 26, 2018, <https://www.inkstonenews.com/tech/chinas-wechat-increasing-censorship-i...>
- [103](#)Arjun Kharpal, “Everything you need to know about WeChat — China’s billion-user messaging app,” CNBC, February 3, 2019, <https://www.cnbc.com/2019/02/04/what-is-wechat-china-biggest-messaging-...>
- [104](#)Alexandra Ma, “Relatives of China’s oppressed Muslim minority are getting blocked online by their own family members, who are terrified to even tell them how bad their lives are,” Business Insiders, February 16, 2019, <https://www.businessinsider.com/family-of-ueighurs-in-china-say-are-bloc...>
- [105](#)Xinmei Shen, “Coronavirus doctor’s last social media post draws commemorations of Tiananmen crackdown,” SCMP, June 4, 2020, <https://www.scmp.com/abacus/culture/article/3087608/coronavirus-doctors...>
- [106](#)Lily Kuo, “Anger in China as doctor who died of COvid-19 omitted from citizens awards,” The Guardian, September 09, 2020, <https://www.theguardian.com/world/2020/sep/09/anger-china-doctor-li-wen...>

- [107](#) Sarah Cook, “China Media Bulletin: 2017 YEAR IN REVIEW (Issue No. 125),” Freedom House, January 2018, <https://freedomhouse.org/china-media/china-media-bulletin-2017-year-in-...>
- [108](#) Bill Bostock, “China enacted a sweeping new law that bars people from posting negative content online, and it could be used to suppress coronavirus news,” Business Insider, March 2, 2020, <https://www.businessinsider.com/china-internet-ban-criticism-could-suppress-...>; CAC, “网络信息内容生态治理规定[Regulations on the ecological governance of network information content],” CAC, December 20, 2019, http://www.cac.gov.cn/2019-12/20/c_1578375159509309.htm
- [109](#) China Law Translate, “Governing the E-cosystem 2,” China Law Translate, March 1, 2020, <https://www.chinalawtranslate.com/en/governing-the-e-cosystem-2/>
- [110](#) Rebecca Davis, “China’s New Internet Censorship Rules Outline Direction For Content,” Variety, January 3, 2020, <https://variety.com/2020/digital/news/china-censorship-law-bytedance-12...>
- [111](#)
- [112](#)
- [113](#) Special Report, “China has the world’s most centralised internet system,” Economist, June 28, 2018, <https://www.economist.com/special-report/2018/06/28/china-has-the-world...>
- [114](#) These propaganda workers are colloquially known as the 50 Cent Party due to the amount they are reportedly paid per post, though other reports have put the going rate as low as 10 cents, while some commentators may be salaried employees. See Perry Link, “Censoring the News Before It Happens,” New York Review (blog), New York Review of Books, July 10, 2013, <https://www.nybooks.com/daily/2013/07/10/censoring-news-before-happens-...>; Rongbin Han, “Manufacturing Consent in Censored Cyberspace: State-Sponsored Online Commentators on Chinese Internet Forums” (paper for Annual Meeting of America Political Science Association, New Orleans, August 31–September 2, 2012), <http://ssrn.com/abstract=2106461>
- [115](#) Murong Xuecun, “Beijing’s Rising Smear Power,” New York Times, September 21, 2014, <http://nyti.ms/1OvsWuZ>; 克里斯蒂安·谢泼德, “中国官媒Twitter账号被疑“僵尸粉”过多 [Chinese official media Twitter account suspected of too many “zombie follower”],” FT中文网, November 23, 2015, <http://m.ftchinese.com/story/001064972>
- [116](#) Jessica Batke & Mareike Ohlberg, “Message Control: How a New For-Profit Industry Helps China’s Leaders ‘Manage Public Opinion,’” China File, December 20, 2020, <https://www.chinafile.com/reporting-opinion/features/message-control-ch...>
- [117](#) Sarah Cook, “Welcome to the New Era of Chinese Government Disinformation,” Diplomat, May 11, 2020, <https://thediplomat.com/2020/05/welcome-to-the-new-era-of-chinese-gover-...>; Bolsover, Gillian, and Philip Howard. “Chinese Computational Propaganda: Automation, Algorithms and the Manipulation of Information about Chinese Politics on Twitter and Weibo.” Information, Communication & Society, 2018, pp. 1–18., doi:10.1080/1369118x.2018.1476576.
- [118](#) Samantha Bradshaw and Philip N. Howard, “The Global Disinformation Order: 2019 Global Inventory of Organized Social Media Manipulation,” Oxford Internet Institute, Computational Propaganda Research Project, September 4, 2019 <https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/09/CyberT...>
- [119](#) “Local Chinese Authorities Use Internet Slang ‘Ziganwu’ in Their Propaganda Recruitments,” Global Voices, June 15, 2015, [https://globalvoices.org/2015/06/15/local-chinese-authorities-use-inter...](https://globalvoices.org/2015/06/15/local-chinese-authorities-use-inter-...)
- [120](#) Oiwan Lam, “Chinese Authorities Think Internet Companies Should Reward Netizens Who ‘Spread Good News,’” Global Voices, December 11, 2015, [https://globalvoices.org/2015/12/11/chinese-authorities-think-the-inter...](https://globalvoices.org/2015/12/11/chinese-authorities-think-the-inter-...)
- [121](#) Sandra Fu, “Central Committee of Communist Youth League Issues an Announcement,” China Digital Times, January 19, 2015, <https://perma.cc/HM8P-PT9J>; Xu Yangjingjing and Simon Denyer, “Wanted: Ten million Chinese students to ‘civilize’ the Internet,” Washington Post, April 10, 2015, <http://wapo.st/1NbD9tb>
- [122](#) Qiao Long, “留学生从“自干五”升团中央宣传部掌控新媒体[International students promote new media from Central Propaganda Department],” Radio Free Asia, November 2, 2016, <http://www.rfa.org/mandarin/yataibaodao/meiti/ql2-11022016100942.html>
- [123](#) Zhou Tian, “团中央新媒体：他们认同了‘团团’，就会更加认同党[Central Youth League New Media: When they identify with ‘Tuantuan’, they will identify with the Party more],” China News Week, February 23, 2017, <https://mp.weixin.qq.com/s?biz=MjM5MDU1Mzg3Mw==&mid=2651195974&idx=1&...>
- [124](#) Gabriel Crossley, Liangping Gao, Anna Ringstrom, and Yilei Sun, “H&M’s Xinjiang labour stance raises social media storm in China,” Reuters, March 24, 2021, [https://www.reuters.com/world/americas/hms-xinjiang-labour-stance-raise...](https://www.reuters.com/world/americas/hms-xinjiang-labour-stance-raise-...)
- [125](#) Jack Hu and Oiwan Lam, “HKFP VOICES POLITICS & PROTEST SCIENCE & TECHNOLOGY: In quest for ‘ideological security’, China pushes to extend Communist Party

- influence inside tech firms,” HKPF, September 19, 2017, <https://www.hongkongfp.com/2017/09/10/quest-ideological-security-china-...>
- ¹²⁶Sina, “知乎成立党支部 CEO周源称值得载入公司历史[Knowing the establishment of the party branch CEO Zhou Yuan said that it is worthy to be included in the company's history],” August 23, 2017, <http://tech.sina.com.cn/i/2017-08-23/doc-ifykiurx1211850.shtml>
 - ¹²⁷Xinmei Shen & Iris Deng, “Big Tech set for starring role at Beijing’s ‘two sessions’ political gala amid regulatory heat and US tech war,” South China Morning Post, February 27, 2021, <https://www.scmp.com/tech/big-tech/article/3123332/big-tech-set-starrin-...>
 - ¹²⁸Shan Li, “Tech Giant Tencent Caught in Chinese Regulatory Trap,” Wall Street Journal, August 15, 2018, <https://www.wsj.com/articles/tencent-disappoints-on-earnings-as-its-gam-...>
 - ¹²⁹“国家网信办公布《互联网新闻信息服务管理规定》[National Network Office Announce “Regulations on the Administration of Internet News Information Services],” Sina, May 4, 2017, <http://finance.sina.com.cn/roll/2017-05-04/doc-ifyexxhw2298844.shtml>; China Copyrights and Media, “Internet News Information Service Management Regulations,” May 2, 2017, <https://chinacopyrightandmedia.wordpress.com/2017/05/02/internet-news-i-...>
 - ¹³⁰“网信办颁新令 矛头指向谁[Internet Information Office issues a new order],” DW, May 2, 2017, <http://www.dw.com/zh/%E7%BD%91%E4%BF%A1%E5%8A%9E%9A%2%81%E6%96%B0%E4%B...>; “Implementing Rules for the Management of Internet News Information Service,” trans. Rogier Creemers, China Copyright and Media, May 22, 2017, <https://chinacopyrightandmedia.wordpress.com/2017/05/22/implementing-ru-...>, noting: “Specifically, those applying for an Internet news information gathering and dissemination license shall be news work units (including work units share-controlled by news work units) or work units controlled by news and propaganda departments. News work units refers to newspaper or periodical publishers, radio stations, television stations, news agencies and news film studios established lawfully and with permission of relevant state departments. Share-controlled means a proportion of over 50% of the capital contribution value, or the proportion of stock held in the total value of corporate capital, or the total share value, or, where even though the proportion in capital contribution value or held stock is less than 50%, the capital contribution value or held stock is sufficient to engender major influence on corporate decision-making. News and propaganda departments include all levels’ propaganda departments, cybersecurity and informatization departments, radio and television departments, etc.”
 - ¹³¹Hogan Lovells, “Are Foreigners Banned from Publishing on the Internet in China?,” May 2016, http://f.datasrvr.com/fr1/716/75489/Final_Publishing_on_Intranet.pdf
 - ¹³²Wen Yunchao, a blogger and activist in New York, says new rules for social media make it impossible for self-media to sustain themselves. “A few newspeople in China tried to use social media to report breaking news, but the CAC’s latest regulations constrain this possibility,” he told Freedom House. “That is to say, Chinese media professionals can’t earn enough from publishing on social media (like WeChat public accounts) to continue their work.” China Media Bulletin no. 125, <https://freedomhouse.org/china-media/china-media-bulletin-2017-year-in-...>. See also: “Forbidden Feeds: Government Controls on Social Media,” PEN America, March 13, 2018, https://pen.org/wp-content/uploads/2018/06/PEN-America_Forbidden-Feeds-...
 - ¹³³Zhang Shuai, “Caixin becomes the first Chinese media outlet to erect paywalls for its products”, China Plus, October 20, 2017, <http://chinaplus.cri.cn/news/business/12/20171020/42045.html>
 - ¹³⁴Qin Chen, “China LGBT groups squeezed as China tightens rules on internet publishing,” inkstone, February 05, 2021, <https://www.inkstonenews.com/society/china-lgbt-groups-squeezed-china-t-...>; Rebecca Davis, “China Imposes New Rules to Restrict Independent Online Content Creators,” Variety, February 23, 2021, <https://variety.com/2021/digital/news/china-cac-self-media-new-regulati-...>
 - ¹³⁵Johanna M. Costigan and Xu Xin, “China’s Digital Cultural Revolution,” Diplomat, April 29, 2020, <https://thediplomat.com/2020/04/chinas-digital-cultural-revolution/>
 - ¹³⁶A recent example of a crackdown would be the closure of Beijing’s Unirule Institute, which founded to promote economic liberalization and democracy. It was shut down after a quarter-century amid government pressure. Chun Han Wong, “China Finally Snuffs Out a Beacon of Liberal Thought and Democracy,” Wall Street Journal, August 27, 2019, <https://www.wsj.com/articles/china-finally-snuffs-out-a-beacon-of-liber-...>
 - ¹³⁷Viola Zhou, “Mainland Chinese evade censors to support Hong Kong protests,” Inkstone, June 13, 2019, <https://www.inkstonenews.com/politics/chinese-internet-users-evade-cens-...>
 - ¹³⁸Darren Byler, “For China’s Muslim minority, the internet was a safe haven—until it wasn’t,” Fast Company, September 23, 2019, <https://www.fastcompany.com/90405715/for-chinas-muslim-minority-the-int-...>; China File, “Islamophobia in China,” China File, May 14, 2019, <http://www.chinafile.com/conversation/islamophobia-china>; Frankie Huang, “China’s Most Popular App Is Full of Hate,” Foreign Policy, November 27, 2018, <https://foreignpolicy.com/2018/11/27/chinas-most-popular-app-is-full-of-...>
 - ¹³⁹Tim Bradshaw, “Apple drops hundreds of VPN apps at Beijing’s request,” Financial Times, November 21, 2017, <https://www.ft.com/content/ad42e536-cf36-11e7-b781-794ce08b24dc>

- [140](#)Hassan Maishera, “China’s Internet Censorship Effort Continues as Authorities Blacklist Hundreds of VPN Servers,” Blokt, May 6, 2019, <https://blokt.com/news/chinas-internet-censorship-effort-continues-as-a-...>; “How does your VPN speed measure against other VPNs in China,” Circumvention Central, accessed October 12, 2020, <https://cc.greatfire.org/en>.
- [141](#)Yuan Yang, “China’s ‘MeToo’ movement evades censors with #RiceBunny,” August 8, 2018, <https://www.ft.com/content/61903744-9540-11e8-b67b-b8205561c3fe>.
- [142](#)Benjamin Haas, “China bans Winnie the Pooh film after comparisons to President Xi,” Guardian, August 6, 2018, <https://www.theguardian.com/world/2018/aug/07/china-bans-winnie-the-pooh-...>.
- [143](#)Yaqiu Wang, “People in China left wondering, ‘what happened in Xinjiang?’” Human Rights Watch, March 25, 2021, <https://www.hrw.org/news/2021/03/25/people-china-left-wondering-what-ha-...>.
- [144](#)Javier C. Hernandez, “China’s investigative journalists warn they are ‘almost extinct’ under Xi Jinping’s strict censorship regime,” Independent, July 14, 2019, <https://www.independent.co.uk/news/world/asia/china-investigative-journ-...>.
- [145](#)Siyuan Meng, “‘A painful read’: New report on the dangers facing China’s delivery drivers going viral,” Radii, September 08, 2020, <https://radiichina.com/delivery-china-driver-safety/>.
- [146](#)王廷瑜, “中國立法嚴格管控 部落客嗾聲接受再教育 [Chinese legislation strictly controls bloggers clamor for reeducation],” Storm Media, July 14, 2015, <http://www.storm.mg/article/57176>.
- [147](#)David Bandurski, “PREVENTING CYBER SHOCK,” China Media Project, November 17, 2018, <http://chinamediaproject.org/2018/11/17/preventing-cyber-shock/>.
- [148](#)Cate Cadell, “Chinese regulator orders detailed user data to fight online mobilization,” Reuters, November 14, 2018, <https://www.reuters.com/article/china-censorship/chinese-regulator-orde-...>.
- [149](#)“China: Detention of activist shows unrelenting assault on freedom of expression,” Amnesty International, February 17, 2020, <https://www.amnesty.org/en/latest/news/2020/02/china-detention-of-activ-...>; Shamil Shams, “China arrests pro-democracy activists in year-end crackdown,” DW, February 1, 2020, <https://www.dw.com/en/china-arrests-pro-democracy-activists-in-year-end-...>; Yibing Feng and Hai Yan, “Sentencing, Arrest of Activists Are Signs of China’s Unrelenting Crackdown,” VOA, May 6, 2020, <https://www.voanews.com/east-asia-pacific/sentencing-arrest-activists-a-...>.
- [150](#)Cao Yin, “Civil code defines, bans sexual harassment,” China Daily, June 1, 2020, http://www.chinadaily.com.cn/a/202006/01/WS5ed45843a310a8b241159c5e_6.h....
- [151](#)Guo Rui, “Two years on, woman who set off #MeToo in China still looking for ‘breakthrough’,” South China Morning Post, December 28, 2019, <https://www.scmp.com/news/china/politics/article/3043702/two-years-woma-...>.
- [152](#)Vincent Ni, “China #MeToo: Court to hear landmark case of intern versus TV star,” BBC, December 02, 2020, <https://www.bbc.com/news/world-asia-china-55140026>.
- [153](#)Emily Feng, “He Tried to Organize Workers in China’s Gig Economy. Now He Faces 5 Years in Jail,” NPR, April 13, 2021, <https://www.npr.org/2021/04/13/984994360/he-tried-to-organize-workers-i-...>.
- [154](#)According to the Supreme People’s Court and the Supreme People’s Procuratorate, the top prosecutorial body, which provided a formal definition in 2013. The definition was given in a judicial interpretation entitled “Regarding the Interpretation of Various Laws Concerning the Handling of Cases of Using the Internet to Carry Out Defamation and Other Crimes.” Human Rights Watch, “China: Draconian Legal Interpretation Threatens Online Freedom,” September 13, 2013, <https://www.hrw.org/news/2013/09/13/china-draconian-legal-interpretatio-...>; Megha Rajagopalan and Adam Rose, “China Crackdown on Online Rumors Seen as Ploy to Nail Critics,” Reuters, September 18, 2013, <https://www.reuters.com/article/net-us-china-internet/china-crackdown-o-...>.
- [155](#)Freedom House, “The Politburo’s Predicament,” 2015, <https://freedomhouse.org/report/special-report/2015/politburos-predicam-...>.
- [156](#)“China: Draconian Legal Interpretation Threatens Online Freedom,” Human Rights Watch, September 13, 2013, <https://www.hrw.org/news/2013/09/13/china-draconian-legal-interpretatio-...>.
- [157](#)For example, Ilham Tohti was found guilty of “separatism” and sentenced to life in prison in September 2014. He was known for his advocacy, both online and off, for China’s Uighur minority. See Edward Wong, “China Sentences Uighur Scholar to Life,” New York Times, September 23, 2014, <https://www.nytimes.com/2014/09/24/world/asia/china-court-sentences-uig-...>; Andrew Jacobs, “Uighur Intellectual Who Won’t Back Down in China,” New York Times, August 20, 2010, <https://www.nytimes.com/2010/08/21/world/asia/21china.html?module=inline>.
- [158](#)“The Battle for China’s Spirit,” Freedom House, February 2017, page 115, https://freedomhouse.org/sites/default/files/FH_ChinasSprit2016_FULL_FL-....

- [159](#)China Law Translate, “People’s Republic of China Criminal Law Amendment (9),” September 1, 2015, <http://chinalawtranslate.com/%E4%B8%AD%E5%8D%8E%E4%BA%BA%E6%B0%91%E5%85...>
- [160](#)Xinhua, “刑法修正案下月起正式实施 微信、微博造谣最高获刑七年 [Criminal law amendments formally implemented next month, up to seven years in prison for rumormongering on Weibo and WeChat],” Xinhua, October 28, 2015, http://news.xinhuanet.com/legal/2015-10/28/c_1116970714.htm
- [161](#)National People’s Congress, “中华人民共和国刑法修正案（十一）[Amendments to the Criminal Law of the People’s Republic of China (11)],” people.cn, December 27, 2020, <http://npc.people.com.cn/n1/2020/1227/c14576-31980014.html>.
- [162](#)Mimi Law, “China introduces new law to ban ‘slander’ of members of armed forces,” South China Morning Post, June 10, 2021, <https://www.scmp.com/news/china/military/article/3136826/china-introduc...>
- [163](#)China Law Translate, “Counter-Terrorism Law (2015),” China Law Translate, December 27, 2015, <https://www.chinalawtranslate.com/en/counter-terrorism-law-2015/>
- [164](#)Rogier Creemers, Paul Triolo, and Graham Webster, “Translation: Cybersecurity Law of the People’s Republic of China (Effective June 1, 2017),” New America, June 29, 2018, <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/tran...>; Jack Wagner, “China’s Cybersecurity Law: What You Need to Know,” Diplomat, June 1, 2017, <https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-...>
- [165](#)Shi Jiangtao, “Chinese authorities say coronavirus control at heart of clampdown on 10 broad categories of crime,” South China Morning Post, February 12, 2020, <https://www.scmp.com/news/china/society/article/3050294/chinese-authori...>
- [166](#)“关于依法惩治妨害新型冠状病毒感染肺炎疫情防控违法犯罪的意见[Opinions on Punishment of Crimes Obstructing the Prevention and Control of the Novel Coronavirus Infection Pneumonia Epidemic According to Law],” People.cn, February 10, 2020, <http://legal.people.com.cn/n1/2020/0210/c42510-31580349.html>
- [167](#)Stanley Lubman, “Arrested, Detained: A Guide to Navigating China’s Police Powers,” Wall Street Journal, August 12, 2014, <https://blogs.wsj.com/chinarealtime/2014/08/12/arrested-detained-a-guid...>
- [168](#)Xinhua, “Victims of Re-education Through Labor System Deserve Justice,” Global Times, January 28, 2013, <http://www.globaltimes.cn/content/758696.shtml>
- [169](#)Economist, “China’s strong-arm approach to drug addiction does not work,” Economist, March 21, 2020, <https://www.economist.com/china/2019/03/21/chinas-strong-arm-approach-t...>
- [170](#)Benedict Rogers, “China’s ‘Residential Surveillance at a Designated Location’ – a licence to disappear, hold and torture dissenters,” Hong Kong Free Press, February 4, 2018, <https://hongkongfp.com/2018/02/04/chinas-residential-surveillance-desig...>
- [171](#)Per an amendment to the criminal procedure law enacted by the National People’s Congress in 2012, which took effect on January 1, 2013. Observers praised other aspects of the measure, including tentative steps toward increasing police accountability for surveillance. Committee to Protect Journalists, “China’s New Law Sanctions Covert Detentions,” March 14, 2012, <http://cpj.org/x/49d9>
- [172](#)“China: Police ‘Big Data’ Systems Violate Privacy, Target Dissent,” Human Rights Watch, November 19, 2017, <https://www.hrw.org/news/2017/11/19/china-police-big-data-systems-viola...>
- [173](#)@SpeechFreedomCN, “武汉新型冠状病毒肺炎事件相关因言获罪案例 [Convictions related to the Wuhan Coronavirus],” accessed June 29, 2021, <https://docs.google.com/spreadsheets/d/1CQBeBp2-A45lw-zr6mneDuPtSBNWg...>
- [174](#)中国文字狱事件盘点 [Inventory of Chinese instances of imprisonments for writings],” @SpeechFreedomCN, “Zhang Wenfang, a Hebei based Weibo user, sentenced to 6 months in prison for a piece of content she posted on Weibo, which mentioned dozens of untold sad stories during the Covid lockdown in Wuhan City, and which authority claimed contained rumors,” Tweet with images, February 22, 2021, <https://twitter.com/SpeechFreedomCN/status/1363792214384652289>; Chinese Human Rights Defenders, “Chen Zhaozhi (陈兆志),” August 28, 2020, <https://www.nchrd.org/2020/08/chen-zhaozhi/>.
- [175](#)Committee to Protect Journalists, “China, Turkey, Saudi Arabia, Egypt are world’s worst jailers of journalists,” Committee to Protect Journalists, December 11, 2019, <https://cpj.org/reports/2019/12/journalists-jailed-china-turkey-saudi-a...>
- [176](#)“Zhang Zhan: China jails citizen journalist for Wuhan reports,” BBC, December 28, 2020, <https://www.bbc.com/news/world-asia-china-55463241>
- [177](#)Yaqiu Wang, “Silenced in China: The Archivists,” Human Rights Watch, July 22, 2020, <https://www.hrw.org/news/2020/07/22/silenced-china-archivists>

- [178](#)Chinese Human Rights Defenders, “China: Release Journalist Chen Jieren Imprisoned for 15 Years for Criticising CCP,” Chinese Human Rights Defenders, April 30, 2020, <https://www.nchrd.org/2020/04/china-release-journalist-chen-jieren-impr...>
- [179](#)Gao Feng, “Chongqing Entrepreneur Gets 20 Years For ‘Subversion’ in Nationwide Campaign,” Radio Free Asia, November 20, 2020, <https://www.rfa.org/english/news/china/entrepreneur-subversion-11202020...>
- [180](#)China Change, “In China, 24 Members of a Subculture Website Sentenced, the Main ‘Culprit’ Gets 14 Years in Prison,” February 03, 2021, <https://chinachange.org/2021/02/03/24-members-of-a-subculture-website-s...>
- [181](#)Rights Defense Network, “湖南泼墨女董瑶琼一个星期前疑被第三度关进精神病院 [Last week, Hunan splash ink woman, Dong Yaoqiong, suspected of being imprisoned in a mental hospital for the third time],” February 14, 2021, https://wqw2010.blogspot.com/2021/02/blog-post_92.html
- [182](#)Ye Bing, “助泼墨女呼救触动高层敏感神经？欧彪峰被扣“煽动”重罪 [Helping the ink-splashing girl’s call for help touches the sensitive nerves of the high-level? Ou Biaofeng detained for ‘inciting subversion,’],” VOA, December 25, 2020, <https://www.voachinese.com/a/citizen-journalist-subversion-charge-refle...>
- [183](#)Linda Lew, “China charges ‘Ink Girl’ supporter with subversion as room for dissent narrows further,” South China Morning Post, August 1, 2021, <https://www.scmp.com/news/china/politics/article/3143327/china-charges-...>
- [184](#)Verna Yu, “Chinese human rights lawyer jailed for four years, says his wife,” The Guardian, June 18, 2020, <https://www.theguardian.com/world/2020/jun/18/chinese-human-rights-lawy...>
- [185](#)PEN America, “Reports: China to escalate charges against PEN America Honoree Xu Zhiyong,” January 2021, <https://pen.org/press-release/reports-china-to-escalate-charges-against...>
- [186](#)Xu Zhiyong, Translated and Annotated by Geremie R. Barmé, “Dear Chairman Xi, It’s Time for You to Go,” China File, February 26, 2020, <https://www.chinafile.com/reporting-opinion/viewpoint/dear-chairman-xi-...>
- [187](#)Guo Rui, “China arrests girlfriend of detained legal activist Xu Zhiyong on subversion charge,” SCMP, March 15, 2021, <https://www.scmp.com/news/china/politics/article/3125558/china-arrests-...>
- [188](#)Emily Feng, “He tried to organize workers in China’s gig economy. Now he faces 5 years in jail,” NPR, April 13, 2021, <https://www.npr.org/2021/04/13/984994360/he-tried-to-organize-workers-i...>
- [189](#)Gao Feng, “Rights attorney formally arrested for ‘subversion’ in China’s Shaanxi: Wife,” Radio Free Asia, April 19, 2021, <https://www.rfa.org/english/news/china/lawyer-arrest-04192021082212.html>
- [190](#)Gao Feng, “Chongqing Entrepreneur Gets 20 Years for ‘Subversion’ in Nationwide Campaign,” Radio Free Asia, November 20, 2020, <https://www.rfa.org/english/news/china/entrepreneur-subversion-11202020...>
- [191](#)Ben Westcott, “Outspoken Chinese billionaire Sun Dawu sentenced to 18 years in prison,” CNN, July 29, 2021, <https://www.cnn.com/2021/07/29/business/sun-dawu-prison-sentence-china-...>
- [192](#)“Chinese farmer who praised lawyer amid crackdown arrested,” Associated Press, November 11, 2020, <https://apnews.com/article/beijing-media-social-media-arrests-xi-jinpin...>
- [193](#)Chinese Human Rights Defenders, “Police Forcibly Disappear Rights Lawyer, Activist and Pastor; Publisher Geng Xiaonan Arrested,” October 26, 2020, <https://www.nchrd.org/2020/10/briefing-police-forcibly-disappear-rights...>
- [194](#)Emily Feng, “China makes it a crime to question military casualties on the internet,” NPR, March 22, 2021, <https://www.npr.org/2021/03/22/979350003/china-makes-it-a-crime-to-ques...>; Global Times, “Seven Chinese netizens detained for defaming PLA martyrs,” February 23, 2021, <https://www.globaltimes.cn/page/202102/1216230.shtml>
- [195](#)International Federation of Journalists, “China: Authorities detain journalist for online remarks,” February 24, 2021, <https://www.ifj.org/media-centre/news/detail/category/press-releases/ar...>
- [196](#)Agence France-Presse, “Chinese ‘Great Firewall’ critic Zhang Jialong ‘jailed for 18 months,’” South China Morning Post, January 10, 2021, <https://www.scmp.com/news/china/politics/article/3117102/chinese-great-...>
- [197](#)Weiquan, “广州公民陈宗因组建微信群而获罪 被判刑1年3个月[Guangzhou citizen Chen Zong convicted of forming a WeChat group and sentenced to 1 year and 3 months in prison],” Weiquan, July 7, 2020, <https://wqw2010.blogspot.com/2020/07/13.html>; CHR D人权捍卫者, “Chen Zong, a Guangzhou-based citizen, sentenced to 15 months’ imprisonment (‘picking quarrels & provoking trouble’) just for setting up WeChat groups (冰火岛), using a VPN to access overseas websites & sharing information from those sites to the groups <https://wqw2010.blogspot.com/2020/07/13.html>,” Twitter, July 6, 2020, <https://twitter.com/CHRDnet/status/1280194508433403904>
- [198](#)Sn Cheng, “Student Flees China After Questioning Over Sharing of VPN Login,” Radio Free Asia, May 19, 2021, <https://www.rfa.org/english/news/china/flees-05192021111036.html>

- [199](#)Gao Feng, “Fine For VPN Use Sparks Rare Backlash on Chinese Internet,” RFA, May 21, 2020, <https://www.rfa.org/english/news/china/vpn-punishments-05212020103537.h...>
- [200](#)Chinese Human Rights Defenders, @CHRDnet, “Guangzhou netizen Chen Zong received 15-month prison sentence on charges of “picking quarrels” for setting up a WeChat group & using Virtual Private Network (VPN)...,” Tweet with images, July 15, 2020, <https://twitter.com/CHRDnet/status/1283469318156627969>.
- [201](#)Gao Feng, “China Jails Activist Who Helped Huang Qi’s Mother For ‘Terrorism,’” Radio Free Asia, November 10, 2020, <https://www.rfa.org/english/news/china/activist-11102020140701.html>.
- [202](#)The Committee to Protect Journalists, “Human rights reporter Zhou Weilin sentenced to 3.5 years in Chinese prison,” August 5, 2021, <https://cpj.org/2021/08/human-rights-reporter-zhou-weilin-sentenced-to-....>.
- [203](#)Chun Han Wong, “Twitters users to prison for posts most Chinese can’t see,” The Wall Street Journal, January 29, 2021, <https://www.wsj.com/articles/china-is-now-sending-twitter-users-to-pris...>
- [204](#)Chun Han Wong, “Twitters users to prison for posts most Chinese can’t see,” The Wall Street Journal, January 29, 2021, <https://www.wsj.com/articles/china-is-now-sending-twitter-users-to-pris...>
- [205](#)“China: Massive Crackdown in Muslim Region,” Human Rights Watch, September 9, 2018, <https://www.hrw.org/news/2018/09/09/china-massive-crackdown-muslim-regi...>
- [206](#)Adrian Zanz, “New Evidence for China’s Political Re-Education Campaign in Xinjiang,” The Jamestown Foundation, May 15, 2018, <https://jamestown.org/program/evidence-for-chinas-political-re-educatio...>
- [207](#)“China has turned Xinjiang into a police state like no other,” Economist, May 31, 2018, <https://www.economist.com/briefing/2018/05/31/china-has-turned-xinjiang...>
- [208](#)Uyghur Human Rights Project, “‘Ideological Transformation’: Records of Mass Detention from Qaraqash, Hotan,” February, 2020, https://docs.uhrp.org/pdf/UHRP_QaraqashDocument.pdf
- [209](#)Gene A. Bunin, “Xinjiang’s Hui Muslims Were Swept Into Camps Alongside Uighurs,” FP, February 10, 2020, <http://archive.vn/GLu1h>; Emily Feng, “Afraid We Will Become The Next Xinjiang’: China’s Hui Muslims Face Crackdown,” NPR, September 26, 2019, <https://www.npr.org/2019/09/26/763356996/afraid-we-will-become-the-next...>
- [210](#)Ng Yik-tung and Sing Man, “China Detains Hui Muslim Poet Who Spoke Out Against Xinjiang Camps,” RFA, January 27, 2020, <https://www.rfa.org/english/news/china/poet-01272020163336.html>; Pen America, “Pen America Concerned Over Detained Chinese Poet’s Safety,” Pen America, March 5, 2020, <https://pen.org/press-release/pen-concerned-poet-safety/>
- [211](#)Josh Rogin, “China’s camps now have survivors, and their ordeals aren’t over,” Washington Post, January 23, 2020, <https://www.washingtonpost.com/opinions/global-opinions/chinas-camps-no...>
- [212](#)Tibetan Review, “Held incommunicado since late 2019, Tibetan monk learnt to be jailed in Chengdu,” April 15, 2021, <https://www.tibetanreview.net/held-incommunicado-since-late-2019-tibeta...>
- [213](#)Human Rights Watch, “China: Tibetan Tour Guide Dies from Prison Injuries,” February 16, 2021, <https://www.hrw.org/news/2021/02/16/china-tibetan-tour-guide-dies-priso...>
- [214](#)“‘Prosecute Them with Awesome Power’ China’s Crackdown on Tengdro Monastery and Restrictions on Communications in Tibet,” Human Rights Watch, July 6, 2021, <https://www.hrw.org/report/2021/07/06/prosecute-them-awesome-power/chin...>
- [215](#)Sarah Cook, “The Battle for China’s Spirit: Religious Revival, Repression, and Resistance under Xi Jinping”, New York: Freedom House, 2017, <https://freedomhouse.org/report/china-religious-freedom>
- [216](#)Catherine Shu, “China doubles down on real-name registration laws, forbidding anonymous online posts,” Tech Crunch, August 28, 2017, <https://techcrunch.com/2017/08/27/china-doubles-down-on-real-name-regis...>; Samm Sacks and Paul Triolo, “Shrinking Anonymity in Chinese Cyberspace,” Lawfare (blog), September 25, 2017, <https://www.lawfareblog.com/shrinking-anonymity-chinese-cyberspace>
- [217](#)Tim Stratford et al., “China Enacts New Data Privacy Legislation,” Covington & Burling LLP, January 11, 2013, <https://www.cov.com/en/news-and-insights/insights/2013/01/china-enacts-...>
- [218](#)Huo Jingnan, “China Introduces Restrictions On Video Games For Minors,” NPR, November 6, 2019, <https://www.npr.org/2019/11/06/776840260/china-introduces-restrictions-...>
- [219](#)Gao Feng, “中国网络文学作者受实名制规管 恐打击创作自由 [Authors of Chinese online literature will now be regulated by a real-name system, threatening to attack creative freedom],” Radio Free Asia, June 17, 2020, <https://www.rfa.org/mandarin/yataibaodao/meiti/gf2-06172020075842.html>.
- [220](#)C. Custer, “China to start seriously enforcing real-name mobile registration, government claims,” Tech In Asia, May 31, 2016, <https://www.techinasia.com/china-start-enforcing-realname-mobile-regist...>

- [221](#)Danny O’Brien, “China’s name registration will only aid cybercriminals,” Committee to Protect Journalists blog, December 28, 2012, <https://cpj.org/x/5177>
- [222](#)BBC, “China due to introduce face scans for mobile users,” BBC, December 1, 2019, <https://www.bbc.com/news/world-asia-china-50587098>
- [223](#)Radio Free Asia, “Chinese Police Order Businesses to Monitor Use of Public Wi-fi,” Radio Free Asia, April 6, 2017, <http://www.rfa.org/english/news/china/monitor-04062017121748.html>
- [224](#)Chris Buckley, “China Passes Antiterrorism Law That Critics Fear May Overreach,” The New York Times, December 28, 2015, <http://www.nytimes.com/2015/12/28/world/asia/china-passes-antiterrorism...>
- [225](#)Adan Segal, “The Cyber Trade War,” Foreign Policy, October 25, 2014, <http://atfp.co/1Qq5LzN>
- [226](#)Yan Luo, Eric Carlson and Zhijing Yu, “China Enacts Encryption Law,” Inside Privacy, October 31, 2019, <https://www.insideprivacy.com/data-security/china-enacts-encryption-law/>.
- [227](#)Jack Nicas, Raymond Zhong & Daisuke Wakabayashi, “Censorship, Surveillance and Profits: A Hard Bargain for Apple in China,” The New York Times, May 17, 2021, <https://www.nytimes.com/2021/05/17/technology/apple-china-censorship-da...>
- [228](#)Bai Tiantian, “Xinjiang asks real-name registration for cellphones, PCs,” Global Times, January 29, 2015, <http://www.globaltimes.cn/content/904898.shtml>
- [229](#)Jessica Batke and Mareike Ohlberg, “State of Surveillance,” ChinaFile, October 30, 2020, <https://www.chinafile.com/state-surveillance-china>.
- [230](#)Yujie Xue, “Anti-fraud app from Chinese police sees soaring downloads amid complaints of forced installs,” SCMP, April 12, 2021, <https://www.scmp.com/tech/policy/article/3129222/anti-fraud-app-chinese...>; China Digital Times, “强制推广的“国家反诈中心APP”上交隐私给国家? [The compulsory promotion of the ‘National Anti-fraud Center APP’ handed in privacy to the country?],” April 09, 2021, <https://chinadigitaltimes.net/chinese/664606.html>; Qimai App Center, “国家反诈中心 [National Anti-fraud Center],” <https://www.qimai.cn/app/downloadEstimate/appid/1552823102/country/cn>.
- [231](#)Jason Loftus, “WeChat Threatens Free Speech,” The Wall Street Journal, October 14, 2020, <https://www.wsj.com/articles/wechat-threatens-free-speech-11602696748>
- [232](#)Human Rights Watch, “China: Big data program targets Xinjiang’s Muslims,” December 9, 2020, <https://www.hrw.org/news/2020/12/09/china-big-data-program-targets-xinj...>
- [233](#)Josh Chin and Clément Bürge, “Twelve Days in Xinjiang: How China’s Surveillance State Overwhelms Daily Life,” Wall Street Journal, December 19, 2017, <https://www.wsj.com/articles/twelve-days-in-xinjiang-how-chinas-surveil...>
- [234](#)Hilary Osborne and Sam Cutler, “Chinese border guards put secret surveillance app on tourists’ phones,” Guardian, July 2, 2019, <https://www.theguardian.com/world/2019/jul/02/chinese-border-guards-sur...>
- [235](#)Raymond Zhong, “Going From Hong Kong to Mainland China? Your Phone Is Subject to Search,” New York Times, August 15, 2019, <https://www.nytimes.com/2019/08/15/world/asia/hong-kong-protest-phone-c...>
- [236](#)Samuel Wade, “China’s social credit system: Black Mirror or red herring?,” China Digital Times, February 16, 2017, <http://chinadigitaltimes.net/2017/02/qa-shazeda-ahmed-on-chinas-social-...>
- [237](#)China Law Translate, “Establishment of a Social Credit System,” China Law Translate, April 27, 2015, <http://archive.vn/Z0H0W>
- [238](#)Louise Matsakis, “How the West Got China’s Social Credit System Wrong,” Wired, July 29, 2019, <https://www.wired.com/story/china-social-credit-score-system/>; Bloomberg, “China’s trial program to rate citizens on public behavior is a bureaucratic mess,” LA Times, June 21, 2019, <https://www.latimes.com/business/la-fi-china-big-brother-social-credit-...>
- [239](#)Dev Lewis, “All Carrots and No Sticks: A Case Study on Social Credit Scores in Xiamen and Fuzhou,” Digital Asia Hub, October 11, 2019, <https://www.digitalasiahub.org/2019/10/11/all-carrots-and-no-sticks-a-c...>
- [240](#)Samuel Wade, “China’s social credit system: Black Mirror or red herring?,” China Digital Times, February 16, 2017, <https://www.scmp.com/news/china/politics/article/2167240/chinese-police...>
- [241](#)Laney Zhang, “Global Legal Monitor,” Library of Congress, November 13, 2018, <https://www.loc.gov/law/foreign-news/article/china-new-regulation-on-po...>; 中共中央网络安全和信息化委员会办公室 (CAC), “具有舆论属性或社会动员能力的互联网信息服务安全评估规定 [Regulation on Internet Information Service Security Assessment with Paradoxical Attributes or Social Mobilization Capabilities],” November 15, 2018, http://www.cac.gov.cn/2018-11/15/c_1123716072.htm
- [242](#)武陵公安, “运营商也需履行网络安全责任, 否则依法处罚 [Network operators also need to fulfill their network security responsibilities, otherwise they will be punished according to law],”

- January 8, 2019, <https://mp.weixin.qq.com/s?biz=MzI4OTYzNTc4NQ==&mid=2247485693&idx=1&...>
- [243](#)Luo Jieqi, “Cleaning Up China’s Secret Police Sleuthing,” Caixin, January 24, 2013, <https://www.caixinglobal.com/2013-01-24/cleaning-up-chinas-secret-polic...>
 - [244](#)Per 2015 amendments. See Central People’s Government of the People’s Republic of China, “Presidential order of the People’s Republic of China, No. 29” [中华人民共和国主席令], July 1, 2015, http://www.gov.cn/zhengce/2015-07/01/content_2893902.htm.
 - [245](#)National People’s Congress, “中华人民共和国国家情报法[National Intelligence Law of the People’s Republic of China]”, NPC, June 27, 2017, http://www.npc.gov.cn/zgrdw/npc/xinwen/2017-06/27/content_2024529.htm
 - [246](#)Economist, “China’s new cyber-security law is worryingly vague,” Economist, June 1, 2017, <https://www.economist.com/news/business/21722873-its-rules-are-broad-am...>
 - [247](#)He Huifeng and Nectar Gan, “All mainland app providers ordered to keep user logs for months to curb spread of ‘illegal information,’” SCMP, June 28, 2016, <http://www.scmp.com/news/china/policies-politics/article/1982756/all-ma...>
 - [248](#)OpenNet Initiative, “China,” August 9, 2012, <http://opennet.net/research/profiles/china-including-hong-kong>
 - [249](#)Jeffrey Knockel, Christopher Parsons, Lotus Ruan, Ruohan Xiong, Jedidiah Crandall, and Ron Deibert, “How International Users Unwittingly Build up WeChat’s Chinese Censorship Apparatus,” The Citizen, May 7, 2020, <https://citizenlab.ca/2020/05/we-chat-they-watch/>
 - [250](#)Open Technology Fund, “Studying ‘Study the Great Nation,’” Open Technology Fund, October 12, 2019, <https://www.opentech.fund/news/studying-study-the-great-nation/>
 - [251](#)Norton Rose Fulbright, “Contact tracing apps in China,” Norton Rose Fulbright, May 11, 2020, <https://www.nortonrosefulbright.com/-/media/files/nrf/nrfweb/contact-tr...>
 - [252](#)Paul Mozur, Raymond Zhong and Aaron Krolik, “In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags,” New York Times, August 7, 2020, <https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveilla...>
 - [253](#)Press Trust of India (PTI), “China launches ‘vaccine passport’ for its citizens on WeChat,” TheWeek, March 09, 2021, <https://www.theweek.in/news/world/2021/03/09/china-launches-vaccine-pas...>
 - [254](#)Paul Mozur, Daisuke Wakabayashi and Nick Wingfield, “Apple Opening Data Center in China to Comply With Cybersecurity Law,” New York Times, July 12m 2017, <https://www.nytimes.com/2017/07/12/business/apple-china-data-center-cyb...>
 - [255](#)Shannon Liao, “Apple officially moves its Chinese iCloud operations and encryption keys to China,” The Verge, February 28, 2018, <https://www.theverge.com/2018/2/28/17055088/apple-chinese-icloud-accoun...>
 - [256](#)Reuters, “Apple to build a second data center in China: Xinhua,” February 6, 2018, <https://www.reuters.com/article/us-apple-datacenter/apple-to-build-a-se...>
 - [257](#)Yoko Kubota and Tripp Mickle, “Apple’s Challenge: Win Over China With Pricy New iPhones,” Wall Street Journal, September 13, 2018, <https://www.wsj.com/articles/apple-faces-uphill-battle-to-win-over-chin...>
 - [258](#)Jack Nicas, Raymond Zhong & Daisuke Wakabayashi, “Censorship, Surveillance and Profits: A Hard Bargain for Apple in China,” The New York Times, May 17, 2021, <https://www.nytimes.com/2021/05/17/technology/apple-china-censorship-da...>
 - [259](#)Dustin Volz and Kirsten Grind, “Airbnb executive resigned last year over Chinese request for more data sharing,” The Wall Street Journal, November 20, 2020, <https://www.wsj.com/articles/airbnb-executive-resigned-last-year-over-c...>
 - [260](#)Office of the Central Cyberspace Affairs Commission, “国家互联网信息办公室、公安部加强对语音社交软件和涉深度伪造技术的 [The State Internet Information Office and the Ministry of Public Security have strengthened their investigations on voice software and in-depth counterfeiting technologies],” March 18, 2021, http://www.cac.gov.cn/2021-03/18/c_1617648089558637.htm; Qiao Long, Chingman, and Gigi Lee, “China clamps down on software used to disguise voiceprints,” Radio Free Asia, March 18, 2021, <https://www.rfa.org/english/news/china/software-03182021114431.html>.
 - [261](#)Rogier Creemers, Mingli Shi, Lauren Dudley, and Graham Webster, “China’s Draft ‘Personal Information Protection Law’ (Full Translation),” New America, October 21, 2020, [https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chin...;](https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chin...) Arjun Kharpal, “China passes major data protection law as regulatory scrutiny on tech sector intensifies,” CNBC, August 20, 2021, <https://www.cnbc.com/2021/08/20/china-passes-key-data-protection-law-as...>
 - [262](#)Clarice Yue, Tiantian Ke, John Shi, and Sven-Michael Werner, “China Data Protection Update: The First Draft of The Long-Awaited PRC Personal Information Protection Law Released,” Bird & Bird, October 2020, <https://www.twobirds.com/en/news/articles/2020/china/china-data-protect...>

- [263](#) Gil Zhang and Kate Yin, “A look at China’s draft of Personal Information Protection Law,” IAPP, October 26, 2020, <https://iapp.org/news/a/a-look-at-chinas-draft-of-personal-data-protect...>; Lavender Au and Benjamin Wilhelm, “China’s New Data Protection Law Won’t Rein in State Surveillance,” World Politics Review, October 28, 2020, <https://www.worldpoliticsreview.com/trend-lines/29174/china-s-new-data-...>.
- [264](#) Dentons, “China finally Defines the Necessity Scope of Personal Information Collected by APPs,” March 26, 2021, <https://www.dentons.com/en/insights/articles/2021/march/26/china-finall...>.
- [265](#) Eileen Yu, “China calls out 33 apps for collecting more user data than deemed necessary,” ZDNet, May 1, 2021, <https://www.zdnet.com/article/china-calls-out-33-apps-for-collecting-mo...>.
- [266](#) Manish Singh and Rita Liao, “Did app pulled from app stores n China after suspension order,” TechCrunch, July 4, 2021, <https://techcrunch.com/2021/07/04/didi-app-pulled-from-app-stores-after...>.
- [267](#) Elena Moore, “China Fines Alibaba \$2.8 Billion For Breaking Anti-Monopoly Law,” Elena Moore, April 10, 2021, <https://www.npr.org/2021/04/10/986112628/china-fines-alibaba-2-8-billio...>.
- [268](#) Changhao Wei, “2020 NPC Session: A Guide to China’s Civil Code,” NPC Observer, updated July 5, 2020, <https://npcobserver.com/2020/05/21/2020-npc-session-a-guide-to-chinas-c...>; Huizhong Wu, “In land of big data, China sets individual privacy rights,” Reuters, May 26, 2020, <https://www.reuters.com/article/us-china-parliament-lawmaking-privacy/i...>.
- [269](#) Colin Zick, “China Adopts New Data Security Law,” JD Supra, August 4, 2021, <https://www.jdsupra.com/legalnews/china-adopts-new-data-security-law-77...>.
- [270](#) Ranking Digital Rights, “2020 Ranking Digital Rights Corporate Accountability Index,” Ranking Digital Rights, accessed May 25, 2021, <https://rankingdigitalrights.org/index2020/explore-services>.
- [271](#) China Blog Staff, “Sorry, no comment - we might get invited to tea,” China Blog, BBC, December 9, 2013, <http://bbc.in/1LKxQ0k>.
- [272](#) “Chinese Police Target Activists Who Supported Hong Kong Protests,” Radio Free Asia, June 1, 2020, <https://www.rfa.org/english/news/china/target-06012020144022.html>.
- [273](#) Kris Cheng, “Liu Xia, widow of Nobel laureate Liu Xiaobo, ‘forced to travel’ ahead of China’s key Congress meeting, says NGO,” Hong Kong Free Press, October 16, 2017, <https://www.hongkongfp.com/2017/10/16/liu-xia-widow-nobel-laureate-liu-...>.
- [274](#) Human Rights Watch, “China: Account for Tiananmen Massacre,” June 3, 2021, <https://www.hrw.org/news/2021/06/03/china-account-tiananmen-massacre>.
- [275](#) Shohret Hoshur, “Uyghur Youth Held After Posting Rare Videos Criticizing Government From Inside China,” RFA, September 18, 2020, <https://www.rfa.org/english/news/uyghur/videos-09182020174137.html?sear...>.
- [276](#) “Defending Human Rights in the Era of Dystopia: The Situation of Defenders in China (2019),” Chinese Human Rights Defenders, February 12, 2020, <https://www.nchrd.org/2020/02/defending-human-rights-in-the-era-of-dyst...>.
- [277](#) “Tiger Chairs and Cell Bosses: Political Torture of Criminal Suspects in China,” Human Rights Watch, May 13, 2015, <https://www.hrw.org/report/2015/05/13/tiger-chairs-and-cell-bosses/poli...>.
- [278](#) Amnesty International, “China: Further Information: Lawyer Allegedly Tortured in Detention: Yu Wensheng,” August 20, 2020, <https://www.amnesty.org/en/documents/asa17/2897/2020/en/>.
- [279](#) Isobel Cockerell, “Inside China’s Massive Surveillance Operation,” Weird, May 9, 2019, <https://www.wired.com/story/inside-chinas-massive-surveillance-operatio...>.
- [280](#) Willem Marx and Olivia Sumrie, “Uighurs accuse China of mass detention, torture in landmark complaint,” NBS NEWS, September 9, 2020, <https://www.nbcnews.com/news/world/uighurs-accuse-china-mass-detention-...>.
- [281](#) Human Rights Watch, “‘Prosecute Them with Awesome Power’, China’s Crackdown on Tengdro Monastery and Restrictions on Communications in Tibet,” July 6, 2021, <https://www.hrw.org/report/2021/07/06/prosecute-them-awesome-power/chin...>.
- [282](#) Taiwan News, “Taiwanese wife of US consul general targeted by Chinese netizens over ‘Nazi’ comparison,” July 27, 2020, <https://www.taiwannews.com.tw/en/news/3974885>.
- [283](#) Lily Kuo and Gerry Shih, “China researchers face abuse, sanctions as Beijing looks to silence critics,” The Washington Post, April 07, 2021, https://www.washingtonpost.com/world/asia_pacific/china-online-threats-....
- [284](#) Akamai, “State of the internet/security Q4 2017 report,” <https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet...>.
- [285](#) Mara Hvistendahl, “The Decline in Chinese Cyberattacks: The Story Behind the Numbers,” MIT Technology Review, October 25, 2016, <https://www.technologyreview.com/s/602705/the-decline-in-chinese-cybera...>.

- [286](#)Patrick Howell O'Neill, "Chinese hackers posing as the UN Human Rights Council are attacking Uyghurs," MIT Technology Review, May 27, 2021, <https://www.technologyreview.com/2021/05/27/1025443/chinese-hackers-uyghurs>.
- [287](#)Mike Dvilyanski, "Taking Action Against Hackers in China," Facebook, March 24, 2021, <https://about.fb.com/news/2021/03/taking-action-against-hackers-in-china>.
- [288](#)零八宪章论坛, "零八宪章论坛所有内容于4月24日突然被人为删除, 由零八宪章签署人义务服务近10年的博客已经"被不存在"! 近期除了博客, 此推特账号亦多次受到攻击。[All contents of Charter 08 Forum were suddenly deleted artificially on April 24, and the blog that has been volunteered by Charter 08 signatories for nearly 10 years has been "non-existent"! In addition to blogs recently, this Twitter account has also been attacked many times.]" Twitter, April 24, 2019, <https://twitter.com/08charterbbs/status/1121247488017457152>
- [289](#)Paul Mozur, "Twitter Users in China Face Detention and Threats in New Beijing Crackdown," New York Times, January 10, 2019, <https://www.nytimes.com/2019/01/10/business/china-twitter-censorship-on-...>

ecoi.net summary:

Report on digital media and
internet freedom (reporting period
June 2020 - May 2021)

Country:

China

Source:

[Freedom House](#)

Original link:

<https://freedomhouse.org/country/china/freedom-net/2021>

Document type:

Periodical Report

Language:

English

Published:

21 September 2021

Document ID:

2060883

Austrian Red Cross
Austrian Centre for Country of Origin and Asylum
Research and Documentation (ACCORD)

Wiedner Hauptstraße 32, 1041 Wien
[T \(Telefon\)](#) +43 1 589 00 583
[F \(Fax\)](#) +43 1 589 00 589
info@ecoi.net

Contact
Imprint & Disclaimer
F.A.Q.
Data Protection Notice

ecoi.net is run by the Austrian Red Cross (department ACCORD) in cooperation with Informationsverbund Asyl & Migration. ecoi.net is funded by the Asylum, Migration and Integration Fund, the Austrian Ministry of the Interior and Caritas Austria. ecoi.net is supported by ECRE & UNHCR.

