OFFICE OF COMMISSIONER BRENDAN CARR

Carr Applauds Bipartisan Legislation on TikTok

The bill bans TikTok unless it severs ties to the CCP

WASHINGTON, DC, March 5, 2024—Today, the bipartisan leaders of the House Select Committee on the Chinese Communist Party introduced the "Protecting Americans from Foreign Adversary Controlled Applications Act." The bill, authored by Chairman Mike Gallagher (R-WI) and Ranking Member Raja Krishnamoorthi (D-IL) and supported by a broad coalition of Republicans and Democrats, would definitively resolve the serious threat TikTok poses to America's national security. House Energy and Commerce Committee Chair Rodgers (R-WA) announced that the Committee will vote on the bill this Thursday, March 7.

The bill would fully address the risks posed by TikTok by banning the application unless TikTok genuinely divests from its ties to the Communist Party of China.

Commissioner Carr issued the following statement:

"TikTok's own conduct makes clear that it is beholden to the CCP and presents an unacceptable threat to U.S. national security. Indeed, TikTok has been caught engaging in a pattern of illicit surveillance and making false statements about personnel in Beijing accessing sensitive U.S. user data. These facts were laid bare for the world to see when the House Energy and Commerce Committee held a TikTok oversight hearing last year. And that is why there is now a broad, bipartisan consensus that TikTok cannot continue to operate in the U.S. in its current form.

"I want to applaud the strong, bipartisan leadership that Members of Congress have shown in advancing this bill, which would definitively resolve the serious national security threats TikTok poses by banning the app or requiring that it genuinely sever ties to the CCP. This is a smart, threat-specific bill that would address a clear and present danger. I hope that this bill will soon become law."

Commissioner Carr provided additional material in support of the bill in the attached below:

###

Office of Commissioner Brendan Carr
www.fcc.gov/about/leadership/brendan-carr

Media Contact: Greg Watson
greg.watson@fcc.gov

H.R. 7521: "Protecting Americans from Foreign Adversary Controlled Applications Act"

The bill protects First Amendment rights because it regulates conduct, not content.

Supreme Court precedent makes clear that Congress can ban TikTok or require it to cut ties with the CCP without violating the First Amendment. Specifically, the Court draws a distinction between laws based on the *content* of speech on the one hand and those based on *conduct* on the other. Laws that fall into the first category almost always violate the First Amendment. But those that fall into the second category by regulating non-expressive conduct do not. Here, this bill is not based on the content of TikTok's protected speech or on any of the lawful content that TikTok users want to share or receive. Instead, the bill takes action based on TikTok's illicit conduct—namely, the concrete threat to national security that TikTok poses as evidenced by its own actions—conduct that is not protected by the First Amendment.

The Supreme Court's decision in *Arcara v. Cloud Books* offers an analogous case in point. There, the government shut down a bookstore because the owner used the facility to engage in illegal conduct. The owner argued that, notwithstanding the illegal conduct, the government could not close the store because the First Amendment protected the selling and purchasing of books. While the Court recognized that closing the store would have an incidental burden on protected speech, because people could no longer use that store to browse books, it upheld the closure because the government acted based on the owner's unlawful conduct, not based on the content of any speech. So too here. The First Amendment does not protect espionage, and the Constitution does not require the government to allow TikTok's national security threat to persist simply because TikTok also enables Americans to use the platform for protected speech. Supreme Court law makes this clear. And this case is an even easier one because the bill allows Americans to continue using TikTok provided that it genuinely cut ties with the CCP.

The bill does not run afoul of the Constitution's Bill of Attainder Clause.

The case law here is clear. The Bill of Attainder Clause does not prevent Congress from passing a law that singles out a particular business.[1] Rather, courts look at whether the legislation unlawfully inflicts punishment for past conduct without judicial protections or instead lawfully regulates conduct or activities on a prophylactic or prospective basis. This bill does the latter. It does not punish TikTok for past conduct. Instead, it takes an appropriate step to protect America's national security interests on a going-forward basis. Indeed, courts have already rejected Bill of Attainder arguments when brought by Huawei and Kaspersky Lab after Congress identified them by name in 2018 and 2019 laws that imposed national security restrictions.[2] And in any event, this bill does not apply solely to TikTok—it covers other apps that are controlled by a foreign adversary.

The bill does not grant the government any new authorities that could be weaponized against individual Americans.

This bill is a smart, targeted, and rifle shot approach that addresses the serious risks posed by TikTok's ties to the CCP. As the text expressly states, "nothing in this Act may be construed to

---

[1] *See, e.g.*, *Nixon v. Administrator of General Services*, 433 U.S. 425 (1977); *see also* Congressional Research Service, Huawei v. the United States: The Bill of Attainder Clause and Huawei's Lawsuit Against the United States at 3-4 (2019), https://crsreports.congress.gov/product/pdf/LSB/LSB10274.

[2] *See Huawei Technologies USA v. United States*, 440 F.Supp.3d 607, 629-650 (E.D. Tex. 2020); *Kaspersky Lab v. United States Department of Homeland Security*, 909 F.3d 446, 454-465 (D.C. Cir. 2018).

authorize the Attorney General to pursue enforcement…against an individual user of a foreign adversary controlled application." The bill goes on to state that "nothing in this Act may, except as expressly provided herein, to alter or affect any other authority provided by or established under another provision of Federal law."

Congress is right to move on TikTok now rather than deferring action.

The argument that Congress should defer action on TikTok while the U.S. considers broader debates about threats from online actors and consumer privacy presents a false choice. For one, TikTok presents a clear and present danger today that warrants action now. For another, the U.S. already has processes in place to identify entities that pose an unacceptable threat to U.S. national security, including through their ties to the CCP and other foreign adversaries. Indeed, the U.S. has already identified and taken action against Huawei, ZTE, Hytera, Hikvision, Dahua, Kaspersky Lab, China Mobile, China Telecom, Pacific Networks, and China Unicom. TikTok's threat has been identified through a national security process and is simply the next one that is ripe for action. For still another, privacy laws and national security laws are not the same thing. Just look at Europe. The E.U. has enacted some of the strictest data privacy laws, and yet it has also taken separate actions to ban TikTok from official devices.[3] Those bans would have been unnecessary if privacy laws alone were adequate to address security risks.

TikTok's "Project Texas" does not resolve the national security concerns.

TikTok has offered to address U.S. national security concerns through an initiative known as "Project Texas," but this scheme fails to protect America's interests. For one, Project Texas would continue to allow personnel in Beijing to access U.S. user data. Indeed, even after promising to wall off U.S. user data, data continues to be accessible from inside China.[4] For another, TikTok personnel themselves have thrown cold water on the idea that U.S. user data will be adequately protected under any new arrangement, with one employee stating that "[i]t remains to be seen if at some point product and engineering can still figure out how to get access, because in the end of the day, it's their tools[.] They built them all in China."[5]

---

[3] *See* Xiaofei Xu, *EU bans TikTok from Official Devices Across All Three Government Institutions* (Mar. 1, 2023), https://www.cnn.com/2023/02/28/tech/tiktok-eu-ban-intl-hnk/index.html.

[4] *See* Georgia Wells, *TikTok Struggles to Protect U.S. Data From Its China Parent* (Jan. 30, 2024), https://www.wsj.com/tech/tiktok-pledged-to-protect-u-s-data-1-5-billion-later-its-still-struggling-cbccf203?mod=e2tw.

[5] *See* Emily Baker-White, *Leaked Audio From 80 Internal TikTok Meetings Shows That US User Data Has Been Repeatedly Accessed From China* (June 17, 2022), https://www.buzzfeednews.com/article/emilybakerwhite/tiktok-tapes-us-user-data-china-bytedance-access.