Freedom House

Issue No. 156: September 2021

# CHINA MEDIA BULLETIN

## Headlines



IMAGE OF THE MONTH

## Police Barricade Flood Memorial

On July 27, police briefly detained Caixin photographer Chen Liang, who used a drone to take this image of makeshift memorials to victims of the devasting floods in Henan that killed over 300 people. Mourners placed flowers and notes outside the entrance to the Shakou Road Station of the Zhengzhou Metro after 14 passengers died in a flooded subway car on July 22. Authorities erected barriers to block the memorials, and detained and roughed up journalists, before eventually removing some of the barriers.

Credit: Chen Liang

ANALYSIS

# Ahead of Hong Kong Elections, Companies Must Act to Protect Digital Rights

By Angeli Datt and Isabel Linzer

Angeli Datt is a senior research analyst for China, Hong Kong, and Taiwan at Freedom House. Isabel Linzer is a research analyst for technology and democracy at Freedom House.

***The private sector may be forced to choose between enabling and resisting state repression.***

Hong Kong police arrested two men in July for posts on a Facebook group that called for a boycott against a pro-Beijing television channel and its advertisers. Separately, Hong Kong police ordered the website of an exiled activist group to be taken offline globally, albeit briefly, then blocked it in the territory in June because it advocated for democracy. And Hong Kongers could face up to five years in prison for "desecrating" the Chinese national flag or emblem on the internet under new legislation that was introduced in August and will soon become law.

These are just a few examples from the past three months that illustrate how steeply internet freedom in Hong Kong has declined in the year since Beijing imposed the National Security Law (NSL) on the territory. Numerous laws have been invoked as part of the recent crackdown, but the draconian NSL—a direct response to the 2019 prodemocracy protest movement—marked a turning point in the broader shift toward tighter control over digital space in Hong Kong.

Now, another moment of reckoning is on the horizon. On December 19, the government will hold long-delayed Legislative Council elections—the first major balloting to be conducted under the NSL and since Beijing ordered drastic changes to the electoral system. Under the new system, all candidates must undergo a screening process run by national security police and a government-appointed body, and the share of directly elected seats has been reduced from half of the Legislative Council to less than a quarter. The prodemocracy opposition camp has also been devastated by a series of expulsions and prosecutions, and many potential candidates have been jailed or fled into exile. Meanwhile, Hong Kong's previously vibrant civil society and media sectors have faced similarly ruthless repression over the past year, and self-censorship has increased online as users delete social media posts that could be deemed illegal.

If this overhaul of political and civic space in Hong Kong is any indication of what is to come, the December elections will likely be a catalyst for fresh eruptions of dissent and even more restrictions on human rights in the territory.

## Anticipating digital election interference

Much of the coming contestation will play out online, and Freedom House has identified four key forms of digital interference to watch for ahead of election day. While many are common in the closed environment of mainland China, they were unknown in Hong Kong until recently. The question is whether leading private companies will help stave off this new wave of repression by defending what remains of Hong Kong's traditionally free and open internet.

First, there is a high risk of arrests for online activity such as critical discussions about the elections or sharing of civil disobedience strategies. Arrests for online activity are a relatively new development in Hong Kong; internet users in mainland China have long had to contend with more severe legal repercussions for their online speech. But Hong Kongers have faced an alarming rise in arrests and prosecutions for online speech under a colonial-era sedition law and the NSL, with potential life sentences in some cases. A new electoral law criminalizes inciting someone to spoil their ballot or leave it blank, and the government is planning legislation that penalizes "fake news," all of which may lead to further arrests and prison sentences for online expression.

Second, government critics may be the targets of cyberattacks. Such campaigns have intensified since 2019, and two significant attacks that were linked to the Chinese state struck the platforms Telegram and LIHKG, which were used by protesters. Leading up to the December elections, cyberattacks against candidates, democracy supporters, journalists, digital media sites, and civil society organizations could disrupt campaigning, the exchange of independent information about the elections, and the mobilization of protests.

Third, news outlets, civil society websites, and social media platforms are at risk of being blocked for hosting content that calls for protests, supports opposition candidates, raises private funds, or criticizes the electoral process and the Hong Kong and Chinese governments. Empowered by the NSL, Hong Kong police have increasingly ordered internet service providers to block websites, with six sites temporarily or permanently blocked since January 2021. While mainland users behind the Great Firewall are restricted from viewing thousands of websites without a virtual private network (VPN), any trend toward broader website blocking in Hong Kong would amount to a serious decline in internet freedom.

Fourth, the elections may trigger pressure on individuals, media organizations, and technology companies to remove online content. In June, police arrested senior Apple Daily staff on NSL-related charges. As a result, the paper closed and deleted all of its online content, and the digital outlet Stand News removed all of its online opinion articles out of fear of a similar prosecution. The public broadcaster Radio Television Hong Kong (RTHK) deleted all of its English-language Twitter posts and all programming older than one year from YouTube and Facebook this summer. In July, the government introduced amendments to the Personal Data (Privacy) Ordinance that would permit the privacy commissioner to order the removal of online content and the arrest of employees from overseas technology companies if the firms fail to comply with takedown requests. The draft bill has encountered pushback from an industry body but is expected to be voted into law before election day.

## The need for a private-sector response to the crackdown

The speed and scale of the crackdown in Hong Kong has been breathtaking and demands a coordinated response from the democratic world. Governments should speak out against arrests and repressive legislation in Hong Kong and China, and back up

their statements with multilateral sanctions against rights abusers and tangible support for civil society, independent media, and exile communities.

But private companies—especially technology companies—also have a crucial part to play. They should resist state demands that violate users' rights, including by rebuffing requests for user data and to remove, block, or otherwise censor content that is protected under international human rights standards. Full transparency around government requests, whether or not companies comply, would lay bare the state's repressive actions and pave the way for accountability.

Technology companies should divert internal resources in preparation for the potential onslaught of digital election interference. Social media platforms should roll out security features to protect users from state-sponsored hackers and increase staff capacity to rapidly respond to incidents, including account takeovers and reports of disinformation or harassment. VPN providers can bolster resources to evade blocks on websites. Website hosting providers can expand distributed denial-of-service (DDoS) mitigation services for independent media and civil society groups facing state-sponsored cyberattacks. Companies should also help protect the privacy and safety of users—and improve their own preparedness—by proactively engaging with and providing support to civil society groups that work on digital rights and security.

Companies in all sectors may face repercussions from Beijing for supporting digital rights or enforcing sanctions against Chinese individuals or entities, particularly following the June passage of a Chinese law meant to counter foreign sanctions. But they can no longer sit on the sidelines. The business community has a fundamental interest in protecting the sorts of freedoms that have long made Hong Kong a dynamic and reliable source of profits and opportunities. International businesses that are active in Hong Kong should conduct transparent due diligence on their operations to avoid complicity in human rights violations. The private sector should also use more of its leverage with the Chinese and Hong Kong governments to impede any legislation or other measures that infringe on free expression. Indeed, previous examples in mainland China indicate that such lobbying could be even more effective at yielding concessions than pressure from foreign governments.

These elections will not be the first or the last to feature online interference by antidemocratic regimes. In Hong Kong, however, private companies can make a difference, and technology companies have an especially important opportunity to show the world that they have learned from past mistakes and are committed to defending the human rights of all users.

# IN THE NEWS
## State media home in on Taliban takeover, COVID-19 disinformation rap, retaliation for Western sanctions

- **Chinese state media, netizens respond to Taliban takeover:** The Taliban takeover of Afghanistan became a regular fixture on Chinese news last month. State media coverage has sought to legitimize Taliban rule, framing the takeover as the "will and choice of the Afghan people;" such coverage is likely intended to pave the way for formal recognition of the Taliban by the Chinese Communist Party (CCP) as Afghanistan's new government. Meanwhile, social media platforms have censored comments critical of the Taliban or Chinese government support of its rule. On August 18, the People's Daily, the CCP mouthpiece, issued a now-deleted viral post on Weibo characterizing the group as having begun as a benign civic movement founded by refugee students, and attributing its growth to "support of the poor." This tacit endorsement was viewed negatively by many netizens who accused the publication of ignoring the Taliban's history of terrorism and human rights violations. Tencent's WeChat platform deleted an article summarizing the controversy hours after it was posted. Similarly, WeChat swiftly deleted a translation of a letter by an Afghan filmmaker pleading for attention to the plight of women and girls. Chinese state media has also seized opportunities to criticize the United States over its Afghanistan policy, and to suggest that the US withdrawal from Afghanistan may be a prelude to its abandonment of Taiwan.

- **Rap as a medium for state-backed COVID-19 disinformation:** A new Chinese government disinformation campaign has emerged, calling for the United States to investigate a CCP-backed conspiracy theory that the coronavirus may have originated in America. The campaign comes in response to the scheduled release in August of a US government report on the origins of COVID-19 examining whether it had leaked accidentally from a lab in Wuhan, or developed in nature. The campaign featured efforts by the Chinese hip-hop group CD Rev, which produced a rap calling for an investigation into Fort Detrick, a Maryland-based biolab that is quickly becoming a household name in China. In the past five years, rap has been increasingly used by the Communist Party to popularize stodgy party ideology with a younger audience, with songs like 2016's "Karl Marx is a post-90s," winning some popularity among youth. In 2016, the CCP paid for CD Rev to travel to a contested part of the South China Sea, where they made a music video supporting China's claim to the area.

- **China expands reciprocal sanctions over Hong Kong:** On July 23, a week after the United States imposed sanctions on seven deputy directors of Beijing's Liaison Office in Hong Kong, the Chinese government added to its growing list of sanctioned Western entities. Those sanctioned included high-profile officials like former US secretary of commerce Wilbur Ross, but also more junior figures like a senior program manager at the International Republican Institute, a democracy watchdog organization. This comes after China's passage of the Anti-Foreign Sanctions Law in early June, which formed a legal base for retaliatory and other foreign sanctions.

State media publicized threats that Western sanctions would be "relentlessly" reciprocated, with China Central Television (CCTV) emphasizing on Sina Weibo's microblogging platform that sanctions hurt the United States more than they do China.

## Censorship updates: Content removals target posts on sexual identity, natural disasters, sports, education, judicial rulings

- **Tencent crackdown on LGBT+ accounts and content:** Beginning July 6, Tencent's WeChat app permanently banned the accounts of university LGBT+ groups across China and deleted all their content. A notice cited new rules introduced in February that require permits for "self-media" accounts, which are independent social media accounts that publish on a range of topics. Later, on August 19, WeChat shut down an account of an LGBT+ friendly hostel, and on August 30 the Tencent-owned QQ messaging platform started blocking search terms related to LGBT+ content. Offline, Shanghai University has asked for information about students who identify as LGBT+. Chinese authorities appear to be turning greater attention to LGBT+ people and content due to CCP perceptions that LGBT+ people identify as such because they are influenced by foreign ideas.

- **Censorship and harassment of journalists covering Henan floods:** Private tech companies and the government blocked access to information about devasting floods in Henan Province in July. Weibo deleted posts about the floods and about the deaths of 14 people on the Zhengzhou Metro. The subway became a focus of people's grief, and authorities installed barriers to hide piles of flowers and notes, and briefly detained a journalist for photographing the memorials. Foreign journalists who covered the floods became targets of online and offline harassment. The provincial Communist Youth League called on its 1.6 million Weibo followers to report the whereabouts of a British Broadcasting Corporation (BBC) correspondent on Weibo, while two foreign correspondents were chased by a mob while attempting to cover the floods. The CCP's propaganda department sent a directive to officials to remind locals not to accept interviews with foreign media.

- **Censorship of Tokyo Olympic coverage:** The Tokyo 2020 Olympics Games received widespread media attention in China, but censors also worked to block content and otherwise shape coverage of the event. Tencent Video's censorship of the Taiwanese team's entry during the opening ceremony on July 23 resulted in it accidentally missing the broadcast of the Chinese team, prompting angry comments online. State media also censored images of Mao Zedong badges worn by two Chinese gold-medal winning athletes on the podium on August 3.

- **Foreign-language apps pulled from Chinese app stores:** Starting August 6, Chinese Android app stores removed several language-learning apps developed by foreign companies, such as Duolingo, amid a wider crackdown on the education sector. In

July, the government had banned teachers based overseas from teaching students inside China, which may have prompted the app removals. (Chinese-developed apps remain available.)

- **Judicial documents disappear from online database:** A Chinese database of court judgements used frequently by lawyers, scholars, and activists removed millions of documents in July, reportedly due to a "migration process." Of the 117 million verdicts, only 11 million remain, and files on every death penalty case in the database has been removed. One Twitter activist documented hundreds of cases of detention for free expression based on verdicts found in the database, while Freedom House's 2017 report *The Battle for China's Spirit* used the database to expose religious persecution.

## Surveillance updates: Landmark personal information law, campaign to regulate apps, local rules

- **Long-awaited personal information law passed:** On August 20, China's National People's Congress passed the Personal Information Protection Law (PIPL), to take effect on November 1. The law outlines conditions for which companies and to a lesser extent government bodies may collect personal data, such as in provisions protecting personal information of those under age of 14. The PIPL also stresses the role of national security in data handling, requires all data on Chinese citizens to be held in the country, and allows for penalties against or banning of foreign entities that violate the law. The heavy-handed internet regulator the Cyberspace Administration of China (CAC), is primarily responsible for implementation of PIPL's broadly worded provisions. In addition to PIPL, the Chinese government has recently passed several other pieces of legislation on data governance. Some make genuine efforts to address grassroots demands for data protection, albeit with exemptions that allow law enforcement agencies to continue operating their vast surveillance systems. Meanwhile, a recent academic paper demonstrated how data collected for COVID-monitoring reasons is being retained and repurposed for national-level surveillance.

- **New campaign to regulate apps on data security:** On July 26, the Ministry of Industry and Information Technology launched a six-month campaign to clean up apps violating consumer rights, posing cybersecurity risks, and "disturbing market order." The campaign is part of a wider national crack down on private companies' use of personal information: in early July, for example, CAC ordered that ride-sharing app Didi be removed from app stores in China over its handling of user data, shortly after it went public in the United States. Didi had reportedly gone ahead with its US listing despite concerns raised by the CAC about its data being acquired by foreigners under US public disclosure requirements; the move was seen as a challenge to the CCP's authority. The latest campaign outlines 22 scenarios requiring rectification, such as failure to encrypt sensitive information, failure to obtain user consent

before transferring data, and the presence of pop-up windows. Social networking platform WeChat temporarily suspended registration of new users in mainland China the day after the campaign was rolled out.

- **Expanded local regulations on data security:** Alongside a slate of national-level data regulations being passed, lower-level entities are also adopting rules to respond to official and netizen concerns about data security. On July 6, Shenzhen released its own data regulations, which will come into effect on January 1, 2022. Shenzhen, the base for many Chinese tech companies, is the first subnational government to release data regulations that build on national law and create local data markets. Shenzhen is also discussing a law that regulates where surveillance cameras are required to be installed, as well as where they are to be banned, in public areas. Further, Zhejiang Province is discussing a rule on the handling of data collected during public emergencies, and how to classify or potentially destroy the data after the emergency ends. As with national-level data protection rules, local regulations will enhance user rights in certain ways, but do not protect citizens significantly against police surveillance and politically motivated reprisals.

## Indictments and convictions for journalists, CCP critics, religious practitioners; poet's suicide

- **Outspoken tycoon sentenced to 18 years in prison:** Sun Dawu, a pig farmer turned billionaire who ran one the largest agricultural businesses in China, received an 18-year prison sentence on July 18. He had been convicted of several charges, including "picking quarrels and provoking trouble," which is often invoked against activists. The court also sentenced several of his associates to prison. The heavy sentence is likely due to his criticism of the CCP, and appears to be part of a wider crackdown on outspoken businesspeople perceived as challenging the party. Prior to his arrest in November 2020, Sun had lamented the lack of political reform in China in a media interview and had expressed support for detained lawyer Xu Zhiyong, who is in jail awaiting trial on charges of "subversion."

- **Tibetan monks sentenced to up to 20 years for online messages:** Monks Choegyal Wangpo, Lobsang Jinpa, Norbu Dondrup, and Ngawang Yeshe received prison sentences of 20, 19, 17, and 5 years respectively in September 2020, according to information that only recently came to light. The monks, from the Tengdro monastery in Tibet, were convicted after police discovered a phone that had belonged to Choegyal Wangpo containing records of communication with monks in Nepal, as well as of donations, following a devastating earthquake there in 2015.

- **Reporter sentenced to 3.5 years for articles and overseas connections:** Reporter and disabled activist Zhou Weilin received a 3.5-year sentence for "picking quarrels" in connection with articles for the Chinese-language human rights website Rights Defense Network (RDN), and for receiving "foreign funding" from the outlet. Authori-

ties detained Zhou in March 2020 and held him incommunicado for months before putting on trial via video link in November. It is unclear if he was allowed a lawyer at his trial. RDN publishes grassroots information on rights abuses and persecution of activists, dissidents, and ethnic and religious minorities in China.

- **Falun Gong practitioners indicted for sending tips to *Epoch Times*:** On April 25, a Beijing court indicted 11 Falun Gong practitioners for sending photos and information about COVID-19 restrictions in the city to the US-based *Epoch Times*. Police initially detained the group in July 2020, and they face potential life imprisonment for "using a heterodox religion to undermine implementation of the law." The newspaper was founded by Falun Gong practitioners, who are severely persecuted in China.

- **Poet's suicide note condemns CCP surveillance, repression:** Guangdong poet Li Huizhi died on July 23 after consuming pesticide. Li's suicide note discussed how he found the increased surveillance under Xi Jinping unbearable, and his lack of hope for the future after the CCP centennial celebrations and speeches. Li's phone was monitored, as was his WeChat account, and he had been required to notify national security officers any time he took a trip. In March 2020, Li had a stroke and despite becoming partially disabled, said he was "more watched, not less" despite writing far less frequently than he had beforehand.

## BEYOND CHINA

## US firms restrict criticism of Beijing, Huawei devices aid web controls, Uyghurs intimidated globally, CGTN fined for forced confessions

- **US firms restrict critical speech about China:** Several American companies restricted access to critical content about China, or from individuals who have spoken out about human rights abuses in China. In July, Kodak apologized and deleted an Instagram post featuring images of Xinjiang shot by a photographer who described his series as a visualization of an "Orwellian dystopia." A report released in August found that some of the political terms that Apple censors on behalf of the CCP in China in its engraving service—in which users can have phrases etched onto their physical devices—are also blocked in Taiwan and Hong Kong. These include references to Xi Jinping, Mao Zedong, and the Falun Gong spiritual movement. In June, Kazakh human rights organization Atajurt announced that YouTube had taken down some of its video testimonies featuring people whose family members had disappeared in Xinjiang, and temporarily blocked access to its channel globally. Since 2017, the group had posted 11,000 videos, which have over 120 million views. YouTube said the channel had been blocked for multiple instances where it had improperly shared personal information, but eventually reinstated some of the videos. In July, Twitter temporarily restricted the account of a New Zealand-based China researcher, and made unavailable tweets she wrote mocking Xi Jinping and the CCP centennial anniversary.

- **Reprisals in Switzerland and Australia for research on CCP:** Two researchers recently faced legal and professional repercussions for their work on China or for criticizing the CCP. In July, Australian journalist and publisher Marcus Reubenstein sued parliamentary researcher Geoffe Wade and the Australian government over tweets Wade sent, and third-party replies, that suggested that Reubenstein had close links to the CCP. In a separate incident, a Swiss doctoral student revealed that he lost his place at the University of St. Gallen in Switzerland in 2020 for sending tweets critical of the CCP. His adviser terminated their relationship because she received "angry emails from China" and was afraid of being denied a visa.

- **Transnational repression, propaganda against Uyghurs:** The CCP has been using a combination of transnational repression and propaganda in a global effort to silence victims and critics of its mass human rights violations in Xinjiang. A June report by the Washington DC-based Uyghur Human Rights Project (UHRP) and Oxus Society for Central Asian Affairs examined the CCP's intimidation and harassment of exile and diaspora Uyghurs, and compiled a data set of as many as 1,546 such cases in 28 countries, of which 85 percent had occurred since 2014. Of the cases, 1,151 are of Uyghurs detained in the host country. Cases also included so called "voluntary" returns of individuals who received threatening messages from officials on WeChat. Countries in the Middle East and North Africa (MENA) region and South Asia were the most complicit. A separate June investigation by the *New York Times* and ProPublica examined over 3,000 videos and clips posted on social media that showed a Chinese government-backed effort to flood the internet with propaganda videos of Uyghurs denying that abuses are happening and to boost them with inauthentic behavior. An August study by the UK-based Centre for Information Resilience (CIR) documented a bot network boosting pro-CCP narratives, such as smears against Uyghurs, to international audiences.

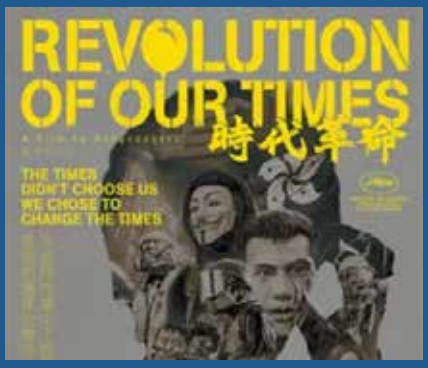
- **Expanding reach of Chinese tech, apps overseas:** Senegal opened a new Huawei-built data center financed by a Chinese loan on June 22 and plans to move all government data and platforms to the center, adopting China's governance model of "digital sovereignty" to host all data inside the country so the state can easily access it. An August 3 study found that 1,799 Huawei middleboxes—devices that sit at key locations in internet infrastructure—are active in 68 countries outside China; of these, 17 countries including Afghanistan, Cuba, Egypt, and Nigeria, are using the Huawei middleboxes to block websites such as those hosting political content, news and media sites, and LGBT+ sites. On August 10, an Access Now report showed the penetration of surveillance technology in Latin America, particularly in Brazil, Argentina, and Ecuador. Chinese companies Huawei, Hikvision, Dahua, and ZTE were noted for providing free donations or cheap prices that were attractive to local governments. A new report from late July showed that relatively unknown social apps like dating and short video platforms developed by China-based companies had been downloaded millions of times and were especially popular in India, Indonesia, and MENA countries. Meanwhile, in the United States and Taiwan, Chinese tech and surveillance firms faced regulatory restrictions. In July, the US Department of Commerce blacklisted 14 Chinese entities, while Taiwan's National

Information and Communication Security Taskforce banned the use of Dahua and Hikvision for government use in January.

- **United Kingdom and United States enforce transparency and broadcast regulations on CGTN, SingTao:** On August 26, the British regulator Ofcom fined state-run China Global Television Network (CGTN) £200,000 ($277,000) for three violations related to broadcasting the forced confessions of two individuals, Swedish publisher Gui Minhai and Hong Konger Simon Cheng. In the United States, the Department of Justice forced Hong Kong newspaper *Sing Tao* to register as a foreign agent after its purchase in February by a relative of a mainland tycoon with close ties to the government.

## FEATURED PUSHBACK
## Scholars, civic groups, Cannes film festival resist Beijing's global censorship efforts

Since late June, several nonstate actors have pushed back against CCP efforts to encourage self-censorship and censor outright content it dislikes. On June 30, the former editor in chief of the science journal *Annals of Human Genetics* said his 2020 resignation came in protest of the journal's refusal to publish an article calling on academic publications to consider a boycott of China over the government's rights abuses against Uyghurs. The journal's publisher, Wiley, reportedly worried the article would cause trouble for its office in China. Another Wiley publication, *Molecular Genetics and Genomic Medicine*, saw 8 out of 25 board members resign this summer in protest of the journal's slow response to demands it remove ethically questionable papers involving studies of minority groups in China.




The poster for the Hong Kong documentary about the 2019 protests.

*Credit: Cannes Festival*

On July 28, 111 Nobel laureates published a letter denouncing the Chinese government's attempts to compel the US National Academy of Sciences and Nobel Foundation to disinvite two speakers—the Dalai Lama and a Taiwanese chemist—from the April Nobel Prize Summit. The organizers rebuffed the Chinese embassy's demands and went ahead with the virtual event, which was hit by two cyberattacks that disrupted proceedings.

In Sweden, civil society organizations issued a letter on August 19 condemning the Chinese embassy in Stockholm's recent verbal attacks against Swedish journalist and publisher Kurdo Baksi. The letter also reiterated support for kidnapped Swedish publisher Gui Minhai, for whom Baksi has organized demonstrations in support of in front of the embassy.

In July, the Cannes Film Festival screened the Hong Kong documentary "Revolution of our Times," which explores the lives of seven participants in the 2019 prodemocracy protests. The festival's director said they were "proud to present this film."

These examples reflect growing awareness and more active responses from nongovernmental actors to CCP global media influence. A February 2021 paper from the National Endowment for Democracy included dozens of such examples from around the world.

# WHAT TO WATCH FOR

- **Heightened tech sector crackdown:** Chinese government regulators continue to enhance their control over social media and other technology platforms. The latest announcements include an unprecedented set of draft regulations governing recommendation algorithms, published by the Cyberspace Administration of China on August 27, as well as a rectification campaign by the agency on "self-media" focused on the gathering and publication of financial information. Meanwhile, another high-level tech executive is facing a corruption investigation, this time a former marketing and public relations director at Sina Weibo. Watch for how social media companies will implement new rules and campaigns, as well as what impact netizen and investor responses to the crackdown—such as large withdrawals from Alibaba's Alipay app—have for China's tech giants.

- **State media faking foreign sources:** As the party-state propaganda apparatus seeks to lend credibility to its narratives for domestic and overseas audiences, several incidents have emerged in which Chinese state media have cited fake analysis by nonexistent individuals. On August 7, the Swiss Embassy in China revealed that a person Chinese state media claimed was a Swiss biologist who had authored an article supporting state narratives on COVID-19, did not actually exist; Chinese state media then erased the article. Meanwhile, media reports and disinformation investigations since July reveal incidents of fake accounts on Facebook promoting CCP talking points. Watch for new examples and tactics involving fake foreigners being deployed to reinforce CCP propaganda and disinformation efforts within China and abroad.

- **Shifting hacking tactics:** Multiple reports since July point to the increasing sophistication and expanded targets of China-based, CCP-aligned hackers. An August 10 report from the cybersecurity firm FireEye outlines a campaign targeting the government and tech sector in Israel, where Chinese hackers attempted to disguise themselves as being based in Iran. Recent indictments in the United States, made public on July 19, indicate that the state security apparatus in China is increasingly recruiting hackers from China's private sector, improving their capabilities but also adding unpredictability as individuals pursue their own goals alongside state objectives. Watch for additional information on this shift and what responses prove effective in defending against increasingly sophisticated attacks.

# TAKE ACTION

- **Subscribe to the *China Media Bulletin*:** Have the bulletin's updates and insights delivered directly to your inbox each month, free of charge. Visit here or e-mail cmb@freedomhouse.org.

- **Share the China Media Bulletin:** Help friends and colleagues better understand China's changing media and censorship landscape.

- **Access uncensored content:** Find an overview comparing popular circumvention tools and information on how to access them via GreatFire.org, here or here. Learn more about how to reach uncensored content and enhance digital security here.

- **Support a prisoner:** Learn how to take action to help journalists and free expression activists, including those featured in passed issues of the *China Media Bulletin,* here.

- **Visit the *China Media Bulletin Resources* section:** Learn more about how policymakers, media outlets, educators and donors can help advance free expression in China and beyond via a new resource section on the Freedom House website.

## For more information

• For archives, go to: www.freedomhouse.org/China-media

• For additional information on human rights and free expression related to China, see: *Freedom in the World 2021*, *Freedom on the Net 2020*, *Beijing's Global Megaphone*, and *The Battle for China's Spirit: Religious Revival, Repression, and Resistance under Xi Jinping*

Freedom House

Freedom House is a nonprofit, nonpartisan organization that supports democratic change, monitors freedom, and advocates for democracy and human rights.

1850 M Street NW, 11th Floor
Washington, DC 20036

111 John Street, Floor 8
New York, NY 10005

www.freedomhouse.org
facebook.com/FreedomHouseDC
@freedomHouseDC

202.296.5101 | info@freedomhouse.org