



Respecting Rights in Responding to the CCP's Influence Campaign through Social Media

Written Testimony by Yaqiu Wang

Research Director for China, Hong Kong, and Taiwan at Freedom House

Testimony before the US House Representatives Select
Committee on the Chinese Communist Party

"Discourse Power: the CCP's Strategy to Shape the Global Information Space."

November 30th, 2023

Chairman Gallagher, Ranking Member Krishnamoorthi, and distinguished members of the committee, thank you for convening this hearing on the Chinese Communist Party's strategy to shape the global information space, a growing issue that the US authorities need to address before the CCP's narratives take hold among the American public.

This testimony draws on Freedom House's years of research on Beijing's global influence campaigns, including a comprehensive study released in September 2022 examining actions taken by the Chinese government and its affiliates to influence information flows abroad in 30 countries.¹ That study found that Beijing's media influence efforts were High or Very High in 16 out of the 30 countries surveyed.

The good news is, in the realm of global public opinion, the CCP is not succeeding at creating a positive narrative for the People's Republic of China abroad. Pew Research Center studies this year show that views of China are broadly negative across 24 countries it surveyed: 67% of adults express unfavorable views while 28% have a favorable opinion.² Moreover, the US is viewed far more positively than China across the 24 countries surveyed, especially in high-income countries.³ Within the US, a Gallup poll in March shows that a record-low 15% of Americans view China favorably.⁴

¹ Sarah Cook, Angeli Datt, Ellie Young, BC Han, Beijing's Global Media Influence, Freedom House, 2022, <https://freedomhouse.org/report/beijing-global-media-influence/2022/authoritarian-expansion-power-democraticresilience>.

² Laura Silver et al., "China's Approach to Foreign Policy Gets Largely Negative Reviews in 24-Country Survey," Pew Research Center, July 27, 2023, <https://www.pewresearch.org/global/2023/07/27/chinas-approach-to-foreign-policy-gets-largely-negative-reviews-in-24-country-survey/>.

³ Laura Silver et al., "Comparing Views of the U.S. and China in 24 Countries," Pew Research Center, November 6, 2023, <https://www.pewresearch.org/global/2023/11/06/comparing-views-of-the-us-and-china-in-24-countries/>.

⁴ Megan Brenan, "Record-Low 15% of Americans View China Favorably," Gallup News, March 7, 2023, <https://news.gallup.com/poll/471551/record-low-americans-view-china-favorably.aspx>.

Such growing negative views correspond with the CCP's worsening repression inside the PRC, including crimes against humanity in Xinjiang, and more aggressive activities abroad, including the world's largest campaign of transnational repression. It is also a result of investments in independent expertise, investigative journalism, and local laws protecting press freedom that help shield reporters from CCP retribution for their work. This attests to the high degree of resilience among democracies to Beijing's disinformation and influence efforts.

That being said, there is no indication that the CCP plans to rein in its operations. In fact, Freedom House and other civil society organizations, tech companies, and cybersecurity firms have all found that Beijing is not only spreading its disinformation across many more platforms, languages, and geographic audiences, it is also experimenting with tactics that are more sophisticated and harder to detect.⁵

In August, Meta reported that it had taken down thousands of accounts and Facebook pages that "were part of the largest known cross-platform covert operation in the world," run by "geographically dispersed operators across China."⁶ A September report by Microsoft found an emerging use of images that were created with generative artificial intelligence (AI) tools.⁷ In November, a report by the Australian Strategic Policy Institute shows the CCP is increasingly using foreign social media influencers to reach younger media consumers globally.⁸

While some disinformation campaigns have struggled to gain genuine engagement from social media users, other recent initiatives have scored more success. Government scrutiny, transparency reports by tech companies, and investigations by third parties have uncovered many disinformation campaigns originating from China. But inconsistency in monitoring and takedowns has been found across platforms.

Given the reach of social media platforms and their design to encourage constant user engagement and viral content, we should be especially vigilant about risks for CCP influence through social media platforms. Below are three such platforms that warrant special attention at the moment:

⁵ Sarah Cook, "China's Increasingly Aggressive Tactics for Foreign Disinformation Campaigns," *Diplomat*, September 18, 2023, <https://thediplomat.com/2023/09/chinas-increasingly-aggressive-tactics-for-foreign-disinformation-campaigns/>.

⁶ Guy Rosen, "Raising Online Defenses Through Transparency and Collaboration," Meta, August 29, 2023, <https://about.fb.com/news/2023/08/raising-online-defenses/>.

⁷ Microsoft, "Sophistication, scope, and scale: Digital threats from East Asia increase in breadth and effectiveness," September 2023, <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW1aFyW>.

⁸ Fergus Ryan et al., "Singing from the CCP's songsheet," Australian Strategic Policy Institute, November 24, 2023, <https://www.aspi.org.au/report/singing-ccps-songsheet>.

WeChat, owned by Chinese tech giant Tencent and heavily used among the Chinese diaspora. Many first-generation Chinese outside the country rely on WeChat exclusively for their information.⁹ Independent researchers, media groups, and civil society organizations have documented how WeChat users outside of China face censorship and surveillance when using the platform.¹⁰ In August, the Canadian government disclosed a network on WeChat engaged in a coordinated campaign to smear the reputation of Parliament member Michael Chong, who has been a vocal critic of Beijing.¹¹ WeChat has yet to share information about campaigns that others have detected on their platform.

X, formerly Twitter, now wholly owned by Elon Musk. Under its new leadership, X has dismantled many of the policies and teams that had increased transparency and thwarted inauthentic behavior on Twitter.¹² In addition, Musk may be particularly vulnerable to pressures from Beijing because he has significant business interests in China and the CCP is deft at leveraging foreign businesses' access to the country to compel them to toe the Communist Party line.¹³ China is Tesla's second-largest market and Tesla's plant in Shanghai is the world's largest electric vehicle factory and the company's primary export hub. Musk's close relationship with the CCP was on display in November during a meeting with President Xi Jinping in which he expressed gratitude to Xi for his support to Tesla's China operation and pledged to "dive deep in China."¹⁴

TikTok, owned by the Chinese company ByteDance. All Chinese social media companies, private or public, are subjected to the control of the CCP, which creates an opportunity for Chinese government censorship, surveillance, and propaganda that affect not only their China-based users, but those around the world.¹⁵

⁹ Yaqiu Wang, "WeChat Is a Trap for China's Diaspora," *Foreign Policy*, August 14, 2020, <https://foreignpolicy.com/2020/08/14/wechat-ban-trump-chinese-diaspora-china-surveillance/>.

¹⁰ Miles Kenyon, "WeChat Surveillance Explained," Citizen Lab, May 7, 2020, <https://citizenlab.ca/2020/05/wechat-surveillance-explained/>.

¹¹ "WeChat account activity targeting Canadian parliamentarian suggests likely foreign state involvement," Government of Canada, accessed November 28, 2023, <https://www.international.gc.ca/transparency-transparence/rapid-response-mechanism-mecanisme-reponse-rapide/wechat.aspx?lang=eng>.

¹² "Twitter disbands Trust and Safety Council," Axis, updated December 13, 2022, <https://www.axis.com/2022/12/13/twitter-disbands-trust-safety-council>.

¹³ Yaqiu Wang, "Why Twitter under Elon Musk is good news for China's rulers," Al Jazeera, November 2, 2022, <https://www.aljazeera.com/opinions/2022/11/2/twitter-elon-musk-china-rulers-tesla>.

¹⁴ Musk-Xi Meeting Shows Tight Relationship China Has With Tesla," Bloomberg, November 16, 2023, <https://www.bloomberg.com/news/articles/2023-11-16/musk-xi-meeting-shows-tight-relationship-china-has-with-tesla>.

¹⁵ Human Rights Watch (HRW), "US: Urge TikTok to Enhance Transparency," March 20, 2023, <https://www.hrw.org/news/2023/03/20/us-urge-tiktok-enhance-transparency>.

TikTok has been found suppressing content critical of the Chinese government in some instances.¹⁶ It has also tracked journalists covering the company's links to China by accessing their data on TikTok.¹⁷ TikTok acknowledged removing hundreds of accounts linked to the aforementioned Meta-exposed network, but only after being queried by reporters.¹⁸

In this context, Freedom House calls on Congress to:

- Enact regulations that require transparency from all social media platforms, including disclosure of their content moderation, recommendation and algorithmic systems, and what content they have censored, suppressed, or promoted at the request of governments.
- Hold a hearing to examine questions regarding Tencent's data protection and content moderation on WeChat as they relate to US-based users.
- Continue to provide funding to civil society initiatives around the world documenting and addressing Beijing's foreign media influence activities and for strengthening local resilience.

Thank you. I look forward to your questions.

¹⁶ Drew Harwell and Tony Roma, "TikTok's Beijing roots fuel censorship suspicion as it builds a huge U.S. audience," *Washington Post*, September 15, 2019, <https://www.washingtonpost.com/technology/2019/09/15/tiktoks-beijing-roots-fuel-censorship-suspicion-it-builds-huge-us-audience/> ; Lily Kuo, "TikTok sorry for blocking teenager who disguised Xinjiang video as make-up tutorial," *The Guardian*, November 28, 2019, <https://www.theguardian.com/technology/2019/nov/28/tiktok-says-sorry-to-us-teenager-blocked-after-sharing-xinjiang-videos> ; David Lee, "TikTok apologises and reinstates banned US teen," British Broadcasting Corporation (BBC), November 27, 2019, <https://www.bbc.com/news/technology-50582101>.

¹⁷ Emily Baker-White, "EXCLUSIVE: TikTok Spied On Forbes Journalists," *Forbes*, December 22, 2022, <https://www.forbes.com/sites/emilybaker-white/2022/12/22/tiktok-tracks-forbes-journalists-bytedance/?sh=a5740f47da57>.

¹⁸ Josh Taylor, "TikTok removes 284 accounts linked to Chinese disinformation group," *The Guardian*, August 31, 2023, <https://www.theguardian.com/technology/2023/aug/31/tiktok-removes-284-accounts-linked-to-chinese-disinformation-group>.

The following materials from relevant Freedom House reports are appended below:

Key findings from the US chapter of Freedom House’s report *Beijing’s Global Media Influence: Authoritarian Expansion and Power of Democratic Resilience*, published in May 2023:¹⁹

- **Increased use of covert and coercive tactics:** The methods deployed by Chinese state actors to influence the US media space have evolved since 2019. Disinformation campaigns, the use of paid social media influencers, cyberattacks on news outlets, and cyberbullying of journalists have occurred with greater frequency as Chinese state media outlets struggle to gain a mainstream audience in the United States, and US public opinion toward Beijing became more negative.
- **Limited impact:** Mainstream media coverage in the United States is broadly independent and critical of the Chinese Communist Party (CCP). Outlets commonly feature reporting on rights abuses, alternative perspectives from China, including accounts by victims of persecution, and investigations of Chinese companies and CCP political or media influence in the country. Narratives preferred by Beijing have gained some traction and repetition on the extremes of the political spectrum (both left and right) and among some state and local political and business leaders. For the most part, however, public opinion across the political spectrum is broadly unfavorable toward the Chinese regime, and aggressive messaging from Chinese officials tends to backfire (see Impact).
- **Paid inserts, local radio programming, and video partnerships:** Chinese state media content reaches news consumers in the United States directly through offline and online paid inserts from *China Daily* or the Xinhua news agency in national and regional news outlets, such as *Time* magazine, the *Los Angeles Times*, *USA Today*, CNN, and *Foreign Policy*. Filings with the Department of Justice indicate that from January 2019 to October 2021, *China Daily* paid print and online publications at least \$7 million to carry such material. At least two radio stations in the Washington, DC, and New York City areas broadcast China Radio International (CRI) programming. The clarity and frequency of labeling attached to the Chinese state content for US news consumers is inconsistent. During the coverage period, several major news outlets—notably the *New York Times* and the *Washington Post*—discontinued previous agreements on paid inserts.

¹⁹ Freedom House, “United States,” in *Beijing’s Global Media Influence 2022*, <https://freedomhouse.org/country/ united-states/beijings-global-media-influence/2022>.

Newswires offering video content and information providers like Discovery and National Geographic, have also established content sharing or coproduction partnerships with Chinese state entities, although the content reaching US audiences from these agreements remains limited (see Propaganda).

- **Broad influence efforts, including subsidized press trips:** Beijing maintains an arsenal of tactics and channels to influence the US information landscape. Diplomats publish op-eds and appear in interviews in mainstream news outlets; vloggers are approached with payment and travel opportunities; and CCP–friendly entities and companies like Huawei and the China-United States Exchange Foundation (CUSEF) subsidize trips for reporters and other opinion leaders to China. Many of these activities are aided by US-based public relations firms in exchange for generous payments from CCP-linked entities. Even as regulators have restricted the presence of Chinese state-owned firms in the US telecommunications infrastructure, social media applications owned by China-based companies with track records of censorship and surveillance within China, notably Tencent’s WeChat and ByteDance’s TikTok, have gained a large following among US users (see Propaganda, Disinformation campaigns).
- **Emerging disinformation campaigns:** Multiple disinformation campaigns targeting US audiences were documented during the coverage period. Thousands of fake accounts on Twitter, Facebook, and YouTube were detected and shuttered for inauthentic behavior, including manipulation of the discourse about events within China (such as prodemocracy protests in Hong Kong and rights abuses in Xinjiang), US relations with Taiwan, the reputation of US-based critics of the Chinese Communist Party, and domestic issues like COVID-19 or US political divisions. Genuine user engagement with the accounts and their impact on public debate appeared limited, but isolated examples reached mainstream audiences. No such campaigns were documented prior to 2019 (See Disinformation campaigns).
- **Wide-ranging censorship efforts:** State-linked actors have deployed a relatively wide range of tactics in an attempt to restrict coverage opportunities for US correspondents in China, inhibit the operations of news outlets, and induce self-censorship. These include obstructing the movement of foreign correspondents, restricting their visas and expelling them from the country, blocking websites and apps in China, retaliating against the families of US-based journalists in China, and engaging in cyberattacks against major news outlets. Increasingly, online actors have verbally attacked or trolled ethnic Chinese journalists working for US media, especially women. These activities have inhibited certain reporting and had a notable economic impact on US news outlets, though they continue to carry critical coverage (see Censorship).

- **Control over diaspora media:** Chinese Communist Party–linked media—especially state broadcaster Chinese Central Television (CCTV) and the pro-Beijing Phoenix TV—retain a strong foothold among Chinese-speaking communities in the United States, as do several pro-Beijing newspapers. WeChat is widely used among the diaspora, and some Chinese Americans—political dissidents, journalists, and average users—have reportedly faced censorship on the platform for sharing content that is critical of the party. Several mainstream US outlets have Chinese-language editions online, while other US-based outlets founded by Chinese Americans continue to publish news on the internet, on television and radio, and in print that is critical of the Chinese Communist Party. They often host political debates and cultural activities (see *Diaspora media*).
- **Robust civil society and government response:** A high level of expertise on China in academic and national media circles, bipartisan public skepticism about the Chinese regime, and a strong legal infrastructure contribute to a high degree of resilience in the face of Chinese Communist Party influence efforts. Laws governing foreign-agent registration and investment screening have been applied to Chinese media influence efforts, and strong legal protections against defamation suits support investigative journalism. Political leaders and government agencies have shown increasing awareness of the potential security challenges posed by Chinese Communist Party media influence, holding congressional hearings and creating new bureaucratic initiatives and government policies to address the problem. For example, since February 2020, the US government has treated Chinese state media operations as extensions of China’s diplomatic missions in the country. News reporters, civil society groups, and technology firms have taken steps to monitor media influence and disinformation, uncovering networks of fake accounts and amplifying filings on paid inserts (see *Resilience*).
- **Vulnerabilities and problematic pushback:** Enforcement of laws like the Foreign Agents Registration Act (FARA), which enhance transparency surrounding Chinese state media activities, remains incomplete, and interagency coordination on how to respond to the Chinese Communist Party’s efforts to influence US politics is nascent. Political polarization and growing distrust in news outlets that are seen as aligned with specific political parties create a fertile environment for disinformation campaigns aimed at enhancing societal divisions, and for domestic actors to repeat talking points from Beijing, even if inaccurate, in pursuit of perceived political gain over their rivals. Growing anti-China sentiment during the COVID-19 pandemic is believed to have contributed to verbal and physical attacks against Asian Americans, while public opinion polling of Chinese and Taiwanese Americans on relevant topics is lacking (see *Vulnerabilities*).

Key findings from Freedom House’s *China Media Bulletin*’s review of forensic investigations, think tank reports, platform transparency reports, and media coverage published between June and September 2023:²⁰

- **Expansion to New Platforms and Audiences:** The first documented Beijing-backed global disinformation campaigns dated to 2017, and typically targeted English and Chinese speakers on large platforms like Twitter (now X), Facebook, and YouTube. But recent reports show that the Chinese Communist Party (CCP) regime’s manipulation efforts are spreading across many more platforms, languages, and geographic audiences.

The network identified in Meta’s August takedown – a persistent revival of a previously exposed and thwarted network known as Spamouflage – notably extended beyond Facebook and Instagram. Links were found to some 50 other applications, including TikTok, Reddit, Pinterest, and Medium, as well as local online forums in Asia and Africa. Meta suggested that the pivot to smaller platforms may have been a deliberate response to larger firms’ increased monitoring, detection, and removals.

A separate report published by Microsoft on September 7 uncovered a range of influence efforts, from networks of fake accounts to a corps of Chinese state-linked influencers who masquerade as independent commentators. The company counted at least 230 such state media employees or affiliates across multiple platforms, with accounts that reached 103 million people using 40 different languages. The report described an expansion to new languages – like Indonesian, Croatian, and Turkish – and new platforms – including Vimeo, Tumblr, and Quora – by both human influencers and automated accounts over the past year.

- **More Sophisticated Tactics for Increasing Engagement and Avoiding Detection:** While some networks, like the one exposed by Meta, have apparently struggled to gain genuine engagement from social media users, other recent initiatives have scored more success. The Microsoft report found an emerging use of images that were created with generative artificial intelligence (AI) tools and shared as memes by accounts mimicking U.S. voters from across the political spectrum. Such images, despite their recognizable AI

²⁰ Freedom House, “Analysis: Beijing’s Increasingly Aggressive Tactics for Foreign Disinformation Campaigns” in *China Media Bulletin* 2022, no. 173 (September 2023), <https://freedomhouse.org/report/china-media-bulletin/2023/new-tactics-foreign-disinformation-anti-espionage-campaign-party#analysis>.

flaws, have reportedly garnered additional circulation by real users. Indeed, video and other visual media are a recurring feature of the content now being shared, according to the report.

Other effective tactics include exploiting popular hashtags related to current events, as has occurred in campaigns on Australian political issues, or programming fake accounts to post comments in the first person.

Another tactic uses unattributed images to avoid easy detection of a link to Chinese state media. An investigation by the cybersecurity firm Nisos found that a network of accounts in Spanish and Portuguese, which had not been labeled as Chinese state media under Twitter's former policy, posted screenshots of state media articles or used images and videos from the China News Service without attribution. In another case, the Australian Strategic Policy Institute (ASPI) found that Beijing-backed disinformation networks were replenishing their ranks after account takedowns by purchasing fake personas from transnational criminal organizations in Southeast Asia, and using them to post false or divisive content.

- **Elaborate Schemes to Launder Content and Narratives:** Among the most striking discoveries from the recent set of investigations are the various ways in which proxy entities or accounts on multiple platforms are used to “launder” content, increasing its credibility and obfuscating its origins to the point that even some people involved in its production are unaware.

One example unveiled in the Meta investigation centered on an error-laden, 66-page “research report” claiming that the U.S. government was hiding the origin of COVID-19. The document was published on Zenodo.org, then promoted by fake accounts via two distinct videos on YouTube and Vimeo; an article based on those items was then posted on LiveJournal, Medium, and Tumblr, and finally, accounts on Facebook, X, Reddit, and other platforms amplified these links.

In another notable set of incidents revealed by the cybersecurity firm Mandiant in July 2023, a Chinese public relations firm known to have ties to the government piggybacked on recruitment websites for freelancers and newswire services in the United States. This enabled them to enlist unwitting Americans to create content that aligned with CCP

narratives or criticized U.S. policies. The firm published the resulting material on legitimate news website domains via the newswire services.

In one case from mid-2022, the public relations firm successfully recruited a musician and actor to organize small real-world protests in Washington, D.C., images of which were then circulated as part of an influence campaign to discredit that year's International Religious Freedom Summit and U.S. lawmakers' efforts to ban the importation of products made by Uyghur forced labor.

- **Use of Smears and Incitement to Discredit Factual Reporting and Disrupt Democratic Societies:** In terms of topical focus, these disinformation campaigns have apparently doubled down on a long-term strategy aimed at moving beyond simple pro-CCP messages and actually attempting to amplify discord on key political and social issues, or to damage the reputations of activists, journalists, policymakers, and democratic governments.

The network that was active on Meta platforms sought to harass or discredit journalists in the United States (such as Jiayang Fan), political commentators and dissidents (such as Chen Pokong), and occasionally elected officials (including Republican Representative Jim Banks and Democratic Representative Nancy Pelosi). In an incident from May that was exposed in August by the Canadian government, a network on Tencent's WeChat platform engaged in a coordinated campaign to smear the reputation of Parliament member Michael Chong, whose father is from Hong Kong and who has been a vocal critic of the increasing repression there and in China.

The disinformation networks have also taken aim at think tanks and other nongovernmental organizations whose investigations of the CCP's transnational repression and disinformation campaigns have been especially effective at spurring public awareness and policy responses. These include the Madrid-based Safeguard Defenders and ASPI, which have been subjected to aggressive and wide-ranging campaigns of harassment, threats, and impersonations. ASPI found that 70 percent of the top 50 Chinese-language search results for the organization's name on YouTube had been "posted by CCP-linked inauthentic accounts."

With respect to divisive topics, the AI-generated memes discovered by Microsoft revolved around issues like gun violence and the Black Lives Matter movement in the United States. ASPI's research is replete with examples of China-linked fake accounts

trying to influence public discourse on domestic social issues such as gender, sexual assault, and Indigenous people’s rights. The accounts have also tried to amplify public frustration over cost-of-living pressures and false scandals targeting Australian institutions like political parties, Parliament, and the banking system.

- **New Vulnerability to Exposure and Pushback:** CCP propagandists have good reason to put greater energy into hiding their disinformation efforts. Thanks in part to the accumulating results of investigations into the tactics now associated with China-linked campaigns, as well as a recent set of U.S. federal indictments that clarified links between networks of fake accounts and China’s Ministry of Public Security, it is becoming easier for observers to trace and attribute specific campaigns to Beijing.

Meta and Microsoft, for example, were able to make relatively definitive attributions, relying on common patterns of posting, the locations of account operators, the use of common proxy or server infrastructure, or information available on the Chinese internet regarding the government ties of public relations companies, cybersecurity firms, and fake news websites. The Canadian government found it “highly probable” that the campaign against Chong was linked to Beijing, while ASPI said the behavior it documented was similar to that of previously exposed CCP-linked covert networks.

Despite the exposure, however, there is no indication that the Chinese regime plans to rein in its manipulation. In fact, it is almost certainly gearing up for more aggressive activity centered on the 2024 presidential elections in the United States and Taiwan.

The recent assessments noted above highlight some of the strengths in current democratic responses that help safeguard the integrity of online communications and political processes, including tech firms’ transparency reports, government monitoring, and investigations by cybersecurity firms. But they also spotlight vulnerabilities, such as the inconsistency of monitoring and takedowns across platforms, particularly newer and more niche services, and the extent to which CCP-linked networks take full advantage of these gaps.

Under its new leadership, X has dismantled many of the policies and teams that had increased transparency and thwarted inauthentic behavior on Twitter. Meanwhile, TikTok, owned by the China-based ByteDance, acknowledged removing hundreds of accounts linked to the Meta-exposed network, but only after being queried by reporters.

WeChat, an app of Chinese tech giant Tencent, has yet to share information about campaigns that others have detected on their platform.

Key Freedom House recommendations on countering Beijing's information and influence operations:

- **Maintain strong funding for media development generally and for documenting Beijing's foreign media influence activities and strengthening local resilience specifically.** These areas have seen increased and strategic support from various US government funders in recent years, helping to raise awareness and enhance resilience to Beijing's authoritarian influence and other threats to free expression. Congress should ensure continued bureaucratic and funding support for such programming globally. Private philanthropists should expand support for civil society research, advocacy, training, and media literacy programs that enhance the United States' own resilience in the face of CCP influence efforts, including among Chinese speakers. Private resources for these activities are especially important given the limited availability of public funding.
- **Improve reporting on China through training, networking opportunities, and funding for journalists, while incorporating China-related topics into broader programming.** Given the global role that Chinese state-linked actors are playing in the media and information space, professional training programs for journalists and other media workers should include background material on China and its regime as well as case studies on CCP propaganda and censorship tactics around the world. To counteract the factually incorrect or incomplete information provided to journalists at Beijing-backed junkets and training programs, democratic donors should sponsor journalist travel and networking opportunities, including engagement with Chinese human rights defenders and representatives of ethnic and religious groups that face persecution in China. Programs tailored to improve expertise on China could provide background information on the different Chinese state media outlets and their ties to the CCP, examples of past disinformation campaigns, and China-based apps' track record of surveillance and censorship within China.
- **Include Chinese-language media and speakers in funding opportunities and media literacy programs.** Media literacy initiatives should include components that serve Chinese-language news consumers and equip them to identify problematic content on WeChat and other CCP-influenced information sources. Donors should support investigative journalism initiatives among diaspora and exile media serving Chinese-speaking communities. They should also finance research dedicated to tracking self-

ensorship and other subtle pressures on media outlets. Any projects focused on supporting Chinese-language media should include those serving diaspora, immigrant, and exile communities, providing dedicated funding for the latter.

- **Impose penalties for transgressions by Chinese officials.** When CCP representatives—including Chinese diplomats in the United States—engage in bullying, intimidation, or other pressure aimed at local journalists and commentators, the US government should respond promptly, for instance by issuing public statements of concern or diplomatic rebukes. In especially serious cases involving threats against journalists and their families, the government should consider declaring the perpetrators persona non grata, and, if necessary, prosecute in accordance with the law. The US government should also deploy targeted sanctions against Chinese officials for the use of transnational repression and screen Chinese diplomats for a history of harassing diaspora members in their postings. US officials—at the highest levels—should publicly condemn assaults on or obstruction of correspondents from US media in China, including the delay or denial of visas, and continue to pursue the matter until a satisfactory resolution is reached.
- **Enhance interagency and multistakeholder coordination.** The federal government should expand recent efforts to improve interagency coordination related to China’s foreign media influence and targeted disinformation campaigns, particularly in advance of national and local elections. Congress should ensure that such agencies and activities are sufficiently funded. Civil society, technology firms, and media outlets should be routinely consulted on emerging trends and to coordinate effective responses.
- **Align US government designations of Chinese state media, enhance transparency mechanisms.** The Department of Justice should examine each of the Chinese state media outlets that have been designated as foreign missions by the Department of State since 2020 to determine whether those outlets should also be registered under FARA. For newly registered Chinese state outlets such as China Global Television Network and Xinhua, the Department of Justice should enforce FARA filing requirements, including submission of details on content partnerships with US media and payments to social media influencers, to the extent possible under current law.
- **Take action against transnational repression.** This should include codifying a definition of transnational repression and providing training for government officials, including law enforcement, who may encounter transnational repression cases. Several agencies including the FBI, Department of State, and Department of Homeland Security have begun instituting trainings, but they vary in consistency and content. Coordinated, mandated requirements across agencies could help ensure officials are equipped with matching and sufficient

information to help protect those at risk and not unwittingly become a player in an authoritarian regime's campaign of transnational repression. US government agencies should also conduct strategic, consistent, and culturally sensitive outreach to communities that are at risk of experiencing transnational repression from the CCP in order to equip them with the resources to report these activities. From this perspective, Freedom House supports adoption of the Transnational Repression Policy Act, which includes a number of important provisions around sanctions, support for victims, reporting, and training for officials.

- **Increase Chinese-language capacity in federal agencies.** As we have engaged with federal agencies over the years, it has become clear that there is a need for Mandarin language skills, including in key offices handling China-related issues. The federal government, with new funding from Congress, if necessary, should employ additional Chinese speakers at key US agencies that deal with CCP media influence.
- **Increase Congressional scrutiny of WeChat censorship and surveillance in the United States.** Tencent's WeChat application and the company's politicized moderation and monitoring actions pose a serious threat to the privacy and free expression of millions of U.S. residents and citizens, particularly Chinese speakers. Yet, information available to the public and to U.S. policymakers about the full extent of this phenomenon is lacking. Congress should hold a hearing to shed greater light on the challenges experienced by users in the United States and include among witnesses Chinese activists and ordinary users who have encountered censorship on the platform in the United States, as well as executives from Tencent. Members of Congress should also write formal letters to Tencent asking explicit questions regarding its data protection, moderation, and official account policies as they relate to users in the United States.
- **Explore a diverse set of responses other than blanket bans when seeking to reduce the vulnerabilities to manipulation and surveillance posed by some apps:** Recognizing both the potential threat posed by PRC-based applications like WeChat or ByteDance's TikTok, but also the disproportionate restriction on freedom of expression that a blanket ban would entail, the US government should first explore other options for addressing the concerns raised by these applications, including: holding hearings, introducing third-party risk assessment audits, restricting usage on government or military devices, and adopting laws that require more transparency on company policies and practices and limit the collection and use of personal data.
- **Address disproportionate data collection and use by social media platforms, including WeChat and TikTok, by promulgating stronger privacy regulations and enacting comprehensive data protection legislation.** Congress should adopt stronger

data privacy laws that limit what can be collected and how it can be stored, used, and shared. Companies should be required to limit the collection of consumer data, particularly intimate information such as health, biometric, and location data, disclose in plain language how they use data they do collect, and limit how third parties can access and use this data. Laws should include guardrails that limit the ways in which social media platforms can use personal data in their AI systems, including algorithmic recommendations, which can reduce the reach of state propaganda campaigns that rely on microtargeting users based on personal characteristics. Updated data-privacy protections should include provisions that provide independent regulators and oversight mechanisms, such as the Federal Trade Commission (FTC), with the ability, resources, and expertise needed to enforce and ensure foreign and domestic companies comply with privacy, nondiscrimination, and consumer-protection laws. Commission should also explore what options exist for improving protections for Americans data under existing authority.

- **Enhance transparency about how social media platforms function and their impact on information integrity.** Legal frameworks addressing online content should establish special obligations for companies tailored to their size and their services, incentivize platforms to improve their own standards, and require human rights due diligence and reporting. Such requirements should prioritize transparency across core products and practices, including content moderation, recommendation and algorithmic systems, collection and use of data, and political and targeted advertising. Laws should also provide opportunities for vetted researchers to access and study platform data—information that can provide insights for policy development, spur additional legislative and regulatory scrutiny, and inform civil society’s analysis and advocacy efforts.