SENATE THIRD READING
SB 74 (Dodd and Jones)
As Amended August 17, 2023
2/3 vote. Urgency

SUMMARY

Establishes a rebuttable presumption that some executive branch state agencies shall prohibit use of certain social media platforms (defined to include TikTok) on state electronic devices but also allows an agency to overcome the presumption and use TikTok on state devices with a written finding that using the platform is necessary for an official state purpose and other requirements.

Major Provisions

1) Requires some state agencies, when implementing existing social media and cybersecurity policies and authorizing any installation or download of an application for a particular social media platform on a state-issued or state-owned electronic device, to adopt risk mitigation strategies tailored to the risks posed by that application for a social media platform.

2) For purposes of adopting risk mitigation strategies, establishes a rebuttable presumption that a state agency shall prohibit installation or download on that agency's state devices any social media platform if a "country of concern," defined to include China, owns or controls that platform, has substantial influence over its content moderation practices, or controls the platform's software or algorithm.

3) Authorizes a state agency to overcome the rebuttable presumption and use the social media platform if the state agency:

   a) implements existing state social media and cybersecurity policies in compliance with the Statewide Information Management Manual (SIMM) administered by the California Department of Technology (CDT);

   b) Makes a written finding that use of the platform is necessary for an official state purpose;

   c) Authorizes use only for that official state purpose and for no longer than necessary to complete that purpose; and

   d) Prior to authorizing installation or download, submits documentation of compliance to CDT, with state agencies already using the platform required to submit documentation of compliance within 30 days of this bill taking effect.

4) Includes an urgency clause stating that it is necessary for this bill to take immediate effect in order to protect against imminent threats to data security.

COMMENTS

1) *California's Existing Social Media Policy for State Agencies*. CDT, as part of its duties to manage the state's information technology (IT) resources, maintains the SIMM, which includes standards that state agencies must use to comply with state IT policy. Section 66B of the SIMM is the "Social Media Standard," which begins by encouraging state agencies to use social media technologies to engage their customers and employees where appropriate,

subject to risk mitigation requirements. Each state agency, before enabling access to a platform on a state device, is required to conduct a formal risk assessment and identify mitigation strategies for risks including "exposure or leakage of sensitive or protected information" and "malware introduction into the organization's IT environment." Agencies can allow connection to only platforms the agency approves in accordance with SIMM.

Many California state officials, the Governor, and legislators regularly use social media platforms including X (formerly Twitter), Facebook, Instagram and TikTok, among others, for reaching the public. Recent reports state that TikTok, which launched in 2017, has about 150 million users nationwide, and is one of the most downloaded social media platforms, especially among young people. A recent court filing by major nationwide news organizations and content providers describes TikTok as "a key part of the digital public square" and a "unique" and "vital" tool for newsgathering and dissemination of information about public affairs.

2) *Federal and State Bans on Use of TikTok*. The genesis of this bill is from the same concern that led the federal government and more than 30 states to impose TikTok bans. TikTok is owned by ByteDance, a company based in China and, according to the Federal Bureau of Investigation, the Chinese Communist Party could use applications owned by ByteDance to exploit Americans' user data for espionage operations, to control their mobile device software, and to manipulate content for influence operations. State bans, by statute or executive order, mostly prohibit use of TikTok on government devices. Many also ban use of TikTok by any state contractor. Montana is the only state that prohibits any use of TikTok by anyone within the state.

   Pending lawsuits claim the Montana law is unconstitutional in violation of the First Amendment right to free speech. Federal courts concluded that executive orders generally banning TikTok by former President Trump were unconstitutional. In contrast, measures like this bill that ban TikTok only on government devices are much less likely to raise First Amendment issues because of government authority to manage its employees and protect the security of government assets. However, some say any government ban on a specific mode of communication can be a slippery slope toward infringing First Amendment rights.

3) *Federal Ban Has Limited Exceptions*. The guidelines implementing the federal TikTok ban issued in February 2023 required all federal executive branch agencies, within 30 days, to remove TikTok from federal devices and, within 90 to 120 days, to ensure that federal contractors do not use TikTok. The guidelines allow "limited exceptions" to the TikTok ban only for law enforcement activities, national security activities, and security research. Agencies' use of TikTok for these limited purposes must be "critical to their mission and alternative approaches [ ] not viable." Blanket exceptions for an entire agency are not permitted. Agency heads must grant any exception in writing with a detailed description of the exception and risk mitigation activities to prevent access to sensitive data. An exception can last only a year and then must be renewed. Agencies are required to report all exceptions granted to the Office of Management and Budget.

4) *This Bill Adds to SIMM Requirements.* The bill builds on the existing SIMM 66B in two ways. It requires agencies to adopt risk mitigation strategies that are tailored to the specific risks of each particular social media platform. It also establishes a rebuttable presumption that an agency shall prohibit use of a social media platform owned or controlled by a

"country of concern." The bill defines "country of concern" to mean countries identified by the International Traffic in Arms Regulations, a list that includes including Belarus, Burma, China, Cuba, Iran, North Korea, Syria, Venezuela, Afghanistan, Cambodia, Central African Republic, Cyprus, Democratic Republic of Congo, Ethiopia, Eritrea, Haiti, Iraq, Lebanon, Libya, Russia, Somalia, South Sudan, Sudan and Zimbabwe. The requirements that must be met for a state agency to overcome the rebuttable presumption and authorize use of TikTok are somewhat aligned with the exception provisions in the federal TikTok ban.

5) *This Bill Has Limited Application*. This bill, an urgency measure, applies to use of social media platforms by any state agency subject to the SIMM, generally the agencies and departments that report to the Governor. This bill does *not* apply to any of the following:

   a) State agencies established by the state constitution, including Secretary of State, Controller, Treasurer, Attorney General, Insurance Commissioner, Superintendent of Public Instruction, and State Board of Equalization

   b) The Legislature

   c) The Lieutenant Governor

   d) The judicial branch

   e) The University of California and California State University systems.

   This bill applies only to state-issued or state-owned devices. It does not apply to a state employee's personal device that may be used for state purposes, such as a personal device with state email. It does not apply to use of TikTok by a state contractor.

6) *Letter from TikTok*. Although not taking a formal position on this bill, TikTok submitted a letter stating the following:

   > "TikTok, Inc., with U.S. headquarters based in Los Angeles, California, is an entertainment company with more than 150 million American users, including 5 million businesses, who use the service to connect with different communities of interest ranging from hiking, education, cooking, books and much more. We offer users a multitude of controls to protect their privacy and personally identifiable information. In addition, we have partnered with Oracle to store all U.S. user data on their cloud infrastructure in the U.S., and they are currently inspecting and validating our source code to ensure it is safe and secure from foreign influence.
   >
   > Citing a recent incident at the Department of Finance, this bill has been characterized as ensuring the state takes all measures to secure the cybersecurity infrastructure from threats of access and breach. If this is the goal of the measure, prohibiting one type of service will not reach this goal.
   >
   > We suggest amending the measure with a more comprehensive approach; specifically, amendments which would prohibit all types of entertainment and social media platforms or applications from being downloaded or installed on state-owned devices. Given the critically important information state agencies hold, we share the goal of ensuring

California has secure cybersecurity infrastructure and look forward to working with you to reach that goal."

According to the Author

Social media apps are ubiquitous in our daily lives, but there is growing concern about information theft and data collection that comes with their use. Prohibiting high-risk apps on state phones and other devices is a commonsense way to prevent exposure of our sensitive material and the possible tracking or data breaches. Clearly there are bad actors out there, and we can't afford to let them in.

Arguments in Support

The Consumer Federation of California, states the following:

Social media applications are a big component of consumers lives, allowing them to network and interact with or generate content. However, many companies are able to collect and access data, often of a personal nature, as a result of a user's interaction with these apps. This data on consumers is the most valuable asset many of these companies have, and is subject to breach as well as manipulation in a situation where a government takes at least a partial ownership interest in a social media company, as is the case with the Chinese government and Bytedance, the owner of TikTok.

Arguments in Opposition

No opposition on file.

FISCAL COMMENTS

According to the Assembly Appropriations Committee:

1) Costs of an unknown, but likely significant, amount across state agencies to adopt specified risk mitigation strategies, which could include IT resources to prohibit staff from accessing certain apps, and, if needed, submit documentation of compliance to CDT to overcome the rebuttable presumption to use certain apps for an official state purpose.

2) Annual costs of approximately $1.5 million to CDT for five positions and a contract with a vendor specializing in mobile apps to ensure oversight of state agencies' risk mitigation strategies, including performing ongoing social media risk analysis for countries of concern and reviewing rebuttable presumption compliance documentation.

VOTES

SENATE FLOOR: 40-0-0
YES: Allen, Alvarado-Gil, Archuleta, Ashby, Atkins, Becker, Blakespear, Bradford, Caballero, Cortese, Dahle, Dodd, Durazo, Eggman, Glazer, Gonzalez, Grove, Hurtado, Jones, Laird, Limón, McGuire, Menjivar, Min, Newman, Nguyen, Niello, Ochoa Bogh, Padilla, Portantino, Roth, Rubio, Seyarto, Skinner, Smallwood-Cuevas, Stern, Umberg, Wahab, Wiener, Wilk

ASM ACCOUNTABILITY AND ADMINISTRATIVE REVIEW: 6-0-1
YES: Petrie-Norris, Dixon, Bains, Davies, Rodriguez, Wilson
ABS, ABST OR NV: Stephanie Nguyen

ASM APPROPRIATIONS: 16-0-0
YES: Holden, Megan Dahle, Bryan, Calderon, Wendy Carrillo, Dixon, Mike Fong, Hart, Lowenthal, Mathis, Papan, Pellerin, Sanchez, Soria, Weber, Wilson

UPDATED

VERSION: August 17, 2023

CONSULTANT: Jacqueline Kinney / A. & A.R. / (916) 319-3600 FN: 0001611