Freedom House

Issue No. 139: October 2019

CHINA MEDIA BULLETIN

Headlines

ANALYSIS China's Surveillance State has Tens of Millions of New Targets **P2**

IN THE NEWS

- Chinese state media, troll networks fuel backlash against NBA in China **P6**
- Foreign and Chinese brands under increased pressure to aid government censorship **P7**
- Surveillance updates: Study app backdoor, facial scans for internet registration, "Super camera" unveiled, facial recognition on subways **P9**
- Hong Kong: Face mask ban, more attacks on journalists signal declining press freedom **P10**
- Beyond China: Blizzard sanctions pro-Hong Kong gamers, TikTok censorship, US limits Chinese tech exports, academic freedom threats **P11**

FEATURED PUSHBACK Uighurs use video-sharing apps to break through information blockade **P12**

WHAT TO WATCH FOR P14

TAKE ACTION P15

IMAGE OF THE MONTH

Cartooning the NBA's Kowtow

This spin-off of the NBA logo was designed by US-based Chinese cartoonist Rebel Pepper, and published on October 7, in the first days of the controversy that engulfed the league after Houston Rockets' General Manager Daryl Morey posted a tweet supporting prodemocracy protesters in Hong Kong. The logo caricature was shared thousands of times and adopted by some advocates as their profile picture. Over the following weeks, as the NBA and top players came under growing criticism for self-censorship in the face of China's lucrative market, dozens of other cartoons were published online and in US newspapers, news websites, social media posts, and cartoon aggregators.

Credit: *Rebel Pepper/Radio Free Asia.*

ANALYSIS

China's Surveillance State has Tens of Millions of New Targets

By Emile Dirks and Sarah Cook

Emile Dirks is a PhD candidate and independent researcher based in Toronto, Canada whose work focuses on extrajudicial detention and government surveillance in the People's Republic of China. Sarah Cook is a Senior Research Analyst at Freedom House and director of its *China Media Bulletin*.

THIS ARTICLE WAS ALSO PUBLISHED BY *FOREIGN POLICY* ON OCTOBER 21, 2019.

So-called key individuals, from users of drugs to religious believers, are singled out in police databases

One evening in the summer of 2017, local police in China made a surprise inspection of a small private language school, checking the visas of all non-Chinese attendees. Among those present was a foreign doctoral student, who had left his passport at his hotel. "Not to worry," said the officer. "What's your name?" The officer took out a handheld device and entered the student's name. "Is this you?" Displayed on the screen was the researcher's name, his passport number, and the address of his hotel.

These kind of incidents are common in Xinjiang, where China has extensively deployed technology against Muslim minorities. But this episode took place in Yunnan Province, near China's southern border with Myanmar. In fact, Public Security Bureaus – one of the main agencies in China for domestic security and intelligence - across the country are using electronic databases coupled with handheld tools to keep track of certain categories of people. These "key individuals," as they are officially known, range from paroled criminals and users of drugs to foreigners, petitioners, and religious believers.

A review of dozens of local government notices, procurement tenders, and promotional material from Chinese companies indicates that the use of such technologies both predates and extends beyond the current crackdown in Xinjiang, affecting tens of millions of people all over China.

As the Chinese Communist Party identifies new targets for repression under the increasingly authoritarian rule of President Xi Jinping], and Chinese companies expand their sales of surveillance equipment abroad, the scale and impact of these databases are likely to increase in the coming years.

Monitoring "key individuals" nationwide

The Ministry of Public Security's 2007 Key Population Management Guidelines define key individuals broadly as those "suspected of threatening national security or public order." Some specific groups are listed, including serious criminal offenders, people released from prisons or labor camps, and users of illegal drugs.

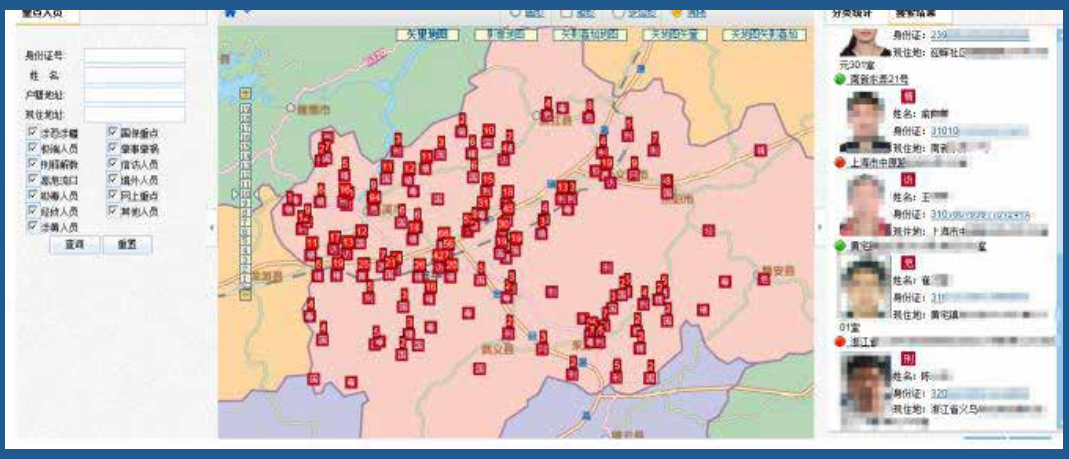
In practice, a far wider range of people are treated as key individuals by China's security apparatus, according to an examination of more than 70 local government notices issued in 26 of China's 34 provinces and administrative regions between 2011 and 2019. Frequently mentioned categories of key individuals include petitioners, members of banned religious groups like Falun Gong, people with mental illnesses, and those involved in "stability maintenance" or "terrorist" activities—two terms that are often

applied to rights activists, protesters, and members of ethnic minority groups like Xinjiang's Uighurs.

As the number of populations under surveillance has grown, so too has the collection of their personal data. The origins of today's massive police databases extend back to the introduction of machine-readable "second generation" national ID cards in the mid-2000s. The cards allowed personal data to be stored electronically and shared easily among branches of the Ministry of Public Security.

In 2006, one of the first nationwide databases of key individuals was launched: the Dynamic Control System. With records on more than two million registered users of drugs, the Dynamic Control System was an early example of ID-based location tracking and biometric data collection. It alerts public security offices whenever registered individuals use their national ID numbers to conduct computer-based transactions, such as buying a train ticket. Police can then determine the individuals' location, intercept them, and conduct a drug test on their urine, the results of which are added to their electronic file. Fingerprints and DNA data are also collected. It was reported in November 2017 that police in Hainan were going door to door collecting DNA samples from registered users of drugs.

The Dynamic Control System soon became a template for other police databases, which Chinese technology firms were contracted to build. By 2008, Hongda Software's Public Security Personnel Information Management Work System was being used to collect information on practitioners of the Falun Gong meditation and spiritual group, whose adherents have been subjected to a large-scale campaign of intimidation, imprisonment, torture, and extrajudicial killing since 1999. Police were able to record who introduced practitioners to the movement, where and with whom they practiced, and their level of spiritual dedication—criteria that resemble precursors to more recent police assessments of Uighurs as "safe," "average," and "unsafe."



Mapping function for police database software developed by Yidiantong that shows the user where different kinds of registered «key individuals» are located within a geographic area. *Credit: Emile Dirks*

A booming surveillance industry

Since the release of Hongda's system, databases on key individuals have become a lucrative part of the country's surveillance technology sector. At least 13 tenders for such projects were issued by Public Security Bureaus in seven provinces or centrally administered cities between October 2015 and May 2019, according to information available online.

Data entry interface for police database of "key individuals" developed by Yidiantong Information Technology in Zhejiang province. *Credit: Emile Dirks*

The companies in question hail from across China, including Shenzhen Yuanzhongrui Technology from Guangdong Province, Beijing's Sensingtech LLC, and Zhejiang Province's Yidiantong Information Technology. Of 40 companies building surveillance database systems, at least 10 provide accompanying handheld devices, like Sensingtech, while 13 mention mapping or geolocation features, like Netposa.

The products themselves are not available for direct examination, but help manuals and screenshots of system interfaces are accessible online. Yidiantong's Key Person Control system allows operators to collect basic identifying information on key individuals (name, date of birth, sex, address) as well as bank account and social media information. Additional categories of data are tailored for particular groups: the results of psychological evaluations for people with mental illnesses; the content of complaints by petitioners; the results of urine tests for users of drugs; or the reason for a foreigner's visit to China and which Chinese counterpart is responsible for the traveler. Some products, like those offered by Hongda Software and Yidiantong, cover populations that are less typical targets of mass monitoring, including internal migrants and clergy from state-approved religious groups.

The diversity of the products—and of the target populations—reflect the decentralized aspects of Chinese policing. There is a nationwide focus on certain groups and a general desire to enforce "social stability" through high-tech surveillance tools. But which populations are prioritized varies across location and time. Local government notices indicate that military veterans petitioning for improved treatment were a concern across China beginning in 2017, while people in community corrections, the mentally ill and petitioners were targeted in the leadup to the 19th Party Congress in 2018. Targets may also vary based on the size of local religious populations: Christians are a greater focus for security services in Zhejiang, Muslims in Xinjiang, Falun Gong practitioners in far northeastern provinces, and Tibetan Buddhists in the Tibetan Au-

tonomous Region, Sichuan, and Qinghai. Adding to the diversity of implementation is the fact that there does not appear to be a single designated supplier for these technologies, leading to a relatively competitive market.

Future uses and implications

There are already signs that disparate databases are being combined with broader state surveillance projects. Yidiantong claims that its Key Person Control database is integrated with the information systems of hotels, internet cafés, airports, and railway stations, enabling real-time data sharing with the police. Several companies even boast that their databases are integrated with facial-recognition cameras capable of identifying key individuals in public places.

The regime's ability to convert data integration into more intensive forms of control and punishment for key individuals is liable to increase. A decade ago, a known dissident, underground Christian, or Falun Gong practitioner might have received a visit from police during politically sensitive periods, like a Communist Party Congress. Today these same people may be monitored continuously, with police receiving automatic alerts about their movements. As the definition of a key individual continues to expand, and new forms of data are added to the tracking systems, there is little to stop police from punishing even minor forms of political or religious dissent and affecting more aspects of a person's life for longer periods of time.

The hoarding of so much personal information in integrated databases with minimal oversight raises obvious concerns about data security. Other surveillance and data-collection systems in China have been found over the past year to have very poor data protection measures, exposing the personal details of millions of people to hackers. Recent official efforts to improve data security have applied almost entirely to how private companies, not the government, handles personal data.

Another concern arises from the potential export of key-individual surveillance technologies to other countries. A study published last month by the Open Technology Fund documents sales of various types of Chinese surveillance and internet censorship equipment to at least 73 countries across five continents. The recipient states are not just other full-fledged autocracies like Egypt or Azerbaijan, but also countries with semiauthoritarian or even democratic systems like Brazil, Malaysia, Tanzania, Poland, and South Korea. At least three technology companies that are listed in the report for providing facial-recognition-enabled cameras to other countries—Dahua, Sensetime, and Hikvision—also offer surveillance technologies aimed at tracking key individuals.

How to respond

Developing effective responses to these surveillance practices is extremely difficult. At a minimum, though, it is worth alerting both Chinese citizens and foreigners traveling in China about the extent of data collection, allowing vulnerable people to take precautions to protect themselves and their acquaintances.

Rights-conscious investors, whether foreign or Chinese, should closely examine their portfolios and eliminate any direct or indirect support for companies that are complic-

it in mass surveillance and rights violations, including through international pension funds and venture-capital firms. A loss of capital could reduce the attraction of contracts from China's security apparatus and dampen enthusiasm for technologies that are specifically designed to track peaceful activism or religious observance.

Finally, officials in democratic settings should be wary of transactions with any of these firms. Among the Chinese commercial entities added this month to a US government export blacklist for their involvement in facilitating repression in Xinjiang, several also sell technologies aimed a broader range of key-individual targets. The United States and democracies in general should apply Xinjiang-style sanctions to Chinese companies that contribute to surveillance-enabled rights violations across the country.

Given the pace at which such dystopian tools of mass repression have proliferated within China, democratic actors should waste no time in halting their spread before they become a fact of life around the world.

IN THE NEWS
Chinese state media, troll networks fuel backlash against NBA in China

On October 4, a simple tweet in support of the ongoing protests in Hong Kong by Daryl Morey, the general manager of the Houston Rockets, elicited a fierce backlash from the Chinese government, state media, and Chinese fans of the NBA. The tweet, which contained an image bearing the words "fight for freedom, stand with Hong Kong," was quickly deleted by Morey, who subsequently apologized, along with the Rockets' owners, to Chinese audiences offended by the message. Despite these damage-control efforts, following an October 8 statement by NBA commissioner Adam Silver supporting free expression, numerous Chinese companies withdrew their sponsorship from the NBA, while banners advertising upcoming NBA exhibition games in China were taken down across the country, and official merchandise was removed from store shelves. Online, viral videos spread of Chinese basketball fans tearing up their tickets, as did messages condemning Morey and the NBA. Silver claimed that the Chinese government had even pressured him to fire Morey.

The controversy around Morey, the NBA, and the Hong Kong protests was not the result of spontaneous Chinese netizen outcries. Rather, it emerged at least in part due to government-led propaganda and content manipulation efforts, including the following:

- **A coordinated Twitter troll attack targeting Morey:** In the hours and days following Morey's initial tweet, tens of thousands of Twitter users apparently based in China were mobilized to respond in a coordinated pro-China intimidation campaign against him. A *Wall Street Journal* analysis of nearly 170,000 tweets directed at Morey concluded that he had been the target of a "troll attack" intended to "manipulate the conversation about the Hong Kong protests," and noted that many of the tweets contained verbal abuse including, among other things, a Chinese acro-

nym meaning "your mother is dead." At the peak of the activity, Morey would have received notifications of such tweets at a rate of nearly two messages per second. Twitter is blocked in China but accessible with circumvention tools; according to experts who analyzed the data and messages, the tweets were likely sent by human users rather than a bot network.

- **Broadcast cancellations by Chinese state media and Tencent:** Chinese state broadcaster China Central Television (CCTV) denounced Adam Silver for defending Morey on free- speech grounds, arguing instead that Morey's tweet challenged "national sovereignty and social stability." CCTV further announced that it would no longer broadcast NBA preseason games. In light of Morey's tweet, the Chinese company Tencent—the NBA's online broadcast partner in China, which also has close ties to the Chinese government—announced that it too would temporarily suspend broadcasts of preseason games.

- **Top-down censorship and manipulation of popular opinion:** Chinese state media responded quickly to the unfolding controversy with both public and behind-the-scenes attempts to manipulate public opinion concerning Morey and the NBA. A Weibo survey released by the *People's Daily*, the official mouthpiece of the Chinese Communist Party, on October 8 asked respondents to pick one of four answers to the question of how they felt about Morey. However, the poll was derided by netizens for only allowing respondents to select from pro-China or anti-Morey answers. On October 10, government censors instructed Chinese websites to remove reports on the NBA from their homepages and to not "hype" topics related to the ongoing controversy.

Persistent public anger in China directed at Morey, Silver, and the NBA in response to Morey's comments and the subsequent fallout, is due also in part to China's notoriously closed media landscape, which has been awash with state disinformation about the Hong Kong protests. Among other smears, participants have been routinely derided as "terrorists" and "cockroaches," as detailed in last month's *China Media Bulletin*. Still, from netizen responses to the People's Daily survey, it is also clear that at least some Chinese fans remain unconvinced by Chinese state propaganda. In one case, a Chinese Rockets fan posted an emotional video in support of his team in which he set fire to China's national flag. However, despite the fan's efforts to cover his face and hide his identity, police were able to track him down and arrest him, sending a chilling message to would-be outspoken fans.

Foreign and Chinese brands under increased pressure to aid government censorship

- **Online travel platforms covered by new censorship rules:** New regulations drafted by China's Ministry of Culture and Tourism will increase censorship of content posted on the platforms of online travel providers. The 42 draft regulations, posted October 10, require the platforms to preemptively review content published in order

to prevent information deemed problematic by the government from spreading. The applications will also be required to store information on people posting on their platforms, and to cooperate with authorities in any investigations related to these people. The rules come on the heels of several other sets of restrictions and content-monitoring efforts imposed over the past year on apolitical platforms like live-streaming, dating, and celebrity gossip applications.

- **South Park "Band in China" episode banned in China:** Chinese government censors have ordered the popular US animated series South Park scrubbed from the internet after a recent episode of the show took satirical aim at the Chinese government. Officials ordered websites to add the show's name to a banned keyword search list, according to a leaked directive published by *China Digital Times*. The episode mocked Chinese censorship and American companies that attempt to appease the Chinese government through self-censorship, while also including politically sensitive references like a scene of Winnie the Pooh being imprisoned in a labor camp because of his use as a meme for Chinese president Xi Jinping. Following the ban, creators Trey Parker and Matt Stone issued on Twitter a faux apology praising the Communist Party and welcoming "Chinese censors into our home and into our hearts." Others have also felt the impact of Chinese government ire at South Park, with musician Zedd announcing on Twitter that he had been banned from performing in China after liking a Tweet from the show's official Twitter account.

- **Apple takes new steps to aid Chinese government censorship:** Numerous reports indicate that tech giant Apple continues to assist Chinese state authorities in censoring content within and outside China. In early October, Quartz's mobile news app was removed from the Chinese version of the App Store due to its coverage of continuing protests in Hong Kong. An app that helps crowdsource data on the location of police in Hong Kong was also removed from the store in early October at the request of local authorities, a decision praised by the state-owned *Global Times*. Apple chief executive Tim Cook defended the move on that grounds that the app was being used to target police officers for violence, but subsequent statements from Hong Kong police indicate that despite official fears, the app had not yet been used in such a way. Buzzfeed has also reported that as early as 2018, Apple was warning show developers for Apple TV+ to avoid topics that might anger the Chinese government. Even emojis have not been spared, with recent updates to iPhone's iOS 13.1 in Macau and Hong Kong removing the Taiwanese flag emoji. In other cases, while Apple itself has not been complicit in government repression, its minimal response has nonetheless concerned critics. According to security researchers at Google Project Zero, the Chinese government has reportedly launched malicious attacks on Uyghur Muslim iPhone users in Xinjiang and abroad in an effort to gain access to the users' location and files. Apple reportedly closed the vulnerability, but declined to comment on the scope or target of the attacks.

Surveillance updates: Study app backdoor, facial scans for internet registration, "Super camera" unveiled, facial recognition on subways

- **Study reveals government-backed study app's surveillance capabilities:** A report by the Open Technology Fund released October 12 provides evidence that a Chinese government app, "Study the Great Nation," can potentially be used for surveillance of users. The app, designed by Chinese tech giant Alibaba, is promoted as a resource through which users can study Communist Party ideology, follow the news, and learn about Chinese President Xi Jinping. However, through backdoors in the app, Chinese authorities can view a user's internet history, text messages, and photos; review their contacts; and even turn on the phone's audio recorder. The app has reportedly been downloaded over 100 million times, and many government employees are required to spend free time accruing points awarded on its programs. In September, regulators announced that journalists' accreditation for 2019 would be based on reporters' performance on an exam drawn in part on the app's content.

- **Facial scans required for internet and phone registration starting in December:** On September 27, China's Ministry of Industry and Information Technology announced that starting December 1, all telecommunications companies must obtain facial scans of all new internet or mobile phone users. Under this same regulation, Chinese citizens would also be prohibited from transferring cell phone numbers to other people. The move, which is being justified in the name of safeguarding the rights and interests of Chinese citizens, marks a further expansion of domestic surveillance and real-name registration requirements for telecommunications customers and netizens—developments that have already discouraged online discussion.

- **"Super camera" unveiled at industry fair:** A team of Chinese scientists unveiled a camera with 500 megapixel resolution capable of capturing detailed still and moving images of faces within panoramic shots of thousands of people. Unveiled in late September at China's International Industry Fair, images from the camera can be uploaded to cloud storage and analyzed in real time. Given the Chinese government's embrace of domestic surveillance, voices in China and abroad have raised serious privacy concerns, asking how such technology could be used in coordination with facial recognition enabled cameras.

- **Free subway ride for facial recognition registration:** In late September, it was reported that Shenzhen has become the latest Chinese city to roll out facial recognition systems for subway commuters. Using technology designed by Huawei, people over the age of 60 who register for the system will be able to gain access to stations for free by scanning their faces. Similar experimental systems have been tested out in Guangzhou, Shanghai, Qingdao, Nanjing, and Nanning. While facial recognition could facilitate the quick passage of people through station barriers, the program could easily give way to broader use by private companies and the government of the facial scans obtained, as surveillance systems in China become increasingly integrated.

HONG KONG
Face masks ban, more attacks on journalists signal declining press freedom

Police violence against journalists in Hong Kong has underscored the worsening climate for press freedom in the Special Administrative Region in recent months, as have scattered attacks on reporters by both protesters and pro-Beijing sympathizers. On October 3, the Hong Kong Journalists Association filed an application for a judicial review against the Commissioner of Police due to his failure to curb police violence, interference, and misconduct directed at journalists. The following are three key developments reflecting deteriorating press freedom in Hong Kong over the previous month:

- **Face mask ban:** On October 4, Hong Kong Chief Executive Carrie Lam invoked a colonial-era emergency ordinance to issue a ban on face coverings, a move that was decried by many international observers. On October 8, the Hong Kong Journalists Association sought clarification from the government on how the prohibition would affect the work of journalists covering protest activity, as well as whether journalists wearing face masks would be in violation of the regulations. Reporters Without Borders has claimed the ban endangers journalists, many of whom wear goggles and gas masks to protect themselves from police tear gas and pepper spray. In response, police say they have the right to ask reporters to remove face masks and arrest those who refuse.

- **More physical attacks on local, foreign journalists:** On September 30, a police officer was caught on camera smiling as he pepper sprayed *Initium Media* journalist Lam Chun Tung, who was attacked despite displaying his press card and wearing a helmet emblazoned with the word "Press." On October 3, Indonesian journalist Veby Indah was left blind in one eye after being struck by a rubber bullet fired by police—the most serious injury to date sustained by members of the media covering the ongoing protests. A few days later on October 6, US journalist Suzanne Salatine was filmed being pushed against a wall and struck with riot shields by police officers; she was subsequently detained but then released without charge. That same day, a journalist for public broadcaster Radio Television Hong Kong (RTHK) was struck by a Molotov cocktail thrown by protesters, causing burns on his face. On October 13, a driver for NowTV was hit with a police projectile outside Mong Kok police station and later detained for two hours and beaten by police officers while in custody.

- **Outlets recall reporters covering National Day protests:** In the face of rising violence, RTHK, the *South China Morning Post*, and Baptist University's student newspaper decided to recall journalists from the frontlines after several incurred injuries during police efforts to disperse protests held on National Day on October 1. Police had used water cannons, pepper spray, and tear gas against protesters, some of whom responded with Molotov cocktails and bricks, during the demonstrations that took place on the sensitive political anniversary. The Hong Kong Journalists Association reported that scores of journalists were injured by rubber bullets and

sponge rounds fired by police, while others were treated for acid attacks, and called on all sides to refrain from interfering with the work of the city's reporters.

BEYOND CHINA

Blizzard sanctions pro-Hong Kong gamers, TikTok censorship, US limits Chinese tech exports, academic freedom threats

- **Blizzard controversy, boycott:** US gaming firm Blizzard has come under fire for sanctioning a player of the popular game Hearthstone who expressed support for the ongoing protests in Hong Kong. During a post-match press conference announcing a gaming victory on October 6, Hong Kong player Chung Ng Wai voiced the popular protest slogan, "liberate Hong Kong, revolution of our times." In response, Blizzard stripped Chung of his prize money and banned him from competing for a year. After an outcry from other players, his winnings were later reinstated and his ban reduced to six months. Nevertheless, calls for a boycott of Blizzard arose, and intensified following the subsequent banning of three US-based Hearthstone players on October 16 for holding up a sign reading "free Hong Kong, boycott Blizz" during a live-streamed match. Seemingly in response to the growing controversy, Blizzard cancelled a product launch in New York City scheduled for October 16. While Blizzard's user base in China is small, the company is seeking to expand in the lucrative software market to make up for lost revenues elsewhere.

- **TikTok censorship of Hong Kong protests and more:** Evidence is growing that the popular social media network TikTok regularly censors material considered sensitive by the Chinese government. The video-sharing platform has emerged as one of the most downloaded and popular applications globally in 2019, especially among teenage users. According to internal documents obtained by the *Guardian*, employees of the company, which is owned by Beijing-based ByteDance, are required to remove content related to such topics as the Tiananmen Square massacre and the persecuted Falun Gong spiritual group. Searches for "Hong Kong" on the site also return surprisingly few results related to the ongoing protests in the city compared to other popular social media platforms. Amid these revelations, on October 9, Senator Marco Rubio requested that the Treasury Department look into the national security implications of the acquisition of the music-based social media service Musical.ly by TikTok, while on October 17 Facebook chief executive Mark Zuckerberg criticized the Chinese company for censoring content. In response, TikTok has hired former US lawmakers now working at law firm K&L Gates to revise its company policies.

- **US places export restrictions on Chinese tech firms aiding repression in Xinjiang:** On October 7, the US Commerce Department announced it would place 28 Chinese entities on a government export blacklist due to their complicity in the Chinese government's ongoing campaign of repression in Xinjiang. Included in the so-called

Entity List are eight Chinese tech companies: Dahua Technology; Hikvision; iFlytek; Megvii Technology; Sense Time; Xiamen Meiya Pico Information Company; Yitu Technologies; and Yixin Science and Technology. In light of the sanctions, two of the largest US public pension funds, the California State Teachers' Retirement System and the New York State Teachers' Retirement System, are said to be reexamining their holdings in Hikvision. Other observers have questioned the impact of the sanctions, and called for stronger measures.

- **New research on Confucius Institutes, Chinese extraterritorial impact on academic freedom:** The impact of Chinese government intimidation and influence on scholarly activity inside China and beyond continues to be a source of concern. On September 24, Scholars at Risk published *Obstacles to Excellence*, a detailed report on challenges to academic freedom linked to activities undertaken by the Chinese government. The report noted a worsening academic environment on both the Chinese mainland as well as in Hong Kong and Macau. The report also examined the extraterritorial reach of Chinese government influence, including via Confucius Institutes operating on campuses across the globe, as well as Chinese government-backed surveillance and intimidation efforts directed at Chinese students and scholars overseas. Separately, Freedom House researcher Sarah Cook and University of Washington student Flora Yan wrote in the Jamestown Foundation's *China Brief* about the intersection between Confucius Institutes and the corporate sector, in particular the increasing efforts by Confucius Institutes to offer courses on Chinese language, politics, and economics to multinational corporations. Their piece also highlights a new partnership program between Hanban—the Confucius Institute Headquarters—and Chinese companies, including tech firms Tencent and iFlytek, both of which are already known for their high level of collaboration with the Chinese government in surveillance and censorship. These revelations raise new concerns about the impact of Confucius Institutes on free expression on campuses, and the potential for these establishments to act as intelligence-gathering organs for the Chinese state.

FEATURED PUSHBACK
Uighurs use video-sharing apps to break through information blockade

Amid a massive campaign of detention, reeducation, and forced labor, China's northwest region of Xinjiang is arguably one of the most tightly controlled information environments in the world. Efforts by Uighur and other Muslim residents of the region to communicate their plight, even to family members overseas, can result in long-term extralegal detention.

It was all the more surprising then to observers of the crisis to see in late August the emergence of dozens of short videos by Uighurs on Douyin, a video-sharing application owned by Chinese firm ByteDance. The clips, often just a few seconds long, typically

showed an ethnic Uighur with a photo of a loved one—who had presumably been taken away to a reeducation camp or state-run orphanage—crying or making other gestures of mourning. Experts who have viewed the videos say they appear to have been filmed and posted from within Xinjiang.

Snapshot of an unnamed Uighur woman appearing to mourn missing family members from a video on Douyin.

The videos' ambiguity appears to have helped them slip past censors initially. It remains unclear how many views the clips received within China—or how long they survived before being deleted, as many were. But the images and videos have spread globally as overseas Uighur activists have reposted them on Twitter, YouTube, and Instagram (all of which are blocked in China). Meanwhile, dozens of international media outlets have published articles about the phenomenon, including the *Wall Street Journal*, *Foreign Policy*, and publications in France and Australia.

Meanwhile, Douyin and its international counterpart Tiktok have emerged as an important, if unlikely, source of video evidence of the Xinjiang crackdown and of the whereabouts of the province's missing children. Despite the difficulty of verifying their accuracy, clips posted by official government or state media accounts have enabled overseas observers and relatives to identify and preserve footage of orphanages for Uighur children whose parents are in detention, instances of mosques being demolished, and images of heavily armed police in training or pro-Communist Party loyalty-building sessions.

WHAT TO WATCH FOR

- **Trial and treatment of rights defender Chen Jianfang:** Chen was detained in March 2019, apparently for publishing an online essay paying tribute to the United Nations–oriented activist Cao Shunli on the fifth anniversary of her death in custody. On August 30, Shanghai prosecutors indicted Chen on charges of "subversion of state power," a serious offense often used to impose long prison sentences on activists, but news of the charges only emerged this month. Chen is a long-time vocal human rights advocate, and UN human rights experts and international human rights groups have written to the Chinese government to express concern about her arrest and denial of due process. Watch for updates on her trial and possible sentencing, whether international pressure on her behalf impacts the outcome of her case, including whether she is granted the legal counsel of her choice, which to date she has been denied.

- **Impact of foreign tech firm attendance at Wuzhen "World Internet Conference":** From October 20 to 22, the Chinese government hosted its sixth annual internet conference in the town of Wuzhen, in Zhejiang. Chinese state media reported that 1,500 people from 80 countries joined. As in past years, the Communist Party had a strong presence at the event, including a keynote speech by Huang Kunming, a member of the Politburo and head of the party's powerful propaganda department, who also read a congratulatory message from Xi Jinping. Several major US tech firms, including Google and Facebook did not attend—possibly because they sought to avoid the blowback that Apple and Google faced in 2017 after sending top executives, and thereby conferring some legitimacy upon the Chinese Communist Party's model of restrictive internet control. But a number of notable hardware, semiconductor, and cloud service companies sent representatives, including Qualcomm, Intel, Microsoft, and Cisco; they joined Chinese tech executives from Alibaba and Baidu. Amid heightened US-China trade tensions and renewed concerns over how Chinese economic ties affect free speech abroad, watch for any fallout for these companies as a result of their participation, or examples of how their attendance influences their business practices.

- **China-Russia treaty on combating "illegal" content online:** On October 8, Reuters reported that China and Russia were planning to sign a treaty later in the month aimed at joining efforts to combat "illegal" content online, based on reports from a Russian state communications agency. Watch for confirmation that the treaty had been signed, any details on its provisions, and emerging evidence of its implementation, including increased Russian efforts to censor political and religious content within its borders on topics that might be deemed sensitive to the Chinese Communist Party.

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 in China, see: *Freedom in the World 2018*, *Freedom of the Press 2017*, *Freedom on the Net 2018*, 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