

Hearing Before the Congressional-Executive Commission on China

“The PRC’s Universal Periodic Review and the Real State of Human Rights in China”

Thursday, February 1, 2024

Written Testimony by Dr. Emile Dirks

Research Associate at The Citizen Lab at the University of Toronto

Representative Smith, Senator Merkley, and distinguished Members of the Commission, thank you for holding this important hearing on the state of human rights in the People’s Republic of China and for the opportunity to testify. The conclusion of the United Nations Human Rights Council’s Universal Periodic Review (UPR) Working Group’s review of China provides an excellent opportunity to reflect on the current state of human rights in China.

My testimony today draws upon the work of myself and other researchers at the Citizen Lab. The Citizen Lab is an interdisciplinary research laboratory based at the Munk School of Global Affairs & Public Policy at the University of Toronto, focused on research, development, and strategic policy and legal engagement at the intersection of information and communication technologies, human rights, and global security.¹ Citizen Lab research has explored transnational repression, spyware, censorship, algorithmic policing, and biometric surveillance.²

Today I will focus my remarks on a particular aspect of China’s human rights record: Chinese state-backed online censorship. My testimony will highlight three key points concerning online censorship. One, state-backed online censorship profoundly impacts Chinese citizens' freedom of opinion and expression, as well as the freedom of opinion and expression of those accessing the internet from within China or using China-accessible online platforms. Two, both Chinese and US companies contribute to online censorship on China-accessible platforms. And three, online censorship is linked to repression inside China and transnational repression outside China, both of Chinese citizens and Chinese, Hong Kong, Uyghur, Tibetan, and other diaspora members.

¹ “About the Citizen Lab,” The Citizen Lab, <https://citizenlab.ca/about/>

² Noura Al-Jizawi, Siena Anstis, Sophie Barnett, Sharly Chan, Niamh Leonard, Adam Senft, and Ron Deibert, “Psychological and Emotional War: Digital Transnational Repression in Canada,” The Citizen Lab, March 1 2022, <https://citizenlab.ca/2022/03/psychological-emotional-war-digital-transnational-repression-canada/>; Bill Marczak, John Scott-Railton, Bahr Abdul Razzak, and Ron Deibert, “Triple Threat: NSO Group’s Pegasus Spyware Returns in 2022 with a Trio of iOS 15 and iOS 16 Zero-Click Exploit Chains,” The Citizen Lab, April 18 2023, <https://citizenlab.ca/2023/04/nso-groups-pegasus-spyware-returns-in-2022/>; Jeffrey Knockel, Jakub Dalek, Levi Meletti, and Ksenia Ermoshina, “Not OK on VK: An Analysis of In-Platform Censorship on Russia’s VKontakte,” The Citizen Lab, July 26 2023, <https://citizenlab.ca/2023/07/an-analysis-of-in-platform-censorship-on-russias-vkontakte/>; Kate Robertson, Cynthia Khoo, and Yolanda Song, “To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada,” The Citizen Lab, September 1 2020, <https://citizenlab.ca/2020/09/to-surveil-and-predict-a-human-rights-analysis-of-algorithmic-policing-in-canada/>; Emile Dirks, “Mass Iris Scan Collection in Qinghai: 2019–2022,” The Citizen Lab, December 14 2022, <https://citizenlab.ca/2022/12/mass-iris-scan-collection-in-qinghai/>

Drawing on these three points, I will conclude with three recommendations for how the United States government can demand accountability from perpetrators and provide assistance to victims. One, the United States government should publicly request that Microsoft, Apple, and other US companies explain how they implement political and religious censorship on their platforms in China. Two, the United States government should publicly request that Microsoft explain how political and religious censorship was applied to the search suggestions of users outside China and what safeguards will ensure this will not reoccur. And three, the US government should provide training to relevant US government officials, including law enforcement and immigration authorities, to recognize digital transnational repression and properly assist victims and their families.

Part One: State-backed Online Censorship

The Chinese government severely restricts Chinese citizens' freedom of opinion and expression through online censorship, as detailed by the United Nations Committee on Economic, Social and Cultural Rights and stakeholders' submissions for China's most recent periodic review.³ Using a sophisticated filtering system known as the "Great Firewall," authorities block access to thousands of websites which provide information which challenges the preferred narratives of the Chinese government.⁴

One of the clearest measurements of state-mandated censorship comes from Great Firewall Watch, a platform created by researchers at Stony Brook University, the University of Massachusetts - Amherst, the University of California, Berkeley, and the Citizen Lab at the University of Toronto.⁵ Since its inception in March 2020, GFWatch.org has discovered more than 640,000 blocked domains.⁶ GFWatch.org can also be used to test whether a particular domain is accessible within China.⁷ Blocked domains include the website of the Congressional-Executive Commission on China, as well as the websites of groups whose members have previously testified before the Commission, including Tibet Action Institute,

³ Committee on Economic, Social and Cultural Rights, "Concluding observations on the third periodic report of China, including Hong Kong, China, and Macao, China," United Nations Social and Economic Council, March 22 2023,

<https://documents.un.org/doc/undoc/gen/g23/048/63/pdf/g2304863.pdf?token=FHXzbyZoVrkAggrFCD&fe=true>; Office of the United Nations High Commissioner for Human Rights, "Summary of stakeholders' submissions on China," United Nations Human Rights Council, November 30 2023,

<https://documents.un.org/doc/undoc/gen/g23/238/40/pdf/g2323840.pdf?token=IBtK9ZRWexoI5WMxLo&fe=true>

⁴ "China: Freedom on the Net 2023," Freedom House, 2023,

<https://freedomhouse.org/country/china/freedom-net/2023>

⁵ Nguyen Phong Hoang, "GFWatch: A Longitudinal Measurement Platform Built to Monitor China's DNS Censorship at Scale" The Citizen Lab, November 4 2021,

<https://citizenlab.ca/2021/11/gfwatch-a-longitudinal-measurement-platform-built-to-monitor-chinas-dns-censorship-at-scale/>

⁶ Great Firewall Watch, 2023, <https://gfwatch.org/>

⁷ "Censored domains," Great Firewall Watch, 2023, https://gfwatch.org/censored_domains

Human Rights Watch, Hong Kong Democracy Council, Uyghur Human Rights Project, and the Australian Strategic Policy Institute.

Blocking websites is not the only way that the Chinese government attempts to restrict freedom of opinion and expression. Online censorship is pervasive even on platforms accessible in China. Numerous Chinese government offices participate in online censorship, including the Cyberspace Administration of China and the Ministry of Public Security. To clarify what broad categories of online material are prohibited, the Chinese government has issued a number of documents, including the *Measures for the Administration of Security Protection of Computer Information Networks with International Interconnections* (1997), the *Cybersecurity Law* (2017), *Norms for the Administration of Online Short Video Platforms and Detailed Implementation Rules for Online Short Video Content Review Standards* (2019), and *Provisions on the Governance of the Online Information Content Ecosystem* (2020).⁸ Prohibited content listed in these documents includes “content harming the image of revolutionary leaders or heroes and martyrs” and information which is “damaging the reputation or interests of the state” or “detrimental to state religious policies, propagating heretical or superstitious ideas.”⁹ The Chinese government also routinely conducts “internet purification campaigns” by which state organs compel websites, platforms, and accounts to remove prohibited content and punish violators through warnings or administrative or criminal penalties.¹⁰

Yet while government authorities stipulate what broad categories of content is prohibited, it is technology companies which are responsible for day-to-day censorship. Technology companies operating in China are required to ensure that content which appears on their platforms complies with legal requirements or political directives from the Chinese state. Companies which fail to moderate content on their platforms can be fined or have their business licenses revoked.¹¹ This

⁸ “Computer Information Network and Internet Security, Protection and Management Regulations - 1997,” Lehman, Lee & Xu, <https://www.lehmanlaw.com/resource-centre/laws-and-regulations/information-technology/computer-information-network-and-internet-security-protection-and-management-regulations-1997.html>; “Translation: Cybersecurity Law of the People’s Republic of China (Effective June 1, 2017),” DigiChina, <https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/>; “Norms for the Administration of Online Short Video Platforms and Detailed Implementation Rules for Online Short Video Content Review Standards,” China Law Translate, <https://www.chinalawtranslate.com/en/norms-for-the-administration-of-online-short-video-platforms-and-detailed-implementation-rules-for-online-short-video-content-review-standards/>; “Provisions on the Governance of the Online Information Content Ecosystem,” World Intermediary Liability Map, <https://wilmap.stanford.edu/entries/provisions-governance-online-information-content-ecosystem>

⁹ Jeffrey Knockel, Ken Kato, and Emile Dirks, “Missing Links: A comparison of search censorship in China,” The Citizen Lab, <https://citizenlab.ca/2023/04/a-comparison-of-search-censorship-in-china/>

¹⁰ Jeffrey Knockel, Ken Kato, and Emile Dirks, “Missing Links: A comparison of search censorship in China,” The Citizen Lab, <https://citizenlab.ca/2023/04/a-comparison-of-search-censorship-in-china/>

¹¹ Rebecca MacKinnon (2009), “China’s Censorship 2.0: How companies censor bloggers,” *First Monday*, 14(2), <https://firstmonday.org/ojs/index.php/fm/article/view/2378>

form of intermediary liability or corporate “self-discipline” is a characteristic feature of information control and online censorship in China.¹²

Citizen Lab researchers have discovered over 60,000 censorship rules on eight China-accessible search platforms: Baidu, Baidu Zhidao, Bilibili, Microsoft Bing, Douyin, Jingdong, Sogou, and Weibo.¹³ Examples of censored content covered by these rules include various creative homographs for the name “Xi Jinping,” references to the June 4 massacre, material related to religious communities, and criticisms of the Communist Party. Citizen Lab research also demonstrates that platforms institute different levels of censorship which fully or partially censor search results for key terms. Partial or “soft” censorship provides results from authorized sources like Chinese government websites or state media, while full or “hard” censorship provides no results.

Citizen Lab researchers have also detailed how China-accessible platforms including WeChat censor discussion of political events. These events include activism in Hong Kong, crackdowns on human rights lawyers, the COVID-19 pandemic, and the deaths of Nobel Peace Prize winner Liu Xiaobo and former premier Li Keqiang.¹⁴ Results from these research investigations demonstrate how China-accessible platforms suppress politically sensitive information and promote narratives favourable to the Chinese state.

Part Two: The Role of US-based Companies in Online Censorship

While Chinese tech companies are the key players in online censorship in China, US companies are also involved. For instance, in 2018 leaked documents revealed that Google was planning to release an app in China that would implement political censorship, a plan they abandoned in

¹² Rebecca MacKinnon, “Commentary: Are China's demands for Internet 'self-discipline' spreading to the West?,” McClatchy DC, January 18 2010, <https://www.mcclatchydc.com/opinion/article24570625.html>

¹³ Jeffrey Knockel, Ken Kato, and Emile Dirks, “Missing Links: A comparison of search censorship in China,” The Citizen Lab, <https://citizenlab.ca/2023/04/a-comparison-of-search-censorship-in-china/>

¹⁴ “Censored Commemoration: Chinese Live Streaming Platform YY Focuses Censorship on June 4 Memorials and Activism in Hong Kong,” The Citizen Lab, June 4 2019, <https://citizenlab.ca/2019/06/censored-commemoration-chinese-live-streaming-platform-yy-focuses-censorship-june-4-memorials-activism-hong-kong/>; Lotus Ruan, Jeffrey Knockel, and Masashi Crete-Nishihata, “We (can’t) Chat: “709 Crackdown” Discussions Blocked on Weibo and WeChat,” The Citizen Lab, April 13 2017, <https://citizenlab.ca/2017/04/we-cant-chat-709-crackdown-discussions-blocked-on-weibo-and-wechat/>; Lotus Ruan, Jeffrey Knockel, and Masashi Crete-Nishihata, “Censored Contagion: How Information on the Coronavirus is Managed on Chinese Social Media,” The Citizen Lab, March 3 2020, <https://citizenlab.ca/2020/03/censored-contagion-how-information-on-the-coronavirus-is-managed-on-chinese-social-media/>; Masashi Crete-Nishihata, Jeffrey Knockel, Blake Miller, Jason Q. Ng, Lotus Ruan, Lokman Tsui, and Ruohan Xiong, “Remembering Liu Xiaobo: Analyzing censorship of the death of Liu Xiaobo on WeChat and Weibo,” The Citizen Lab, June 16 2017, <https://citizenlab.ca/2017/07/analyzing-censorship-of-the-death-of-liu-xiaobo-on-wechat-and-weibo/>; Jeffrey Knockel and Emile Dirks, “Chinese censorship following the death of Li Keqiang,” The Citizen Lab, November 21 2023, <https://citizenlab.ca/2023/11/chinese-censorship-following-the-death-of-li-keqiang/>

2019 after criticism from within and outside the company.¹⁵ On their China-accessible platforms, US companies have imposed restrictions on political and religious content. And like the restrictions imposed by Chinese counterparts, those imposed by US companies have impacted users both inside China and in other world regions, including the United States.

Citizen Lab research shows that the Chinese version of Microsoft's Bing, the only major non-Chinese search engine accessible in China, engages in extensive censorship.¹⁶ In China, Bing only displays results for censored search queries from authorized websites, such as government and state media websites. Like Chinese search platforms, Bing's censorship rules target political material related to Xi Jinping, religious material, references to Nobel Peace Prize winner Liu Xiaobo, and terms related to the June 4 massacre. Compared with Baidu, Bing's political censorship rules are also broader, affect more search results, and lead to search results for a greater number of websites being restricted.

The impact of censorship on Bing is not limited to users within China. Citizen Lab researchers found that Bing's censorship of search suggestions, though not search results, was applied to users in the United States and other countries for at least eight months from October 2021 to May 2022.¹⁷ Bing's censorship of politically sensitive search suggestions in both English and Chinese applied to multiple regions outside China, including the United States and Canada. Suggestions including the names of politically sensitive figures were censored, including those of Xi Jinping, the doctor Li Wenliang who had warned his colleagues about early Covid-19 infections in Wuhan, religious figures including the 11th Panchen Lama Gedhun Choekyi Nyima, and references to the "Tank Man" photographed standing in front of a column of tanks leaving Tiananmen Square on June 5 1989. In response to a May 10 2022 letter addressed Microsoft's Chief Digital Security Officer, Microsoft communicated to the Citizen Lab that it had discovered and resolved a misconfiguration on Bing which had prevented valid autosuggestions from appearing for users outside China.¹⁸ However, while Microsoft ceased

¹⁵ Ryan Gallagher, "Google Plans To Launch Censored Search Engine In China, Leaked Documents Reveal," The Intercept, August 1 2018, <https://theintercept.com/2018/08/01/google-china-search-engine-censorship/>; Sarah McKune and Ronald Deibert, "Google's Dragonfly: A Bellwether for Human Rights in the Digital Age," Just Security, August 2 2018,

<https://www.justsecurity.org/59941/googles-dragonfly-bellwether-human-rights-digital-age/>; "Google's Project Dragonfly 'terminated' in China," BBC News, July 17 2019, <https://www.bbc.com/news/technology-49015516>

¹⁶ Jeffrey Knockel and Emile Dirks, "Chinese censorship following the death of Li Keqiang," The Citizen Lab, November 21 2023, <https://citizenlab.ca/2023/11/chinese-censorship-following-the-death-of-li-keqiang/>

¹⁷ Jeffrey Knockel and Lotus Ruan, "Bada Bing, Bada Boom: Microsoft Bing's Chinese Political Censorship of Autosuggestions in North America," The Citizen Lab, May 19 2022, <https://citizenlab.ca/2022/05/bada-bing-bada-boom-microsoft-bings-chinese-political-censorship-autosuggestions-no-rth-america/>

¹⁸ "Citizen Lab Letter to Microsoft," The Citizen Lab, May 10 2022, <https://citizenlab.ca/wp-content/uploads/2022/05/Citizen-Letter-to-Microsoft.pdf>; Jeffrey Knockel and Lotus Ruan, "Bada Bing, Bada Boom: Microsoft Bing's Chinese Political Censorship of Autosuggestions in North America," The Citizen Lab, May 19 2022, <https://citizenlab.ca/2022/05/bada-bing-bada-boom-microsoft-bings-chinese-political-censorship-autosuggestions-no-rth-america/>

Chinese political censorship of autosuggestions in countries outside of China including the United States, there is no indication that Microsoft has ceased censoring autosuggestions for users of Bing in China.

Microsoft is not the only US company which performs Chinese political censorship. In 2021, Citizen Lab researchers found that Apple applied censorship to product engravings in China.¹⁹ Censored political content included the names of Chinese leaders, Chinese dissidents, and independent news organizations, as well as general terms related to religion, democracy, and human rights. Apple applied these censorship rules not only in China, but in Hong Kong and Taiwan as well. Research findings also indicated that Apple did not fully understand what content they censored. Instead, many censored keywords appeared to have been reappropriated from other sources, including censorship lists compiled by Chinese companies. Since the release of this report, Apple eliminated Chinese political censorship in Taiwan, but has continued keyword-based political censorship in both mainland China and Hong Kong.²⁰

Bing and Apple's extensive censorship inside China shows that US tech companies cannot introduce services in China without integrating restrictions on expression. Furthermore, our findings show that it is inevitable that such censorship will be applied, either accidentally or otherwise, to users outside of China, including Taiwan and the United States.

Part Three: The Offline Harms of Online Censorship

State-backed restrictions on political and religious expression do not exist in a vacuum. Online censorship is linked to offline harms. Chinese citizens who attempt to access or share sensitive information online do so at risk to their personal freedom. Authorities have jailed Chinese citizens for a range of offenses, including selling software that allows people to circumvent the Great Firewall, making comments in private chat groups, sharing videos of protests, and even

¹⁹ Jeffrey Knockel and Lotus Ruan, "Engrave Danger: An Analysis of Apple Engraving Censorship across Six Regions," The Citizen Lab, August 18 2021,

<https://citizenlab.ca/2021/08/engrave-danger-an-analysis-of-apple-engraving-censorship-across-six-regions/>

²⁰ Jeffrey Knockel and Lotus Ruan, "Engrave Condition: Apple's Political Censorship Leaves Taiwan, Remains in Hong Kong," The Citizen Lab, March 22 2022,

<https://citizenlab.ca/2022/03/engrave-condition-apples-political-censorship-leaves-taiwan-remains-in-hong-kong/>

posting on social media platforms like X (Twitter) which are blocked in China.²¹ Such cases highlight the severe rights impacts that censorship has on the people of China.

While some Chinese citizens risk detention and even torture for their online activities, state-affiliated actors use these same platforms to launch attacks against opponents of the party-state. As detailed by Citizen Lab researchers, a 2019-2021 harassment campaign nicknamed “HKLEAKS” used websites and social media to distribute personal information about Hong Kong pro-democracy activists.²² Actors involved in the campaign used proprietary websites and social media accounts to publish personal identifiable information about targeted activists. Those connected to the campaign claimed they were members of Hong Kong volunteer committees. However, Citizen Lab researchers uncovered indications that this was a coordinated information operation conducted by professional actors aligned with the Chinese state.

Victims of other online harassment campaigns live outside China. This Commission has previously discussed how the Chinese government silences overseas critics through transnational repression.²³ For years, the Chinese government has used transnational repression to intimidate, threaten, and surveil diaspora members it views as threats.²⁴ Many of these victims are Tibetan.²⁵

²¹ Benjamin Haas, “Man in China sentenced to five years' jail for running VPN,” The Guardian, December 22 2017, <https://www.theguardian.com/world/2017/dec/22/man-in-china-sentenced-to-five-years-jail-for-running-vpn>; Eva Dou, “Jailed for a Text: China’s Censors Are Spying on Mobile Chat Groups,” The Wall Street Journal, December 8 2017, <https://www.wsj.com/articles/jailed-for-a-text-chinas-censors-are-spying-on-mobile-chat-groups-1512665007>; Amy Hawkins, “Uyghur student convicted after posting protests video on WeChat,” The Guardian, June 8 2023, <https://www.theguardian.com/world/2023/jun/08/uyghur-student-convicted-posting-protests-video-wechat-kamile-w-ayit>; Chun Han Wong, “China Is Now Sending Twitter Users to Prison for Posts Most Chinese Can’t See,” The Wall Street Journal, January 29 2021, <https://www.wsj.com/articles/china-is-now-sending-twitter-users-to-prison-for-posts-most-chinese-cant-see-11611932917>

²² Alberto Fittarelli and Lokman Tsui, “Beautiful Bauhinia: “HKLeaks” – The Use of Covert and Overt Online Harassment Tactics to Repress 2019 Hong Kong Protests,” The Citizen Lab, July 13 2023, <https://citizenlab.ca/2023/07/hkleaks-covert-and-overt-online-harassment-tactics-to-repress-the-2019-hong-kong-protests/>

²³ “Countering China’s Global Transnational Repression Campaign,” CECC, September 12 2023, <https://www.cecc.gov/events/hearings/countering-chinas-global-transnational-repression-campaign>; “Preserving Tibet: Combatting Cultural Erasure, Forced Assimilation and Transnational Repression,” CECC, March 28 2023, <https://www.cecc.gov/events/hearings/preserving-tibet-combating-cultural-erasure-forced-assimilation-and-transnational>; “The Threat of Transnational Repression From China and The U.S. Response,” CECC, June 15 2022, <https://www.cecc.gov/events/hearings/the-threat-of-transnational-repression-from-china-and-the-us-response>

²⁴ Eric Hsu and Ai-Men Lau, “Silenced Voices, Hidden Struggles: PRC Transnational Repression on Overseas Human Right Activists,” Doublethink Lab, June 1 2023, <https://doublethinklab.medium.com/silenced-voices-hidden-struggles-prc-transnational-repression-on-overseas-human-right-activists-8f34aece7ae6>; “China: Transnational Repression Origin Country Case Study,” Freedom House, 2021, <https://freedomhouse.org/report/transnational-repression/china>; ““They Don’t Understand the Fear We Have” How China’s Long Reach of Repression Undermines Academic Freedom at Australia’s Universities,” Human Rights Watch, June 30 2021, <https://www.hrw.org/report/2021/06/30/they-dont-understand-fear-we-have/how-chinas-long-reach-repression-undermines>

²⁵ “Chinese Transnational Repression of Tibetan Diaspora Communities 2024,” Tibetan Centre for Human Rights & Democracy, 2024,

Since 2009, Citizen Lab researchers have investigated digital attacks and espionage against Tibetan diaspora communities. These attacks include cyber espionage programs targeting Tibetan institutions, one-click mobile exploits and malware used to install spyware in a target's phone, and phishing operations conducted against diaspora Tibetan organizations.²⁶

State-backed proxies and online nationalists also harass Chinese, Hong Kong, Tibetan, Uyghur, and other diaspora members on Chinese and US social media platforms. Some of the most vicious instances of digital transnational repression are directed at women.²⁷ As Citizen Lab researchers have documented, Chinese and Hong Kong women activists in Canada have suffered online threats of physical and sexual violence.²⁸ Digital transnational repression has profound consequences for victims and their relatives. Many suffer intense psychological harm, while others self-censor or limit their online activities. Still others have had to contend with state harassment of family members in China, a form of transnational repression known as “coercion-by-proxy.”²⁹

Recommendations

Through state-backed online censorship, the cooperation of Chinese and US technology companies, and domestic and transnational repression, the Chinese state severely restricts the freedom of opinion and expression of people in and outside China. Addressing restrictions on

<https://tchrd.org/wp-content/uploads/2024/02/Chinese-Transnational-Repression-of-Tibetan-Diaspora-Communities.pdf>

²⁶ Jane, “Tracking GhostNet: Investigating a Cyber Espionage Network,” The Citizen Lab, March 28 2009, <https://citizenlab.ca/2009/03/tracking-ghostnet-investigating-a-cyber-espionage-network/>; Adam Hulcoop, Matt Brooks, Etienne Maynier, John Scott-Railton, and Masashi Crete-Nishihata, “It’s Parliamentary KeyBoy and the targeting of the Tibetan Community,” The Citizen Lab, November 17 2016, <https://citizenlab.ca/2016/11/parliament-keyboy/>; Jakub Dalek, Masashi Crete-Nishihata, and John Scott-Railton, “Shifting Tactics: Tracking changes in years-long espionage campaign against Tibetans,” The Citizen Lab, March 10 2016, <https://citizenlab.ca/2016/03/shifting-tactics/>; Katie Kleemola, Masashi Crete-Nishihata, and John Scott-Railton, “Tibetan Uprising Day Malware Attacks,” The Citizen Lab, March 10 2015, <https://citizenlab.ca/2015/03/tibetan-uprising-day-malware-attacks/>; Geoffrey Alexander, Matt Brooks, Masashi Crete-Nishihata, Etienne Maynier, John Scott-Railton, and Ron Deibert, “Spying on a Budget: Inside a Phishing Operation with Targets in the Tibetan Community,” The Citizen Lab, January 30 2018, <https://citizenlab.ca/2018/01/spying-on-a-budget-inside-a-phishing-operation-with-targets-in-the-tibetan-community/>; Bill Marczak, Adam Hulcoop, Etienne Maynier, Bahr Abdul Razzak, Masashi Crete-Nishihata, John Scott-Railton, and Ron Deibert, “Missing Link: Tibetan Groups Targeted with 1-Click Mobile Exploits,” The Citizen Lab, September 24 2019, <https://citizenlab.ca/2019/09/poison-carp-tibetan-groups-targeted-with-1-click-mobile-exploits/>

²⁷ Albert Zhang and Danielle Cave, “Smart Asian women are the new targets of CCP global online repression,” The Strategist, June 3 2022, <https://www.aspistrategist.org.au/smart-asian-women-are-the-new-targets-of-ccp-global-online-repression/>

²⁸ Noura Al-Jizawi, Siena Anstis, Sophie Barnett, Sharly Chan, Niamh Leonard, Adam Senft, and Ron Deibert, “Psychological and Emotional War: Digital Transnational Repression in Canada,” The Citizen Lab, March 1 2022, <https://citizenlab.ca/2022/03/psychological-emotional-war-digital-transnational-repression-canada/>

²⁹ Fiona B. Adamson and Gerasimos Tsourapas, “At Home and Abroad: Coercion-by-Proxy as a Tool of Transnational Repression,” Freedom House, 2020, <https://freedomhouse.org/report/special-report/2020/home-and-abroad-coercion-proxy-tool-transnational-repression>

these freedoms requires holding Chinese and US companies responsible for their role in online censorship and supporting victims of digital harassment and intimidation. Therefore, I recommend that the United States government do three things:

One, publicly request that Microsoft, Apple, and other US companies explain how and why they implement political and religious censorship on their platforms in China. Citizen Lab researchers have discovered censorship rules that US companies have implemented on China-accessible platforms and measured the breadth and impact of these rules. However, it is not clear how US companies develop and implement these censorship rules, nor why US companies are willing to censor political and religious content on their China-accessible platforms. Requesting Microsoft, Apple, and other US companies to provide this information would contribute to more informed and effective policies pertaining to addressing the rights and privacy impacts of online platforms and digital technologies.

Two, publicly request that Microsoft explain how political and religious censorship was applied to the search suggestions of users of Bing outside China and what safeguards will ensure this will not reoccur. Citizen Lab researchers discovered that for a period of at least eight months from October 2021 to May 2022 Microsoft's Bing search engine censored politically sensitive Chinese search suggestions in different world regions, including the United States. It is unclear why Microsoft censored these suggestions and what steps Microsoft has taken to prevent this kind of censorship from reoccurring. Requesting Microsoft answer these questions would deepen understanding of how individuals outside China, including in the United States, are impacted by Chinese state-backed censorship on China-accessible platforms.

And three, train US government officials, including law enforcement and immigration authorities, to recognize digital transnational repression and properly assist victims and their families. Many victims of transnational repression, including digital transnational repression, live in the United States. The United States government has a duty to protect both US and non-US citizens who are victims of transnational repression. Providing protection requires recognizing the severity of the problem. Personnel working in relevant government offices, including US Citizenship and Immigration Services and federal, state, and local law enforcement, should receive training to help them identify both victims and perpetrators of transnational repression. Training should also include learning how to conduct outreach to victims and their families and how to provide appropriate assistance to those at risk of transnational repression. By helping victims of transnational repression in the United States, the US government will demonstrate support for those exercising their freedom of expression and opinion on and offline.

Thank you for the opportunity to testify today. I look forward to your questions and comments.