1630 Connecticut Avenue, N.W., Suite 500
Washington, DC 20009
Tel: 202-612-4321
Fax: 202-612-4333; 202-478-2988

HUMAN RIGHTS WATCH

HRW.org

July 18, 2016

Mr. Mark Zuckerberg
Chairman and Chief Executive Officer
Facebook

Dear Mr. Zuckerberg:

We write to express our concern about the significant risks associated with Facebook's possible entry into China. Though Facebook remains blocked in the country, we understand that your firm has engaged local partners for your advertising services. You have also sought ties inside and outside China with senior Chinese government officials. As you consider whether and how to operate in China, we urge you to be certain that your operations will neither assist nor enable Chinese authorities in censoring peaceful expression, conducting abusive surveillance, or retaliating against netizens who wish to use Facebook to "share and make the world more open and connected."[i] Given China's worsening human rights climate and a regulatory regime that requires companies to conduct censorship and surveillance, Facebook's formal entry would entail considerable risk of it becoming complicit in serious human rights abuses. The company should not proceed without publicly clarifying how it will approach these issues and taking a strong stance in support of freedom of expression and user privacy.

Human Rights Watch is an international nongovernmental organization that monitors and reports on human rights abuses in some 90 countries around the world. We have documented abuses and advocated for redress in China for more than two decades, and similarly defended the freedom of expression and privacy online for over a decade. In the course of our work, we have had to opportunity to engage with Facebook on a range of issues related to online censorship and privacy, including through the Global Network Initiative (GNI).

Netizens across China have made remarkable use of the Internet and social media to publicize injustices, access and share information, and mobilize public opinion, vigorously embracing the only relatively free public space available to them. Through discussing public events like the Tianjin warehouse blast in 2015, the Wenzhou train crash in 2011, or unsafe consumer products, such as the 2008 melamine baby formula scandal, people across the country have

collectively pushed for greater accountability and transparency from their government.

Since assuming leadership in March 2013, however, President Xi Jinping's government has reversed gains in freedom of expression and presided over the most severe assault on human rights in two decades. The government has moved aggressively to limit free expression and the activities of civil society. It has severely restricted access to virtual private networks (used by some netizens to access blocked content), further compelled bloggers to register with their real name so they can be identified and targeted, and pressured companies to store user data locally so that it is more accessible to law enforcement. In 2014, Instagram was reportedly blocked in mainland China as pro-democracy protesters used it to document the Umbrella Revolution protests.[ii]

The government views the Internet as a threat to its power, "the primary battlefield for ideological struggle," and believes all media should serve to "protect the [Chinese Communist] Party's authority and unity."[iii] Its long-term strategy has been and remains protecting domestic Internet companies in China, monitoring and punishing online critics, and retaining as much control as possible over what information users may share and access.

To implement Beijing's goals, the government enlists Internet companies, foreign and domestic, to disclose user data and ensure technologies are "secure and controllable." In 2015, the government passed several new security laws that require Internet firms, including foreign ones, to censor content and verify the identity of customers.[iv] Authorities also stated they plan to embed police within major domestic Internet companies to combat "malicious" online content.[v] In May 2016, the Ministry of Public Security enlisted Sina Weibo to launch an online platform for identifying and investigating "rumors" on the service, potentially leaving Weibo users more vulnerable to abuse if they share independent information that deviates from official narratives.[vi] All technology firms, including foreign firms, are required to assist with broad surveillance powers and law enforcement access to data to investigate online crimes, with no real safeguards or legal controls.

Such expanded surveillance powers come at a particularly dangerous time for social media users. In September 2013, the government issued a new judicial interpretation expanding existing law to punish expression online.[vii] In recent years, the Chinese government has cracked down on "rumors" by targeting netizens who share independent information on subjects as varied as air pollution, industrial disasters, or stock market troubles on social media.[viii] Authorities have targeted for detention and imprisonment well-known online commentator Charles Xue and other popular social media personalities, known as "Big Vs," on Weibo and have closed down popular public accounts on WeChat.[ix] In December 2015, one of China's best-known human rights lawyers, Pu Zhiqiang, was found guilty of "picking quarrels and

stirring up troubles" and "inciting ethnic hatred" for comments he made on social media, including comments that criticized government crackdowns on ethnic minorities.[x] The laws used by the government in these cases penalize peaceful expression in ways that are inconsistent with China's human rights obligations.

While Facebook's goal may be to enable users in China to express themselves, authorities there will see Facebook's products as an invaluable platform for surveillance and yet another arena for information control. Recently adopted laws, clear political intent, and longstanding government practice make clear that Facebook will be asked to aid abuses against its users.

In this context, the company should undertake extensive human rights due diligence and implement clear human rights protections to ensure that its operations do not contribute to or exacerbate an already dire human rights environment. Broad assumptions that the Chinese people would be better off with than without Facebook are no substitute for these essential precautionary measures—both to avoid Facebook's complicity in Chinese abuses and to ensure that Facebook's presence is really a net plus for the Chinese people.

To that end, we ask that you publicly disclose information on any human rights policies or procedures that Facebook will implement to protect users in China. This includes policies in place globally, as part of its commitments as a GNI member, and those specific to China. In addition, we have specific questions about your possible operations in China, including:

1) **Protection of user data and "authentic identity" policy**: Facebook holds highly sensitive information about users' contacts and networks, affiliations, location and movements, and the contents of private communications. The government would seek access to such information, potentially as part of abusive prosecutions of peaceful expression, among other risks. In addition, the company's "authentic identity" policy exacerbates the danger that Facebook will contribute directly to human rights abuses in China because it prevents users who may share politically sensitive content from using pseudonyms. Facebook's "authentic identity" policy requires individuals to use their "authentic name," one that is commonly used by family and friends, but that would also be found on certain types of identity documents. Human rights organizations, including HRW, have long criticized this policy because it can chill online expression.[xi] The policy is also likely to be disproportionately enforced against those already at risk of reprisals, including at-risk minorities and online activists.[xii]

    a) How will Facebook protect its users in China from reprisals for their online activity?
    b) How will Facebook respond to data localization requirements, formal or informal, to store user data inside the country?

c) Given the government's current crackdown on social media users, how will Facebook respond to government requests for user information and how will the company assess such requests in order to prevent the government from using Facebook's user data to silence, intimidate, and punish independent voices?

2) **Censorship of content**: The Chinese government requires Internet companies to censor content on its behalf through both legal and informal pressure. Chinese social media companies employ hundreds (if not thousands) of content "censors" to monitor and take down content that could run afoul of the government's vaguely worded requirements, often doing so proactively without waiting for a request that identifies specific posts.

   a) How will Facebook respond to China's censorship requirements, and will the company proactively take down content in the absence of a specific government request that identifies particular posts deemed unlawful?
   b) How will Facebook staff resist pressures, formal and informal, to limit access to content in the absence of a specific government directive?
   c) What type of infrastructure will Facebook have to put into place to comply with Chinese laws and regulations?
   d) If Facebook offers the same version of its service that is available globally, rather than a domestic Chinese version, how will Facebook ensure government censorship requirements do not affect access to posts by users outside China?
   e) Will Facebook commit to notifying users when specific content they attempt to access has been censored under Chinese law?

3) **Encryption and "technical assistance"**: Human Rights Watch welcomes WhatsApp's decision to implement end-to-end encryption for its global user base. We encourage Facebook to refrain from retaining WhatsApp message metadata, which could be disclosed at the request of governments.

   China's new counterterrorism law, passed in December 2015, is also drafted broadly enough to potentially require companies to build "back doors" into secured systems or retain encryption keys and make them available in counter-terrorism investigations, as well as provide other kinds of unspecified "technical assistance."[xiii]

   a) Will Facebook offer WhatsApp in China in its current, end-to-end encrypted form?
   b) How will you respond if the government asks for technical assistance to circumvent or re-design security features in WhatsApp, Messenger, or other Facebook products?

c) How will the company respond to requests for source code or invasive "security audits"?

4) **Local partners**: China has long imposed restrictions on foreign investment in industries the government views as crucial to maintaining power, including the Internet and telecommunications industries. In practice, such limits oblige foreign Internet companies to operate with or through a local partner in China.

   a) What criteria will Facebook use to vet potential local partners for human rights risk?
   b) How will Facebook ensure local partners, subsidiaries, and other entities linked to the firm's operations respect the rights of users and implement the company's human rights policies?
   c) What access to user data will such local partners and business entities have?

Liu Xiaobo, the 2010 Nobel Peace Prize winner and the world's only imprisoned laureate, once described the Internet as "God's gift to China," an essential tool for people in China to "strive for freedom." We urge that as Facebook considers its future in China, it places human rights at the core of its discussions and clarify to its users worldwide how it will resist becoming an agent of repression.

Sincerely,

Kenneth Roth
Executive Director

---

[i] Facebook mission statement, available at Facebook Investor Relations FAQ, http://investor.fb.com/faq.cfm (accessed May 26, 2016).

[ii] Ryan Vlastelica, Instagram Reportedly Blocked in China Amid Hong Kong Protests," *Reuters*, September 28, 2014, http://www.reuters.com/article/us-china-instagram-idUSKCNoHNoVW20140928.

[iii] Shannon Tiezzi, "Chinese Military Declares the Internet an Ideological 'Battleground,'" *The Diplomat*, May 21, 2015, http://thediplomat.com/2015/05/chinese-military-declares-the-internet-an-ideological-battleground; Edward Wong, "Xi Jinping's News Alert: Chinese Media Must Serve the Party," *New York Times*, February 22, 2016, http://www.nytimes.com/2016/02/23/world/asia/china-media-policy-xi-jinping.html.

[iv] "China: Reverse Downward Rights Spiral," Human Rights Watch news release, January 27, 2016, https://www.hrw.org/news/2016/01/27/china-reverse-downward-rights-spiral-o.

[v] Eva Dou, "China to Embed Internet Police in Tech Firms," *Wall Street Journal*, August 5, 2015, http://www.wsj.com/articles/china-to-embed-internet-police-in-tech-firms-1438755985.

[vi] "China Launches 'Rumor-Busting' Website to Enforce Party Line," Radio Free Asia, May 13, 2016, http://www.rfa.org/english/news/china/china-launches-rumor-busting-website-to-enforce-party-line-05132016093057.html.

[vii] "China: Draconian Legal Interpretation Threatens Online Freedom," Human Rights Watch news release, September 13, 2013, https://www.hrw.org/news/2013/09/13/china-draconian-legal-interpretation-threatens-online-freedom.

[viii] Chun Han Wong, "China 'Punishes' Nearly 200 for Spreading Rumors," *Wall Street Journal*, August 31, 2015, http://www.wsj.com/articles/china-punishes-nearly-200-for-spreading-rumors-1440991960; "China: New Ban on 'Spreading Rumors' About Disasters," Human Rights Watch news release, November 2, 2015, https://www.hrw.org/news/2015/11/02/china-new-ban-spreading-rumors-about-disasters; Elizabeth C. Economy, "A Chill, Ill Wind Blows Across China," *Council on Foreign Relations: Asia Unbound*, September 16, 2013, http://blogs.cfr.org/asia/2013/09/16/a-chill-ill-wind-blows-across-china.

[ix] Chris Buckley, "Crackdown on Bloggers Is Mounted by China," *New York Times*, September 13, 2013, http://www.nytimes.com/2013/09/11/world/asia/china-cracks-down-on-online-opinion-makers.html; "Fresh China media crackdown hits popular accounts on Tencent's WeChat," *South China Morning Post*, March 14, 2014, http://www.scmp.com/news/china/article/1448182/crackdown-hits-popular-accounts-tencents-wechat.

[x] Sophie Richardson, "Dispatches: Showing Diplomatic Solidarity at Lawyer's Trial in China," Human Rights Watch dispatch, December 11, 2015, https://www.hrw.org/news/2015/12/11/dispatches-showing-diplomatic-solidarity-lawyers-trial-china.

[xi] Henry Peck, "Dispatches: Time to Fix Facebook's Name Policy," Human Rights Watch dispatch, October 7, 2015, https://www.hrw.org/news/2015/10/07/dispatches-time-fix-facebooks-name-policy.

[xii] Appendix to Letter from the Nameless Coalition to Facebook About its Real Names Policy, October 5, 2015, https://www.eff.org/document/appendix-october-5-2015-coalition-letter-facebook.

[xiii] Paul McKenzie, Gordon Milner, and Wei Zhang, "China's Anti-Terrorism Law Raises Data Security Concerns," Morrison Foerster Client Alert, January 20, 2016, (accessed June 14, 2016), http://www.mofo.com/~/media/Files/ClientAlert/2016/01/160120ChinaAntiTerrorism.pdf.