SENATE COMMITTEE ON GOVERNMENTAL ORGANIZATION
Senator Bill Dodd
Chair
2023 - 2024 Regular

Bill No:	SB 74	**Hearing Date:**	4/25/2023
Author:	Dodd & Jones, et al.		
Version:	4/10/2023 Amended		
Urgency:	Yes	**Fiscal:**	Yes
Consultant:	Brian Duke		

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

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) Imposes various duties on the director, including advising the Governor on the strategic management and direction of the state's IT resources and to identify, assess, and prioritize high-risk, critical information technology services and systems across state government, as specified.

3) 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.

4) Defines "social media company" to mean a person or entity that owns or operates one or more social media platforms.

5) 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, as specified.

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) 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.

3) 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.

4) Defines "state entity" to mean 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.

5) Includes an urgency statute necessary for the immediate preservation of the public peace, health, or safety in order to protect against imminent threats to data security.

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.

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."

Further, 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.

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, "[i]t 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.

Existing law defines a "social media platform" as a public or semipublic internet-based service or application that has users in California and that meets both of the following criteria: a substantial function of the service or application is to connect users in order to allow users to interact socially with each other within the service or application; the service or application allows users to construct a public or semipublic profile, populate a list of other users with whom an individual shares a social connection within the system, and create or post content viewable by other users.

This bill includes an urgency statute, emphasizing the need for immediate action to protect against data security threats.

Policy Considerations. As currently drafted, this bill applies to all state-owned and state-issued electronic devices. CDT reports that there are approximately 25,400 such devices in California. Some of these state-owned or state-issued devices are controlled by state law enforcement entities or for communicating important information to constituents in an effective manner that reaches citizens in the virtual communities that they are inhabiting.

The author may wish to consider amending the bill to allow for limited and narrow exemptions for legitimate state use of high-risk apps on state-owned or state-issued devices, when applicable, by adding the following:

(c)(1) This section 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, any of the following:

(A) Official communications to the public on behalf of the state entity.
(B) Cybersecurity research.
(C) Law enforcement activities.

(2) A state entity utilizing the exception provided in paragraph (1) shall report each use of that exception to the Department of Technology.

Prior/Related Legislation

SB 573 (Wahab, 2023) would limit employment opportunities for Legislative staff who separate from their employment with the Legislature, for any reason, for a period of two years after the separation, as specified. (Pending in the Senate Appropriations Committee)

SB 845 (Stern, 2023) would mandate third-party safety software providers to register with the Attorney General's (AG) office and meet specified requirements to access social media, requires large social media platforms to register with the AG within 30 days of meeting certain criteria, as specified. (Pending in the Senate Judiciary Committee)

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)

AB 1027 (Petrie-Norris, 2023) would require a social media platform to maintain records of communications between users of the platform for at least 168 hours. (Pending in the Assembly Privacy and Consumer Protections Committee)

AB 587 (Gabriel, Chapter 269, Statutes of 2022) requires social media companies to post their terms of service in a manner reasonably designed to inform all users of specified policies, and requires a social media company to submit semiannual reports, as specified, starting January 1, 2024, to the AG.

AB 1844 (Campos, Chapter 618, Statutes of 2012) prohibits an employer from requiring or requesting an employee or applicant for employment to disclose a user name or password for the purpose of accessing personal social media, to access personal social media in the presence of the employer, or to divulge any personal social media

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

SUPPORT:

None received

OPPOSITION:

None received