Office of Senate Floor Analyses
(916) 651-1520 Fax: (916) 327-4478

THIRD READING

Bill No: SB 74
Author: Dodd (D) and Jones (R), et al.
Amended: 5/18/23
Vote: 27 - Urgency

SENATE GOVERNMENTAL ORG. COMMITTEE: 15-0, 4/25/23
AYES: Dodd, Wilk, Alvarado-Gil, Archuleta, Ashby, Bradford, Glazer, Jones, Nguyen, Ochoa Bogh, Padilla, Portantino, Roth, Rubio, Seyarto

SENATE APPROPRIATIONS COMMITTEE: 7-0, 5/18/23
AYES: Portantino, Jones, Ashby, Bradford, Seyarto, Wahab, Wiener

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

SOURCE: Author

DIGEST: This bill requires state entities to prohibit the downloading or installation of high-risk social media applications on those entities' state-owned or state-issued devices if a country or entity of concern owns or controls the social media company, as specified.

ANALYSIS:

Existing law:

1) Establishes the Department of Technology (CDT) and provides for a Director of Technology to supervise the department and report directly to the Governor on issues relating to information technology (IT).

2) Requires the Office of Emergency Services (OES) to establish and lead the California Cybersecurity Integration Center (Cal-CSIC) to reduce the likelihood and severity of cyber incidents that could damage California's economy, its critical infrastructure, or public and private sector computer networks in the state.

This bill:

1) Requires state entities 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 application.

   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, as specified.

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

2) Includes an exception from the above prohibition if the state entity uses that application for official state purposes, including, but not limited to, any of the following: 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 as set forth in Section 126.1 of Part 126 of Title 22 of the Code of Federal Regulations.

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) Includes an urgency statute necessary for the immediate preservation of the public peace, health, or safety.

Background

Purpose of the Bill. According to the author's office, "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."

Growing Concern Surrounding High-Risk Social Media Applications. In an attempt to keep U.S. data safe, the federal Office of Management and Budget Director Shalanda Young told agencies in a guidance memorandum sent in March of this year that all federal agencies must eliminate certain high-risk apps from their federal phones and electronic systems. That order proceeded action by the U.S. Congress in 2022, and similar actions from Canada, the European Union, Taiwan, India, and more than half of U.S. states.

The prohibitions, which apply to internet-enabled devices such as mobile phones, tablets, and computers, have been growing quickly since November 2022, when Federal Bureau of Investigation (FBI) Chris Wray expressed concerns that the Chinese Communist Party (CCP) could use apps owned by tech giant ByteDance to exploit Americans' user data for espionage operations and to control their mobile device software. Later the next month, Wray again warned that these apps could be used to manipulate content for influence operations.

These warnings came on the heels of an internal investigation by ByteDance that found employees had tracked multiple journalists covering the company on the east coast of the United States, improperly gaining access to their IP addresses and user data in an attempt to identify whether they had been in the same locales as ByteDance employees. According to materials reviewed by *Forbes,* ByteDance tracked multiple *Forbes* journalists as part of a covert surveillance campaign, which was designed to unearth the source of leaks inside the company following a drumbeat of stories exploring the company's ongoing links to the CCP.

Further, TikTok is not available in mainland China. However, ByteDance does operate a separate version of the app for their domestic market. While that app and TikTok have similar user interfaces and features, they are separate apps and have separate user bases due to China's internet regulation practices, often referred to as the "Great Firewall." Most American social media apps such as Facebook, Instagram, Twitter, and Snapchat are blocked in mainland China, due to the country's stringent internet censorship policies. This policy is used to regulate the internet domestically and block access to certain foreign websites and platforms.

December 2022 Cybersecurity attack on Department of Finance. In late 2022, multiple federal and state agencies responded to a cybersecurity attack on the California Department of Finance (DOF). According to OES, the "intrusion was proactively identified through coordination with state and federal security partners. Upon identification of this threat, digital security and online threat-hunting experts were rapidly deployed to assess the extent of the intrusion and to evaluate, contain and mitigate future vulnerabilities.

The response effort includes multiple public and private agencies including the partners who make up the Cal-CSIC: the Governor's Office of Emergency Services, Department of Technology, California Military Department and California Highway Patrol. While we cannot comment on specifics of the ongoing investigation, we can share that no state funds have been compromised, and the Department of Finance is continuing its work to prepare the Governor's Budget that will be released next month."

OES stated that the "incident serves as an important reminder as to why Governor Gavin Newsom launched the state's first multi-year cybersecurity roadmap Cal-Secure, which strengthens the state's cybersecurity measures and prioritizes the resources to manage the most significant cyber risks and safeguard those services. The Newsom Administration, in partnership with the legislature, has advanced $260 million to bolster the state's ability to prevent and respond to cyberattacks. The FY21-22 state budget also included $38.8 million ongoing to mature the state's overall security posture, improve statewide information security initiatives, analyze cyber threat intelligence and mitigate potential threats."

While full details around the attack are still limited, the Russia-affiliated group claiming responsibility stated they had stolen 76GB of files from the agency, including "databases, confidential data, financial documents, certification, IT documents, and sexual proceedings in court." The investigation into the attack and total extent of the damage is still under investigation.

High-Risk Apps and Artificial Intelligence. In recent years, the increasing power and influence of artificial intelligence (AI) and algorithms on social media platforms have raised critical concerns about data privacy, information manipulation, and potential threats to democracy. As more users turn to social media platforms for news, communication, and entertainment, understanding the impact of these algorithms on user behavior and data security is crucial.

One of the primary concerns regarding social media algorithms is the lack of transparency and accountability. Users and regulators often have little to no understanding of how these algorithms function or how they influence the content users see on their feeds. This opacity can lead to the spread of misinformation, radicalization, and polarization among users, causing harm to individuals and society as a whole.

An algorithm is a set of rules or instructions that a computer follows to perform a task or solve a problem. In the context of social media platforms, algorithms are used to determine what content to show you, based on your interests, behavior, and other factors. The problem with countries of concern controlling social media

algorithms is that they might have different priorities or motivations than domestic companies. A country of concern could potentially push certain types of content into our consciousness without us being aware of it. This could be done for various reasons, such as promoting their own interests, spreading misinformation, or influencing public opinion.

Imagine you're scrolling through a social media app, and it persistently displays videos related to a specific topic or promoting a certain viewpoint. Gradually, this can shape your perception of the world and influence your beliefs and opinions, all without you ever realizing it, much like a frog in a slowly warming pot on the stove. The issue lies in our inability, as users, to monitor or control the algorithm's actions. We cannot discern how it determines which content to display or why it promotes particular media.

By downloading an app that employs such advanced technologies, it's as if we're unwittingly inviting third-party algorithms into our lives to make decisions for us, without even recognizing their influence. This lack of transparency and control is concerning for several reasons: (1) Manipulation: High-risk apps could use their control over algorithms to manipulate our perceptions and beliefs, leading to a distorted view of reality; (2) Misinformation: Algorithms can spread false information or fake news, which can have serious consequences for society, such as eroding trust in institutions or fueling polarization; (3) Privacy: Foreign companies might have access to our personal data and online behavior, which could potentially be misused or shared with countries of concern without our consent; (4) State security: A country of concern exerting control over social media algorithms could pose a risk to California's security if it's used to sway public opinion on sensitive issues or interfere in elections.

It is important to remember that algorithms are not conscious, moral, or ethical decision-makers and therefore do not have First Amendment rights. They are artificially created sets of instructions designed to perform specific tasks, such as curating content on social media platforms. These algorithms are not human beings expressing opinions or ideas but rather tools created and controlled by companies or governments. The technology has advanced to such a point that many experts, and the very creators of the algorithms, sometimes cannot explain why the machine made a certain decision.

Recent Revelations. National media reported in March of 2023, that the Biden administration had been moving to ban a specific social media app (TikTok) from the United States unless the app's owners (ByteDance) agreed to spin off their share of the social media platform. This preceded an apparent ultimatum by the

United States multiagency panel known as the Committee on Foreign Investments in the United States (CFIUS). CFIUS is the regulatory arm that reviews foreign investments in the U.S. The panel has been reviewing national security risks under heightened to pressure to wrap up from U.S. senators on both sides of the aisle. The divestiture request was first reported in March by the *Wall Street Journal*, and later confirmed by the company while declining to discuss specifics of the request.

Additionally, a dozen United States Senators introduced bipartisan legislation expanding President Joe Biden's legal authority to ban specific social media platforms nationwide. The legislation, called the Restricting the Emergence of Security Threats that Risk Information and Communications Technology (RESTRICT) Act, does not target individual companies, but instead aims to give the United States government new powers, up to and including a ban, against foreign-linked producers of electronics or software that the United States Commerce department deems to be a national security risk. On March 23rd, TikTok's CEO Shou Zi Chew, testified during an informational hearing in Washington D.C. in front of the United States Congress.

In April 2023, the FBI arrested two alleged agents working for the CCP accused of attempting to harass and silence its critics in the United States. The Federal Department of Justice also charged 34 officers of the CCP's national police, all of whom are believed to live in China, with related offenses. Prosecutors allege that the CCP opened an "undeclared police station" in New York City that was used at least once to track down a pro-democracy activist living in California. These revelations, however, are not new. According to a recent report by Madrid-based human rights group Safeguard Defenders, the CCP has set up more than 100 such posts to monitor activity around the globe using bilateral security arrangements as a cover.

In May of this year, a former executive at ByteDance accused the company of a "culture of lawlessness," including stealing content from rival platforms in its early years, and called the company a "useful propaganda tool for the Chinese Communist Party." That claim is part of a wrongful dismissal suit filed by a former head of engineering for ByteDance's United States operations from August 2017 to November 2018. The lawsuit was recently filed in San Francisco Superior Court, and other claims include accusing ByteDance of having a special unit of Chines Communist Party members who "guided how the company advanced core Communist values." In an emailed statement responding to the lawsuit, ByteDance said that the company would "vigorously oppose what we believe are baseless claims and allegations in this complaint."

High-Risk Apps on State Devices. This bill seeks to address potential data security threats arising from the installation or download of specific social media platforms on state-owned electronic devices. By targeting social media platforms that are owned, controlled, or influenced by countries or entities of concern, the proposal aims to protect sensitive information and ensure the privacy of California employees and the data on their state-controlled devices. According to CDT, there are approximately 25,400 active mobile phones owned or controlled by the state of California.

This bill requires state entities to prohibit apps for social media from being installed or downloaded on that entity's state-issued or state-owned or state-issued electronic device if 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 app. This bill applies only to those state-owned and state-issued phones. This bill 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.

The bill references the International Traffic in Arms Regulations as set forth in the Code of Federal Regulations for guidance on the enumeration of "countries of concern."

According to that section of federal law, it is "the policy of the United States to deny licenses and other approvals for exports and imports of defense articles and defense services, destined for or originating in certain countries." Under existing federal law, the following countries have a policy of denial: Belarus, Burma, China, Cuba, Iran, North Korea, Syria, and Venezuela.

This bill includes exemptions for official use by a state entity, including but not limited to: official communications to the public on behalf of the state entity, cybersecurity research, and law enforcement activities. This bill includes an urgency statute, emphasizing the need for immediate action to protect against data security threats.

Related/Prior Legislation

AB 227 (Sanchez, 2023) would prohibit a person from installing a social media app on a state-owned or state-issued electronic device if specified conditions are met. (Pending in the Assembly Privacy and Consumer Protection Committee)

FISCAL EFFECT: Appropriation: No Fiscal Com.: Yes Local: No

According to the Senate Appropriations Committee, unknown fiscal impact for state entities that provide state-issued or state-owned electronic devices to meet the

enforcement requirements of this bill. One-time costs include IT resources to prohibit users from downloading or accessing certain social media applications or websites and staff time to develop or update trainings or notices regarding IT security on state-issued devices.

CDT anticipates the need for one permanent position and $663,000 in the first year and ongoing (General Fund). Costs include funding for a contract with a vendor that specializes in mobile applications.

SUPPORT: (Verified 5/18/23)

Consumer Federation of California

OPPOSITION: (Verified 5/18/23)

None received

ARGUMENTS IN SUPPORT: In support of this bill, the Consumer Federation of California writes that, "[s]ocial 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 ot 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."

Prepared by: Brian Duke / G.O. / (916) 651-1530
5/23/23 11:06:04

****** END ******