Date of Hearing: July 5, 2023

ASSEMBLY COMMITTEE ON ACCOUNTABILITY AND ADMINISTRATIVE REVIEW
Cottie Petrie-Norris, Chair
SB 74 (Dodd) – As Amended May 18, 2023

SENATE VOTE: 40-0

SUBJECT: State entities: state-owned or state-issued devices: social media platforms

SUMMARY: This bill requires state entities to prohibit use of a social media platform on a state-issued or state-owned electronic device if the platform is owned or controlled by a "country of concern" but also provides that a state entity is not prohibited from using such a social media platform for "official state purposes." Specifically, **this bill**:

1) Requires a state entity to prohibit an application for a social media platform from being installed or downloaded on that entity's state-issued or state-owned electronic device if any of the following conditions are met:

    a. An "entity of concern" or a "county of concern" directly or indirectly owns, directly or indirectly controls, or holds 10 percent or more of the voting shares of the social media company that owns the platform.

    b. An "entity of concern" or a "country of concern" has substantial direct or indirect influence over the social media company that owns the social media platform.

    c. The social media platform uses software or an algorithm controlled by a "country of concern."

2) Provides that this bill does not prohibit an application for a social media platform from being installed or downloaded on a state entity's state-issued or state-owned electronic device if the state entity uses that application for official state purposes, including, but not limited to, official communications to the public on behalf of the state entity, cybersecurity research, and law enforcement activities.

3) Defines "country of concern" to mean a country identified by the International Traffic in Arms Regulations in Section 126.1 of Part 126 of Title 22 of the Code of Federal 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.

4) Defines "entity of concern" to mean a company that is domiciled in, is headquartered in, has its principal place of business in, or is organized under the laws of, a country of concern.

5) Defines "state entity" to mean an entity within the executive branch under direct authority of the Governor, including, but not limited to, all departments, boards, bureaus, commissions, councils, and offices.

6) 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.

EXISTING LAW:

1) Makes it unlawful for any elected state or local officer, appointee, employee, or consultant, to use or permit others to use "public resources" for a campaign activity or personal or other purposes not authorized by law, with "public resources" defined to include state telephones and computers. (Gov. Code Sec. 8314)

2) Establishes the California Department of Technology (CDT) within the Government Operations Agency with duties to manage and direct the state's IT resources and establish IT policies for state agencies, including state use of social media platforms. (Gov. Code Sec. 11545)

3) Requires each state agency to have a chief information officer with duties that include ensuring the agency complies with state IT policies established by CDT and other agencies, including IT security. (Gov. Code Sec. 11546.1)

4) Establishes the California Office of Emergency Services (CalOES) with duties to lead the state's cybersecurity initiatives and response to cyber incidents that could damage the state's infrastructure including IT and computer networks. (Gov. Code Sec. 8585)

5) Defines "social media company" to mean a person or entity that owns or operates one or more social media platforms. (B&P Code Sec. 22675)

6) Defines "social media platform" to mean a public or semipublic internet-based service or application that has users in California and that meets other criteria. (B&P Code Sec. 22675)

FISCAL EFFECT: The Legislative Counsel has keyed this bill as fiscal.

COMMENTS:

1) *Author's Purpose*: 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."

2) *California's Existing Social Media Policy for State Agencies*. CDT, as part of its duties to manage the state's IT resources, maintains the Statewide Information Management Manual (SIMM), which includes standards, instructions, forms and templates that state agencies must use to comply with state IT policy. Each individual agency is responsible for its own IT policy consistent with the SIMM. Section 66B of the SIMM is the "Social Media Standard" (SIMM 66B), which begins by encouraging state agencies to use social media technologies to engage their customers and employees where appropriate, subject to risk mitigation

requirements.[1] Many California state officials, the Governor, and legislators regularly use social media platforms including 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.

SIMM 66B requires each state agency, before authorizing and enabling internet access from a state device to any social media platform, to conduct a formal risk assessment and identify mitigation strategies for risks including potential "exposure or leakage of sensitive or protected information" and "malware introduction into the organization's IT environment." Further, SIMM 66B requires each agency to allow connection to "only those Social Media web sites that have been authorized by agency management in accordance with the requirements within this and other agency and state policies." These other policies include, for example, SIMM 5300, state agency cybersecurity requirements[2] and all cybersecurity policies of CalOES or any other state agency with cybersecurity duties.

3) *Federal and State Bans on Use of TikTok.* Although this bill does not call out TikTok by name, its genesis is from the same concern that led the federal government and more than 30 states to impose a variety of bans on use of TikTok. This concern is that 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. Some also prohibit use of WeChat, a Chinese instant messaging application. Montana is the only state that prohibits any use of TikTok by anyone within the state.

   Separate lawsuits by TikTok and TikTok users/creators 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.

4) *Federal Ban on TikTok on Government Devices, with Limited Exceptions*. The federal "No TikTok on Government Devices Act," enacted in December 2022 as part of an omnibus appropriations bill, directs the Office of Management and Budget (OMB) to develop guidelines for agencies to remove TikTok from federal devices. An OMB memorandum issued in February 2023 required all executive branch agencies, within 30 days, to remove and disallow installation of TikTok on federal devices.[3] Within 90 to 120 days, each federal agency is required to ensure that its contracts do not involve use of TikTok by any contractor.

---

[1] https://cdt.ca.gov/wp-content/uploads/2021/04/SIMM_66B.pdf.
[2] Statewide Information Management Manual (SIMM) | CDT (ca.gov)
[3] M-23-13 (whitehouse.gov).

In addition, federal agencies are required to establish a process to adjudicate "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 OMB.

5) *This Bill's Ban Has a Broad Exception*. This bill is an urgency measure, to take effect immediately, based on the stated need "to protect against imminent threats to data security." The bill requires a state entity to prohibit installing or downloading on a state device any social media platform that the author describes as "high-risk" by virtue of it being owned or controlled by a "country of concern." At the same time, despite this prohibition, the bill provides that it does *not* prohibit a state entity to install or download this same "high-risk" social media platform if the state entity uses it for "official state purposes." This bill does not define "official state purpose." Under current law that prohibits use of any state resources for personal use, "official state purpose" could be any use of a "high-risk" platform that is not a personal use.

6) *This Bill Applies to Some Executive Branch Agencies*. This bill applies to use of social media platforms by any state entity within the executive branch that is under the direct authority of the Governor, including all departments, boards, bureaus, commissions, councils, and offices. Under this definition, the bill's ban on use of "high risk" social media platforms does *not* apply to any of the following:

   - 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
   - The Legislature
   - The Lieutenant Governor
   - The judicial branch
   - 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.

7) *This Bill Applies to "High Risk" Platforms*. The ban in this bill applies only to a social media platform that is "high risk" under the definitions and criteria in the bill. These include if the platform is owned by a company domiciled in one of the 24 countries "of concern" or one of those countries has substantial control over the platform by being able to:

   - compel the company to share American users' data with that country
   - control the platform's content moderation practices
   - control the platform's software or algorithms

   The author and TikTok have both stated that the bill covers TikTok. It is uncertain what other social media platforms may be covered.

8) *Amendment to Align this Bill with SIMM and Ensure Accountability*. Given this bill's very broad exception to its prohibition on agency use of TikTok, the bill effectively operates to authorize any state entity to use TikTok for any "official state purpose." If the bill is enacted, this new *statutory* authorization for a state entity to use TikTok for any "official state purpose" may supersede the SIMM, which is a *regulation*, not a statute. Therefore, TikTok may be the only social media platform a state entity could use for any "official state purpose" without the risk analysis, risk mitigation strategies, and other requirements specified in SIMM 66B. Moreover, this bill provides no enforcement or accountability for how or when a state entity may authorize use of TikTok for an "official state purpose." The SIMM process, on the other hand, provides accountability by requiring state agencies to document and certify its compliance with risk mitigation, cybersecurity, and other requirements. In addition, the exception in this bill is more permissive than the federal TikTok ban on government devices, which provides for only limited exceptions with significant documentation and accountability requirements.

   For all of these reasons, this bill may be more likely to accomplish the author's intent by shifting the framework from a prohibition with a big exception to instead align with SIMM 66B and require agencies to adopt appropriate risk mitigation strategies tailored to the specific risks posed by any particular social media platform. For example, if risks posed by a social media platform due to its ownership and control by a hostile or authoritarian foreign country are deemed unacceptable, the mitigation strategy could be for an agency to not authorize *any* use of that platform, even for an "official state purpose." *Thus, the committee may wish to consider amending this bill by striking the prohibition and exception provisions and instead state the following*:

   > A state agency, when implementing its social media policy pursuant to the Department of Technology's State Information Management Manual, and authorizing any agency use of a particular social media platform on a state-issued or state-owned electronic device for an official state purpose, shall adopt risk mitigation strategies tailored to risks posed by that social media platform.

9) *Amendment to Apply this Bill to Agencies Subject to SIMM*. This bill applies to any state entity that reports to the Governor. The SIMM applies to the following as specified in Government Code Section 11546.1(e):

   > (e) (1) For purposes of this section, "state agency" means the Transportation Agency, Department of Corrections and Rehabilitation, Department of Veterans Affairs, Business, Consumer Services, and Housing Agency, Natural Resources Agency, California Health and Human Services Agency, California Environmental Protection Agency, Labor and Workforce Development Agency, and Department of Food and Agriculture.
   >
   > (2) For purposes of this section, "state entity" means an entity within the executive branch that is under the direct authority of the Governor, including, but not limited to, all departments, boards, bureaus, commissions, councils, and offices that are not defined as a "state agency" pursuant to paragraph (1).

   Thus, to conform with the amendment to align with the SIMM, the committee may wish to consider amending this bill by making it apply to the same entities subject to the SIMM.

10) *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.
>
> These data breaches are a threat not only to consumers but also to state agencies. In December 2022 the California Office of Emergency Services (OES) announced the state's Cybersecurity Integration Center responded to an incident involving the California Department of Finance. At least two dozen states have instituted some type of limitation on the use of high-risk apps on state-controlled or provided devices. The Biden Administration also announced in February that it was giving federal agencies 30 days to remove specific apps from government devices.
>
> Senate Bill 74 seeks to ensure this commitment in the state of California by requiring that state entities prohibit access to high-risk social media apps on state-owned or state issues electronic devices if specified conditions are met, including that an entity of concern or a country of concern directly or indirectly owns, controls, or holds 10% or more of the voting shares of the social media company that owns the app. Rather than naming apps, the bill sets forth criteria that would apply to all applications. SB 74 does not apply to any private phones or electronic devices of any private individual in California, or the personal mobile devices of any state employee. Furthermore, it only reinforces the prohibition of high-risk apps once a situation triggering this action has occurred."

11) *Letter from TikTok*. Although not taking a formal position on this bill, TikTok submitted a letter to the committee 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."

12) *Related Legislation*. AB 227 (Sanchez, 2023). This bill bans use of TikTok on state devices but was never heard in the Assembly Privacy and Consumer Protections Committee. The author joined SB 74 as a principal co-author.

REGISTERED SUPPORT / OPPOSITION:

Support

Consumer Federation of California

Opposition

None on file.

Analysis Prepared by: Jacqueline Kinney / A. & A.R. / (916) 319-3600