118TH CONGRESS
2D SESSION

H. RES. 1051

Recognizing the importance of the national security risks posed by foreign adversary controlled social media applications.

IN THE HOUSE OF REPRESENTATIVES

MARCH 5, 2024

Mr. GALLAGHER (for himself and Mr. KRISHNAMOORTHI) submitted the following resolution; which was referred to the Committee on Energy and Commerce

---

RESOLUTION

Recognizing the importance of the national security risks posed by foreign adversary controlled social media applications.

Whereas TikTok collects vast amounts of data on Americans, though the total extent of its collection is unknown:

(1) On August 6, 2020, the President concluded that TikTok ''automatically captures vast swaths of information from its users'' and that TikTok's ownership by ByteDance Ltd. enables the People's Republic of China (referred to in this resolution as the ''PRC'') and Communist Party of China (referred to in this resolution as the ''CCP'') to gain access to ''Americans' personal and proprietary information,'' potentially allowing the CCP ''to track the locations of Federal employees and

contractors, build dossiers of personal information for blackmail, and conduct corporate espionage''.

(2) Outside reporting has confirmed the breadth of TikTok's reach, concluding that its data collection practices extend to age, phone number, precise location, internet address, device used, phone contacts, social network connections, content of private messages sent through the application, and videos watched.

(3) On November 11, 2022, Federal Communications Commissioner Brendan Carr explained that ''underneath [TikTok], it operates as a very sophisticated surveillance app.''. He characterized it as ''a big risk'' for multiple reasons, including espionage. The risk posed by TikTok is exacerbated by the difficulty in assessing precisely which categories of data it collects. For example, outside researchers have found embedded vulnerabilities that allow the company to collect more data than the application's privacy policy indicates.

Whereas PRC law requires obligatory, secret disclosure of data controlled by Chinese companies at the PRC's unilateral request:

(1) Pursuant to PRC law, the PRC can require a company headquartered in the PRC to surrender all its data to the PRC, making it an espionage tool of the CCP.

(2) The National Intelligence Law, passed in China in 2017, states that ''any organization'' must assist or cooperate with CCP intelligence work. Such assistance or cooperation must also remain secret at the PRC's request.

(3) The PRC's 2014 Counter-Espionage Law states that ''relevant organizations . . . may not refuse'' to collect evidence for an investigation.

(4) The PRC's Data Security Law of 2021 states that the PRC has the power to access and control private data.

(5) The PRC's Counter-Espionage Law grants PRC security agencies nearly unfettered discretion, if acting under an effectively limitlessly capacious understanding of national security, to access data from companies.

(6) On September 17, 2020, the Department of Commerce concluded that the PRC, to advance ''its intelligence-gathering and to understand more about who to target for espionage, whether electronically or via human recruitment,'' is constructing ''massive databases of Americans' personal information'' and that ByteDance has close ties to the CCP, including a cooperation agreement with a security agency and over 130 CCP members in management positions.

(7) On December 2, 2022, the Director of the Federal Bureau of Investigation, Christopher Wray, stated that TikTok's data repositories on Americans ''are in the hands of a government that doesn't share our values and that has a mission that's very much at odds with what's in the best interests of the United States. . . . The [CCP] has shown a willingness to steal Americans data on a scale that dwarfs any other''.

(8) On December 5, 2022, the Director of National Intelligence, Avril Haines, stated, when asked about TikTok and PRC ownership, ''It is extraordinary the degree to which [the PRC] . . . [is] developing frameworks for collecting foreign data and pulling it in, and their capacity to then turn that around and use it to target audiences for information campaigns and other things, but also to have it for the future so that they can use it for a variety of means''.

(9) On December 16, 2022, the Director of the Central Intelligence Agency, William Burns, explained that ''because the parent company of TikTok is a [PRC] company, the [CCP] is able to insist upon extracting the private data of a lot of TikTok users in this country, and also to shape the content of what goes on to TikTok as well to suit the interests of the Chinese leadership''.

(10) On August 2, 2020, then-Secretary of State, Mike Pompeo, stated that PRC-based companies ''are feeding data directly to the Chinese Communist Party, their national security apparatus''.

(11) Public reporting has repeatedly confirmed statements made by the executive branch regarding the tight interlinkages between ByteDance, TikTok, and the CCP.

(A) The Secretary of ByteDance's CCP committee, Zhang Fuping, also serves as ByteDance's Editor-in-Chief and Vice President and has vowed that the CCP committee would ''take the lead'' across ''all product lines and business lines'', which include TikTok.

(B) On May 30, 2023, public reporting revealed that TikTok has stored sensitive financial information, including the Social Security numbers and tax identifications of TikTok influencers and United States small businesses, on servers in China accessible by ByteDance employees.

(C) On December 22, 2022, public reporting revealed that ByteDance employees accessed TikTok user data and IP addresses to monitor the physical locations of specific United States citizens.

(D) On June 17, 2022, public reporting revealed that, according to leaked audio from more

than 80 internal TikTok meetings, China-based employees of ByteDance repeatedly accessed nonpublic data about United States TikTok users, including the physical locations of specific United States citizens.

(E) On January 20, 2023, public reporting revealed that TikTok and ByteDance employees regularly engage in practice called ''heating,'' which is a manual push to ensure specific videos ''achieve a certain number of video views''.

(F) In a court filing in June 2023, a former employee of ByteDance alleged that the CCP spied on pro-democracy protestors in Hong Kong in 2018 by using backdoor access to TikTok to identify and monitor activists' locations and communications.

(G) On November 1, 2023, public reporting revealed that TikTok's internal platform, which houses its most sensitive information, was inspected in person by CCP cybersecurity agents in the lead-up to the CCP's 20th National Congress.

Whereas the PRC's access to American users' data poses unacceptable risks to United States national security:

(1) As a general matter, foreign adversary controlled social media applications present a clear threat to the national security of the United States.

(2) The Department of Homeland Security has warned that the PRC's data collection activities in particular have resulted in ''numerous risks to U.S. businesses and customers, including: the theft of trade secrets, of intellectual property, and of other confidential business information; violations of U.S. export control laws; violations of U.S. privacy laws; breaches of contractual provisions and terms of service; security and privacy

risks to customers and employees; risk of PRC surveillance and tracking of regime critics; and reputational harm to U.S. businesses''. These risks are imminent and other, unforeseen risks may also exist.

(3) On September 28, 2023, the Department of State's Global Engagement Center issued a report that found that ''TikTok creates opportunities for PRC global censorship''. The report stated that United States Government information as of late 2020 showed that ''ByteDance maintained a regularly updated internal list identifying people who were likely blocked or restricted from all ByteDance platforms, including TikTok, for reasons such as advocating for Uyghur independence''.

(4) On November 15, 2022, the Director of the Federal Bureau of Investigation, Christopher Wray, testified before the Committee on Homeland Security of the House of Representatives that TikTok's national security concerns ''include the possibility that the [CCP] could use it to control data collection on millions of users or control the recommendation algorithm, which could be used for influence operations if they so choose, or to control software on millions of devices, which gives it an opportunity to potentially technically compromise personal devices''.

(5) On March 8, 2023, the Director of the Federal Bureau of Investigation, Christopher Wray, testified before the Select Committee on Intelligence of the Senate that the CCP, through its ownership of ByteDance, could use TikTok to collect and control users' data and drive divisive narratives internationally.

Whereas Congress has extensively investigated whether TikTok poses a national security threat because it is owned by ByteDance:

(1) On October 26, 2021, during the testimony of Michael Beckerman, TikTok head of public policy for the Americas, before a hearing of the Subcommittee on Consumer Protection of the Committee on Commerce, Science, and Transportation of the Senate, lawmakers expressed concerns that TikTok's audio and user location data could be used by the CCP.

(2) On September 14, 2022, lawmakers expressed concerns over TikTok's algorithm and content recommendations posing a national security threat during a hearing before the Committee on Homeland Security and Governmental Affairs of the Senate with Vanessa Pappas, Chief Operating Officer of TikTok.

(3) On March 23, 2023, during the testimony of TikTok CEO, Shou Chew, before the Committee on Energy and Commerce of the House of Representatives, lawmakers expressed concerns about the safety and security of the application, including TikTok's relationship with the CCP.

(4) On February 28, 2023, former Deputy National Security Advisor, Matthew Pottinger, emphasized that it has already been confirmed that TikTok's parent company ByteDance has used the application to surveil United States journalists as a means to identify and retaliate against potential sources. The PRC has also shown a willingness to harass individuals abroad who take stances that contradict the Communist Party lines. The application can further be employed to help manipulate social discourse and amplify false information to tens of millions of Americans.

(5) On March 23, 2023, Nury Turkel, the Chair of the United States Commission on International Religious Freedom, raised the alarm that TikTok's parent com-

pany, ByteDance, has a strategic partnership with China's Ministry of Public Security, and China's domestic version of the application, Douyin, has been used to collect data and sensitive information from Uyghurs and other oppressed ethnic minority groups.

(6) On July 26, 2023, William Evanina, the former Director of the National Counterintelligence and Security Center, pointed to TikTok as just one of many areas of concern that combine to paint a concerning picture of the CCP's capabilities and intent as an adversarial, malign competitor.

(7) On November 30, 2023, John Garnaut of the Australian Strategic Policy Institute (ASPI) remarked that TikTok has sophisticated capabilities that create the risk that TikTok can clandestinely shape narratives and elevate favorable opinions while suppressing statements and news that the PRC deems negative.

(8) On January 18, 2024, the Select Committee on Strategic Competition between the United States and the Chinese Communist Party of the House of Representatives was briefed by a set of senior interagency officials to discuss these matters.

(9) On March 22, 2023, elements of the intelligence community provided a classified briefing on the threat to members of the Permanent Select Committee on Intelligence of the House of Representatives and leadership for the Committee on Energy and Commerce of the House of Representatives.

(10) On April 26, 2023, the executive branch provided a classified briefing on the threat to members of the Committee on Commerce, Science, and Transportation and the Select Committee on Intelligence of the Senate.

(11) On June 5, 2023, the executive branch provided a classified briefing on the threat to staff of the Committee on Banking of the Senate and the Committee on Energy and Commerce of the House of Representatives.

(12) In June 2023, at the request of the Permanent Select Committee on Intelligence of the House of Representatives, the intelligence community provided a classified threat briefing open to all Members of the House of Representatives.

(13) On November 15, 2023, elements of the intelligence community provided a classified briefing to the Select Committee on Intelligence and the Committee on Commerce, Science, and Transportation of the Senate on, inter alia, the Peoples Republic of China's conduct of global foreign malign influence operations, including through platforms such as TikTok.

Whereas Congress and the executive branch are of one mind on the risks presented by TikTok's data collection practices:

(1) On May 15, 2019, the President issued an Executive Order on Securing the Information and Communications Technology and Services Supply Chain, which stated that ''unrestricted acquisition or use in the United States of information and communications technology or services designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries . . . constitutes an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States''.

(2) On June 9, 2021, the President issued an Executive Order on Protecting Americans' Sensitive Data

from Foreign Adversaries, which stated that ''[f]oreign adversary access to large repositories of United States persons' data also presents a significant risk.'' The EO stated that ''the United States must act to protect against the risks associated with connected software applications that are designed, developed, manufactured, or supplied by persons owned or controlled by, or subject to the jurisdiction or direction of, a foreign adversary''.

(3) In May 2019, in connection with a review by the Committee on Foreign Investment in the United States (CFIUS), a company based in the PRC agreed to divest its interest in a popular software application reportedly due to concerns relating to potential access by the PRC to American user data from the application.

(4) On July 8, 2020, then-National Security Advisor, Robert O'Brien, stated that the CCP uses TikTok and other PRC-owned applications to collect personal, private, and intimate data on Americans to use ''for malign purposes''.

(5) On August 14, 2020, the President found ''there is credible evidence . . . that ByteDance, Ltd. . . . might take action that threatens to impair the national security of the United States''.

(6) In February 2023, the Deputy Attorney General, Lisa Monaco, stated, ''Our intelligence community has been very clear about [the CCP's] efforts and intention to mold the use of [TikTok] using data in a worldview that is completely inconsistent with our own.''. Deputy Attorney General Monaco also stated, ''I don't use TikTok and I would not advise anybody to do so because of [national security] concerns''.

(7) On July 13, 2022, Federal Communications Commission Commissioner, Brendan Carr, testified be-

fore the Subcommittee on National Security of the Committee on Oversight and Reform of the House of Representatives that ''there is a unique set of national security concerns when it comes to [TikTok]''.

(8) On March 23, 2023, the Secretary of State, Antony Blinken, testified before the Committee on Foreign Affairs of the House of Representatives that TikTok is a threat to national security that should be ''ended one way or another''.

Whereas the executive branch has sought to address the risks identified above through requiring ByteDance to divest its ownership of TikTok:

(1) On August 14, 2020, the President issued an Executive order directing ByteDance to divest any assets or property used to enable or support ByteDance's operation of the TikTok application in the United States and any data obtained or derived from TikTok application or Musical.ly application users in the United States. The Order, however, remains the subject of litigation.

(2) On August 6, 2020, the President issued an Executive order (E.O. 13942) that directed the Secretary of Commerce to take actions that would have prohibited certain transactions related to TikTok in 45 days if ByteDance failed to divest its ownership of TikTok. The companies and content creators using the TikTok mobile application filed lawsuits challenging those prohibitions, as a result of which two district courts issued preliminary injunctions enjoining the prohibitions.

(3) Following the multiple judicial rulings that enjoined the executive branch from enforcing the regulations contemplated in E.O. 13942, on June 9, 2021, the President issued a new Executive order that rescinded E.O. 13942, and directed the Secretary of Commerce to

more broadly assess and take action, where possible, against connected software applications that pose a threat to national security.

Whereas Congress has passed, and the executive branch has implemented, a ban on ByteDance-controlled applications like TikTok from Government devices because of the national security threat such applications pose; even so, the application's widespread popularity limits the effectiveness of this step:

(1) Prior to 2022, several Federal agencies, including the Departments of Defense, State, and Homeland Security, had issued orders banning TikTok on devices for which those specific agencies are responsible.

(2) On December 29, 2022, following its adoption by Congress, the President signed into law a bill banning the use of TikTok on Government devices due to the national security threat posed by the application under its current ownership.

(3) A majority of States in the United States have also banned TikTok on State government devices due to the national security threat posed by the application under its current ownership.

(4) To date, as long as TikTok is subject to the ownership or control of ByteDance, no alternative to preventing or prohibiting TikTok's operation of the application in the United States has been identified that would be sufficient to address the above-identified risks.

(5) The national security risks arise from and are related to the ownership or control of TikTok by a foreign adversary controlled company. Severing ties to such foreign adversary controlled company, for example by a full divestment, would mitigate such risks.

(6) As has been widely reported, TikTok, Inc. has proposed an alternative, a proposal referred to as ''Project Texas,'' which is an initiative to try and satisfy concerns relating to TikTok's handling of United States user data.

(A) Under the proposal, United States user data would be stored in the United States, using the infrastructure of a trusted third party.

(B) That initiative would have allowed the application algorithm, source code, and development activities to remain in China under ByteDance's control and subject to PRC laws, albeit subject to proposed safeguards relating to cloud infrastructure and other data security concerns. Project Texas would also have allowed ByteDance to continue to have a role in certain aspects of TikTok's United States operations.

(C) Project Texas would have allowed TikTok to continue to rely on the engineers and back-end support in China to update its algorithms and the source code needed to run the TikTok application in the United States.

(D) Allowing code development in and access to United States user data from China potentially exposes United States users to malicious code, backdoor vulnerabilities, surreptitious surveillance, and other problematic activities tied to source code development.

(E) Allowing back-end support, code development, and operational activities to remain in China would also require TikTok to continue to send United States user data to China to update the machine learning algorithms and source code for the

application, and to conduct related back-end services, like managing users' accounts.

(7) On January 31, 2024, the Director of the Federal Bureau of Investigation, Christopher Wray, testified before the Select Committee on Strategic Competition between the United States and the Chinese Communist Party of the House of Representatives that TikTok gives the PRC ''the ability to control data collection on millions of users, which can be used for all sorts of intelligence operations or influence operations,'' and ''the ability, should they so choose, to control the software on millions of devices, which means the opportunity to technically compromise millions of devices''.

(8) The risks posed by TikTok's data collection would be addressed by the Protecting Americans from Foreign Adversary Controlled Applications Act, despite the potential that the PRC might purchase similar types of data from private data brokers.

(9) The degree of risk posed by TikTok has increased alongside the application's immense popularity in the United States.

Resolved, That the House of Representatives has determined that ByteDance and TikTok pose an unacceptable risk to the national security of the United States.

○