SB 757 - Carozza Testimony_FINAL.pdf
Uploaded by: Senator Mary Beth Carozza
Position: FAV

MARY BETH CAROZZA
Legislative District 38
Somerset, Wicomico,
and Worcester Counties

Education, Energy, and
the Environment Committee

Executive Nominations Committee

Annapolis Office
James Senate Office Building
11 Bladen Street, Room 316
Annapolis, Maryland 21401
410-841-3645 · 301-858-3645
800-492-7122 *Ext.* 3645
Fax 410-841-3006 · 301-858-3006
MaryBeth.Carozza@senate.state.md.us

THE SENATE OF MARYLAND
ANNAPOLIS, MARYLAND 21401

February 29, 2024
The Senate Education, Energy, and Environment Committee
SB 757 – State Information Technology – Prohibited Applications and Websites
Statement of Support by Bill Sponsor Senator Mary Beth Carozza

Thank you Chair Feldman, Vice Chair Kagan, and my fellow members of the esteemed Senate Education, Energy, and Environment Committee for this opportunity to present Senate Bill 757 – State Information Technology – Prohibited Applications and Websites as amended. I want to thank Committee members, Senators Hester, Brooks and Gallion for cosponsoring this legislation.

The amended bill reflects the recommendations of the Maryland Department of Information Technology. As amended, this legislation would establish a comprehensive Technology Advisory List similar to the U.S. State Department's Travel Advisories. This List would encompass applications and hardware solutions that pose a threat to Maryland's IT Infrastructure. The Maryland Department of Budget and Management would work collaboratively with DoIT to publish clear guidelines for units of State government to remove and prevent access to the software on this List. By taking this broader approach, Maryland can adapt to emerging threats to ensure the security of our State.

This legislation represents a critical step forward in safeguarding our State's information technology systems. Cybersecurity threats pose a constant and ever-evolving challenge, and we have a duty to protect the sensitive data of Marylanders and to ensure their safety and privacy is respected.

I thank you for your kind attention and consideration, and I respectfully request a favorable report on SB 757.

SB 757 Reprint.pdf
Uploaded by: Senator Mary Beth Carozza
Position: FAV

UNOFFICIAL COPY OF SENATE BILL 757

SENATE BILL 757

S1, P1 4lr2742
HB 1141/23 - HGO CF HB 617

By: **Senators Carozza, Bailey, Brooks, Charles, Elfreth, Gallion, Gile, Hester, James, Ready, and West**
Introduced and read first time: February 1, 2024
Assigned to: Education, Energy, and the Environment

A BILL ENTITLED

AN ACT concerning

State Information Technology - ~~Prohibited Applications and Websites~~ Restricted Software

FOR the purpose of prohibiting certain ~~applications from being used and certain websites~~ restricted software from being accessed , downloaded, or used by certain employees, agents, or entities on any information technology owned or leased by a unit of State government; requiring the Department of Budget and Management, in collaboration with the Department of Information Technology, to prepare guidance for units of State government to remove from and prohibit the use of and access to ~~certain applications and websites~~ restricted software on information technology owned or leased by the unit; and generally relating to ~~applications, websites,~~ restricted software and State information technology.

BY adding to
Article - State Finance and Procurement
Section 3.5-801 to be under the new subtitle "Subtitle 8. ~~Prohibited Applications and Websites~~ Restricted Software "
Annotated Code of Maryland
(2021 Replacement Volume and 2023 Supplement)

SECTION 1. BE IT ENACTED BY THE GENERAL ASSEMBLY OF MARYLAND, That the Laws of Maryland read as follows:

Article - State Finance and Procurement

SUBTITLE 8. ~~PROHIBITED APPLICATIONS AND WEBSITES~~ RESTRICTED SOFTWARE.

3.5-801.

(A) (1) IN THIS SECTION THE FOLLOWING WORDS HAVE THE MEANINGS INDICATED.

~~(2) "BYTEDANCE LTD." MEANS THE CHINESE INTERNET TECHNOLOGY COMPANY FOUNDED BY ZHANG YIMING AND LIANG RUBO IN 2012, AND ANY SUCCESSOR COMPANY OR ENTITY OWNED BY THE COMPANY.~~

~~(3)~~ (2) "INFORMATION TECHNOLOGY" HAS THE MEANING STATED IN § 3.5-301 OF THIS TITLE.

~~(4) "TENCENT HOLDINGS LTD." MEANS THE CHINESE MULTINATIONAL TECHNOLOGY AND ENTERTAINMENT CONGLOMERATE AND HOLDING COMPANY HEADQUARTERED IN SHENZHEN, CHINA, AND ANY SUCCESSOR COMPANY OR ENTITY OWNED BY THE COMPANY.~~

~~(5) "TIKTOK" MEANS THE VIDEO-SHARING APPLICATION DEVELOPED BY BYTEDANCE LTD. THAT HOSTS USER-SUBMITTED VIDEOS.~~

~~(6) "WECHAT" MEANS THE MULTIPURPOSE SOCIAL MEDIA, MESSAGING, AND PAYMENT APPLICATION DEVELOPED BY TENCENT HOLDINGS LTD.~~

(3) "RESTRICTED SOFTWARE" MEANS SOFTWARE THAT THE DEPARTMENT DETERMINES POSES A THREAT TO THE SECURITY OF THE STATE, INCLUDING SOFTWARE CREATED, OPERATED, OR OWNED BY A COMPANY THAT THE DEPARTMENT DETERMINES POSES A THREAT TO THE SECURITY OF THE STATE.

(B) THE DEPARTMENT SHALL PUBLISH AND MAINTAIN A LIST OF RESTRICTED SOFTWARE AND COMPANIES THAT THE DEPARTMENT DETERMINES POSES A THREAT TO THE SECURITY OF THE STATE.

~~(B)~~ (C) EXCEPT AS PROVIDED IN SUBSECTION ~~(C)~~ (D) OF THIS SECTION, AN EMPLOYEE OR AGENT OF A UNIT OR AN ENTITY CONTRACTING WITH A UNIT MAY NOT ACCESS, DOWNLOAD , OR USE ~~ANY APPLICATION, INCLUDING TIKTOK OR WECHAT, OR ACCESS ANY WEBSITE DEVELOPED BY BYTEDANCE LTD. OR TENCENT HOLDINGS LTD.~~ RESTRICTED SOFTWARE:

(1) ON ANY INFORMATION TECHNOLOGY OWNED OR LEASED BY THE UNIT; OR

(2) WHILE CONNECTED TO ANY WIRED OR WIRELESS INTERNET NETWORK OWNED, OPERATED, OR MAINTAINED BY THE STATE.

~~(C)~~ (D) THIS SECTION DOES NOT APPLY WHERE THE USE OF THE ~~APPLICATION OR ACCESS TO THE WEBSITE~~ RESTRICTED SOFTWARE IS NECESSARY FOR:

(1) LAW ENFORCEMENT ACTIVITIES;

(2) PROTECTING NATIONAL SECURITY; OR

(3) RESEARCH ON SECURITY PRACTICES.

(E) THE EXECUTIVE DIRECTOR OF THE DEPARTMENT OF LEGISLATIVE SERVICES MAY USE THE LIST MAINTAINED UNDER SUBSECTION (B) OF THIS SECTION AS GUIDANCE WHEN DEVELOPING INFORMATION TECHNOLOGY POLICIES FOR THE GENERAL ASSEMBLY AND THE DEPARTMENT OF LEGISLATIVE SERVICES.

SECTION 2. AND BE IT FURTHER ENACTED, That, on or before December 31, 2024, the Department of Budget and Management, in collaboration with the Department of Information Technology, shall publish guidelines to assist units of State government in:

(1) removing and preventing access to ~~applications and websites~~ restricted software prohibited under § 3.5-801 of the State Finance and Procurement Article, as enacted by Section 1 of this Act, from information technology owned and leased by the unit;

(2) maintaining an ongoing prohibition on ~~prohibited applications and websites~~ restricted software being installed, maintained, or accessed on any information technology owned and leased by the unit; and

(3) permitting the installation, maintenance, and access to prohibited ~~applications and websites~~ restricted software where it is necessary for:

(i) law enforcement activities;

(ii) protecting national security; and

(iii) research on security practices.

SECTION 3. AND BE IT FURTHER ENACTED, That this Act shall take effect October 1, 2024.

Senate Amendment.pdf
Uploaded by: Senator Mary Beth Carozza
Position: FAV

SB0757/613926/1

AMENDMENTS PREPARED BY THE DEPT. OF LEGISLATIVE SERVICES

14 FEB 24
09:45:50

BY: Senator Carozza
(To be offered in the Education, Energy, and the Environment Committee)

AMENDMENTS TO SENATE BILL 757
(First Reading File Bill)

AMENDMENT NO. 1

On page 1, in line 2, strike "**Prohibited Applications and Websites**" and substitute "**Restricted Software**"; in line 3, strike "applications from being used and certain websites" and substitute "restricted software"; in line 4, after "accessed" insert ", downloaded, or used"; in line 8, strike "certain applications and websites" and substitute "restricted software"; in lines 9 and 10, strike "applications, websites," and substitute "restricted software"; and in lines 13 and 14, strike "Prohibited Applications and Websites" and substitute "Restricted Software".

AMENDMENT NO. 2

On page 1, in line 20, strike "**PROHIBITED APPLICATIONS AND WEBSITES**" and substitute "**RESTRICTED SOFTWARE**".

On page 2, strike in their entirety lines 1 through 3, inclusive; in line 4, strike "**(3)**" and substitute "**(2)**"; strike in their entirety lines 6 through 14, inclusive; after line 14, insert:

"**(3) "RESTRICTED SOFTWARE" MEANS SOFTWARE THAT THE DEPARTMENT DETERMINES POSES A THREAT TO THE SECURITY OF THE STATE, INCLUDING SOFTWARE CREATED, OPERATED, OR OWNED BY A COMPANY THAT THE DEPARTMENT DETERMINES POSES A THREAT TO THE SECURITY OF THE STATE.**

(B) THE DEPARTMENT SHALL PUBLISH AND MAINTAIN A LIST OF RESTRICTED SOFTWARE AND COMPANIES THAT THE DEPARTMENT DETERMINES POSES A THREAT TO THE SECURITY OF THE STATE.";

in lines 15 and 24, strike "**(B)**" and "**(C)**", respectively, and substitute "**(C)**" and "**(D)**", respectively; in line 15, strike "**(C)**" and substitute "**(D)**"; in line 16, after "**NOT**" insert "**ACCESS,**"; in line 17, after "**DOWNLOAD**" insert a comma; strike beginning with "**ANY**" in line 17 down through the period in line 19 and substitute "**RESTRICTED SOFTWARE**"; strike beginning with "**APPLICATION**" in line 24 down through "**WEBSITE**" in line 25 and substitute "**RESTRICTED SOFTWARE**"; and after line 28, insert:

"**(E) THE EXECUTIVE DIRECTOR OF THE DEPARTMENT OF LEGISLATIVE SERVICES MAY USE THE LIST MAINTAINED UNDER SUBSECTION (B) OF THIS SECTION AS GUIDANCE WHEN DEVELOPING INFORMATION TECHNOLOGY POLICIES FOR THE GENERAL ASSEMBLY AND THE DEPARTMENT OF LEGISLATIVE SERVICES.**".

On page 3, in lines 1 and 8, in each instance, strike "applications and websites" and substitute "restricted software"; and in lines 4 and 5, strike "prohibited applications and websites" and substitute "restricted software".

SB757_USM_FWA.pdf
Uploaded by: Andy Clark
Position: FWA

SENATE EDUCATION, ENERGY, AND THE ENVIRONMENT COMMITTEE
Senate Bill 757
State Information Technology - Prohibited Applications and Websites
February 29, 2024
Favorable with Amendment

Chair Feldman, Vice Chair Kagan and committee members, thank you for the opportunity to share our position on Senate Bill 757. The bill bans the downloading and use of all products by ByteDance Ltd. and TenCent Holdings Ltd. from all state-owned information technology, including all devices and networks.

The University System of Maryland (USM) comprises 12 distinguished universities and three regional centers with distinct and unique approaches to the mission of educating students and promoting the economic, intellectual, and cultural growth of its surrounding community. These institutions are located throughout the state, from Western Maryland to the Eastern Shore. A range of institutional types complement this geographic diversity. The USM includes land-grant universities, regional universities, and HBCUs, together with universities whose missions focus on online education, professional and graduate education, and environmental education.

The Chancellor, USM Presidents, and the Board of Regents all understand the importance of protecting information and technological systems from foreign government hacking and monitoring and have found it's best to take a risk-based approach in the USM. The ability to tailor our environment to support the use of technology and information in low-risk situations while restricting and protecting our technology and information in high-risk situations is crucial. The USM believes strongly that it is best to pursue a more flexible approach than Senate Bill 757, as written, allows.

The global cybersecurity threat landscape is constantly evolving, and it is well known that, in addition to ByteDance Ltd. and TenCent Holdings Ltd., many other companies and applications are owned and influenced by foreign adversaries. For example, Telegram Messenger and Kaspersky Labs have known ties to the Russian government; and Pinduoduo, Alibaba, Huawei, and ZTE also have ties to the Chinese government.

Given how quickly modern technologies are developed and existing technologies evolve and change names; it may make more sense for the state to establish and maintain a list of

companies, applications, and hardware solutions that pose a threat to Maryland. This list could operate similarly to the way the US Department of State monitors global threats and maintains their Travel Advisories list. The Maryland Code could be used to establish and allocate resources to maintain a global technology advisory list, while the list itself is kept outside of the Maryland Code. The Maryland Department of Information Technology already operates the Office of Security Management (OSM) and the Maryland Information Sharing and Analysis Center (MD-ISAC). The OSM and the MD-ISAC could be logical groups to establish and maintain a global technology advisory list on behalf of all state units.

The solution we are suggesting is in line with the direction that the federal government began discussing last spring. On March 7, 2023, Congress introduced the RESTRICT Act. The bill requires federal actions to identify and mitigate foreign threats to information and communications technology (ICT) products and services (e.g., social media applications). Specifically, the US Department of Commerce must identify, deter, disrupt, prevent, prohibit, investigate, and mitigate transactions involving ICT products and services (1) in which any foreign adversary (such as China) has any interest, and (2) that pose an undue or unacceptable risk to U.S. national security or the safety of U.S. persons. The RESTRICT Act moves away from naming specific companies and products in statute or regulation and creates a structure to monitor and take appropriate steps to address the influence of foreign adversaries on our technology. We are suggesting that Senate Bill 757 be amended to operate similarly.

Lastly, instead of banning the use of particular technologies by state units, we recommend that Senate Bill 757 require all state units or entities contracting with a state unit perform an analysis of the risks and benefits posed by high-risk technologies on the state's technology advisory list, and as necessary put in place appropriate controls to address each risk. The controls a unit decides are best to address a risk can include banning the technology; but, if necessary, it could also include more nuanced controls. Compliance with this provision could be included in IT audits performed by the Maryland Office of Legislative Audits.

In the end, we all agree that we need to protect the state from the risks posed by foreign adversaries and malicious actors in general. The structure we have outlined above is forward looking and creates a solution that can evolve over time, provides the flexibility to keep up with the fast pace of the cybersecurity threat landscape, allows units to implement appropriate controls while still serving their communities, and includes checks and balances to hold state units accountable.

The USM understands that amendments have been proposed in the crossfile (House Bill 617) allowing the Executive Director of the Department of Legislative Services to use the restricted software list developed by DoIT as guidance.

The USM, and more importantly, all senior public institutions of higher education need the same, if not greater, flexibility to assess DoIT recommendations to restrict certain software deemed a "threat to the security of the State."

On page 2; after line 28 of the re-printed House-amended bill, the USM proposes a clarifying section to read:

(F) This subtitle applies to all units of the Executive Branch of State government including public institutions of higher education other than Morgan State University, the University System of Maryland, St. Mary's College of Maryland, and Baltimore City Community College.

The proposed amendment is not a blanket exemption. On the contrary, the proposed amendment is a recognition USM institutions have a need for flexibility that works for students, researchers, faculty, and staff.

Thank you for allowing the USM to propose this important clarifying amendment to Senate Bill 757.

USM Office of Government Relations – Susan Lawrence: slawrence@usmd.edu

TikTok - Protecting National Security Interests.pd

Uploaded by: Kiley Smith

Position: UNF

Protecting U.S. National Security Interests

TikTok recognizes our heritage has raised questions about whether TikTok poses a national security threat. In response to these concerns, we launched an initiative - undertaken voluntarily and wholly at TikTok's expense - to build a secure environment for protected U.S. user data*, to ensure the platform remains free from outside influence, and to implement additional safeguards on our content recommendation and moderation tools. We take national security very seriously, and our work to address related concerns remains thorough and ongoing. Here's the progress we've made:

U.S. Data Security

In May 2022, TikTok created a new organization called TikTok U.S. Data Security (TikTok USDS). This special purpose subsidiary is staffed by U.S.-based employees (with some exceptions in the U.K. and Australia to provide global coverage). USDS controls access to protected U.S. user data, content recommendation, and moderation systems in the secure Oracle Cloud. This structure brings heightened focus and governance to our data protection policies and content assurance protocols to keep U.S. users and their data safe. Teams within USDS are dedicated to delivering on our commitments, and span functions such as Engineering, User Operations, Privacy, Security Operations, Trust and Safety, Legal, Finance, and more. Many of the organization's leaders have U.S. national security experience.

Software Assurance: Preventing Backdoors and Content Manipulation

All source code entering the secure environment will be inspected by Oracle. If the source code has not gone through the review process, it will not run in this environment.

All TikTok app code will go through Oracle's review process (including technology or human review). Oracle will compile the app, and deploy it to the app stores, maintaining chain of custody for assurance. The code that powers TikTok's recommendations - the For You feed - will be inspected, reviewed, and validated by third parties.

Content moderation processes, both human and machine, will be vetted, reviewed, and tested to ensure that moderation is based only on our published Community Guidelines. All videos removed will be subject to audit.

A Secure Environment for the U.S. App

New protected U.S. user data is stored by default in the Oracle Cloud and USDS infrastructures with controlled and monitored gateways. Once deletion of backup data is complete (a process currently underway), only approved USDS personnel will have access to protected U.S. user data in the Oracle cloud. All business functions that require access to protected U.S. user data will be part of USDS.

There will be limited situations where protected U.S. user data can leave the secure environment to maintain a globally interoperable platform. For example:

- A U.S. TikTok user might want to send a message to a non-U.S. TikTok user, requiring the content of the message to leave the Oracle Cloud Infrastructure to reach its intended recipient.
- A U.S. creator wanting to share their content globally would need their public content - their videos and their public profile information - to leave the Oracle Cloud Infrastructure.

There are some limited exceptions where non-USDS employees may be granted access to protected data, for example, for legal and compliance, but such access must be expressly authorized by USDS pursuant to a robust data access protocol.

(Effective Jan. 2024)

Timeline

March 2021 — Project work begins.

May 2022 — USDS department formalized.

June 2022 — 100% of new, protected U.S. user data routed to Oracle Cloud Infrastructure and USDS controlled infrastructure with traffic temporarily backed-up/ synced to global TikTok servers in Virginia and Singapore.

October 2022 — Stopped synchronizing/ backing-up the data between Oracle systems and the servers in Virginia and Singapore.

January 2023 — Access to TikTok Oracle Cloud Infrastructure can only be accessed by USDS personnel.

January 2023 — First Dedicated Transparency Center opens in Maryland for source code inspection by Oracle.

July 2023 — Oracle begins reviewing entire TikTok app source code.

Transparency, Oversight, and Accountability

This initiative is the framework we developed with the U.S. Government (the Committee on Foreign Investment - or CFIUS - in the U.S.) to allow it to verify that U.S. data on TikTok is secure. Since 2021, we have been working to reach a national security agreement that would legally require TikTok to implement this initiative, but we're already doing that voluntarily.

Under a signed agreement with the U.S. Government, we would take additional steps to provide even more transparency, oversight, and accountability of this program, including:

- TikTok USDS would be governed by an independent board made up of CFIUS-vetted and approved directors, each with significant national security experience;
- USDS key management personnel will be vetted by CFIUS; they will report up to the USDS board, with no reporting lines to TikTok or ByteDance leadership; and
- Employees of USDS will be vetted and hired in accordance with requirements—including restrictions on citizenship and country of origin—put forth by CFIUS.

If an agreement with the US Government is fully implemented, we'll be the only platform whose controls and defenses are regularly vetted, tested, and scrutinized by U.S. national security agencies and their trusted partners, like Oracle. This structure will make us far more secure than other companies in the industry that collect extensive data on U.S. users.

Our Corporate Structure

TikTok's parent company, ByteDance, was founded by Chinese entrepreneurs. It isn't owned or controlled by the Chinese government or any other state entity. ByteDance is a private, global company, nearly 60 percent of which is owned by global institutional investors such as General Atlantic and Susquehanna International Group, with the rest owned primarily by the company's founders and its employees - including thousands of Americans.

The TikTok platform may be global, but we take a local approach to regulatory compliance, working with stakeholders to ensure that we understand local concerns and meet our regulatory commitments.

*How we define protected data:

Protected data broadly means personal information collected from a U.S.-based user of TikTok. Subject to exceptions, protected data include the following categories of data, even if deidentified, anonymized, or aggregated: user data, such as email and birthdate; non-public user content, such as private videos and direct messages; behavioral data, such as user interaction with content including likes and favorites; data inputs to TikTok's recommendation engine, such as video completion and video viewing time; and device and network data, such as IP address and device model.

(Effective Jan. 2024)

TikTok - Trust & Safety.pdf
Uploaded by: Kiley Smith
Position: UNF

TikTok

Trust & Safety on TikTok: By The Numbers

TikTok is an entertaining and joyful place because we prioritize safety.

How we keep TikTok safe

30 policies in our Community Guidelines

40k trust and safety professionals

70+ languages supported for moderation

How we empower our community

15+ youth safety and well-being tools

10+ LIVE safety tools

12+ safety and well-being guides

Enforcing our rules: video and account removals in Q1 2023

91M violative videos

17M accounts suspected to be under the age of 13

51M fake accounts

How we removed

97% removed before they were reported to us

90% removed within 24 hours

92% of community-reported content removed within two hours

TikTok WAPO Article.pdf
Uploaded by: Kiley Smith
Position: UNF

The Washington Post
Democracy Dies in Darkness

Congress had a lot to say about TikTok. Much of it was wrong.

'Nyquil chicken' and the 'blackout challenge' were both phenomena before TikTok even existed

By Taylor Lorenz

March 28, 2023 at 6:00 a.m. EDT

LOS ANGELES — On Thursday, Republican Rep. Earl L. "Buddy" Carter of Georgia lambasted TikTok CEO Shou Chew for alleged viral challenges he attributed to TikTok.

With a board behind him featuring so-called "sleepy chicken" (chicken sautéed in NyQuil), he claimed that the Chinese Communist Party was engaging in "psychological warfare through TikTok to deliberately influence U.S. children" specifically through TikTok challenges.

"We've heard from parents who are with us who have lost children," he said. "Why is it that TikTok consistently fails to identify and moderate these kinds of harmful videos, why is it that you allow it to go on?"

When Chew tried to respond, Carter cut him off. "This is TikTok, we're talking about, TikTok. Tell me why this goes on." It was a dramatic and heart wrenching moment. It was also untrue.

NyQuil chicken was never a "TikTok challenge." The idea originated on the fringe website 4chan in 2017 — a year before TikTok launched in the United States. Known as "sleepy chicken," the alleged recipe has been an internet meme for years. It spread in viral posts on Reddit, image boards and humor websites years ago. Images and video of chicken being cooked in NyQuil can also be found on YouTube and Instagram.

"if she makes you nyquil chicken ... do NOT let her go," read one viral tweet from 2017 that received nearly 10,000 shares. That was a year before TikTok was available in the United States.

On Monday, Carter's office declined to say where the congressman had gotten the information or discuss last Thursday's hearing.

Also declining to discuss assertions he'd made during the hearing was the office of Rep. Robert E. Latta (R-Ohio) who attributed the death of a 10-year-old girl to the "blackout challenge," which he accused TikTok of promoting.

But the "blackout challenge," also called the "choking game," isn't a recent phenomenon. In 2008, the Centers for Disease Control and Prevention reported that 82 children in the United States had died playing the choking game between 1995 and 2007. TikTok wasn't founded until 2016 and didn't launch in the United States until 2018.

It was not the first use of inaccurate information to slam TikTok. Last year, The Washington Post reported that Meta, Facebook's parent company, had hired a consulting firm to malign the app in local news media across the country. The firm, Targeted Victory, successfully planted op-eds in regional news outlets falsely tying TikTok to viral challenges that, in some cases, originated on Facebook. In one case, Targeted Victory worked to spread rumors of a "Slap a Teacher' TikTok challenge" in local news. But, no such challenge existed on TikTok. The rumor may have started on Facebook.

There was no evidence that Targeted Victory played a role in Thursday's hearing, and legislators asked to comment Monday on how they'd come by the information they cited — none acknowledged being a TikTok user — declined to comment.

A spokeswoman for the House Energy and Commerce Committee chair, Rep. Cathy McMorris Rodgers (R-Wash.), declined to comment.

"Legislators using misinformation to back up their policies is not particularly new," said Abbie Richards, a disinformation researcher at Accelerationism Research Consortium, a nonprofit studying the threat of far-right extremism to democratic societies. "We're certainly seeing that when it comes to LGBTQ legislation that's being implemented. They're finding misinformation that backs up their points to justify their view that we should ban TikTok."

Lawmakers made a number of other claims that were inaccurate or at least debatable.

When Chew denied that TikTok censors videos related to the Uyghur genocide or the Tiananmen Square massacre, McMorris Rodgers warned him that, "Making false or misleading statements to Congress is a federal crime." But a simple search on the app reveals dozens of videos bashing China and calling attention to the Uyghur genocide and the Tiananmen Square massacre.

Frustrated by that line of questioning, some TikTok users last week began uploading graphic content of the Tiananmen Square massacre to show that it would not be removed. "Oddly enough I tried posting this on Facebook and got a 24 hour ban," one TikTok user commented in a TikTok video showing footage from the Tiananmen Square massacre that had been viewed more than 132,500 times.

Jackson said he believes it's on Apple to better police this sort of access and help consumers understand what data they're giving and why. "Apple could do a better job communicating the risk and making sure developers justify the use of these APIs to Apple," he said. "It should be part of the Apple review process."

"TikTok follows industry norms, and like other apps, may ask permission to discover and connect to devices on the networks people use," a company spokesperson said. "We do not sell personal information, and people can choose to allow or revoke permission at any time."

Fighting misinformation about TikTok is especially difficult, said Richards, the Accelerationism Research Consortium researcher, because the false information often goes viral and plays into people's preexisting beliefs. "It's one of those classic debunking struggles," she said, "It doesn't matter how much you debunk it because the lie has spread so much farther than the truth ever will."

For instance, in 2020, a viral tweet accused TikTok of blocking the #BlackLivesMatter hashtag. While a temporary glitch hid view counts for all hashtags on the app for a number of hours one day in 2020, the app did not block the Black Lives Matter hashtag, or cease counting views on the hashtag. In fact, the company promoted the #BlackLivesMatter hashtag repeatedly within the app throughout the summer of 2020, and videos containing the hashtag received tens of millions of views. A Post poll of TikTok users found its user base is largely young and people of color.

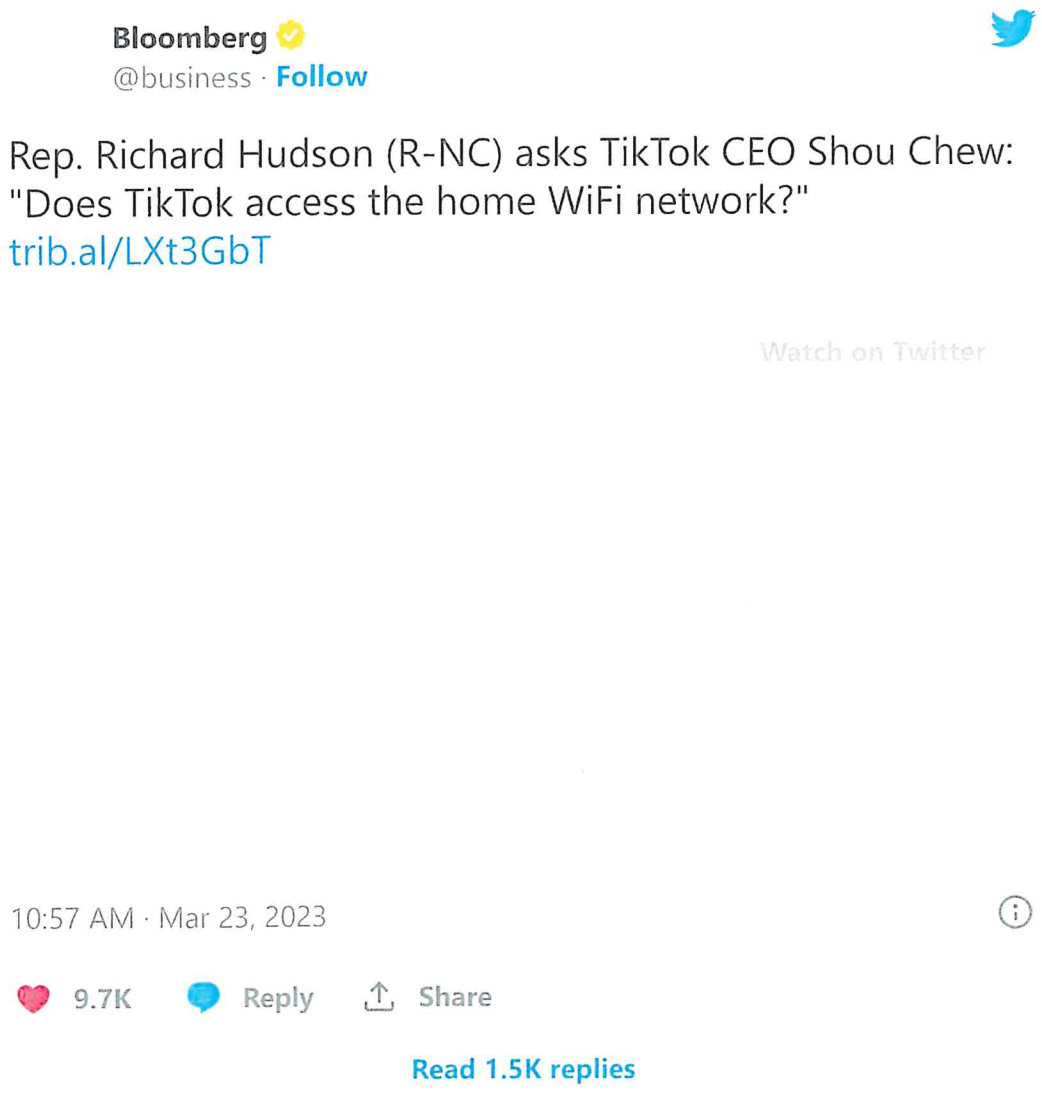
Jamie Cohen, an assistant professor of media studies at CUNY Queens College, said that the lawmakers displayed "willful ignorance of internet culture." However, he added that the media also should take some responsibility for perpetuating the false information repeated at the hearing.

"Much like the way young people know how to game algorithms on social media, news media knows how to create panic to get viewership and ratings," he said. "There would be no sleepy chicken behind a congressperson if the news media didn't perpetuate the notion that it exists. It doesn't exist, but it creates a fear factor."

Amin Shaykho, founder of Kadama, a tutoring app for students that is promoted widely on TikTok, said he was disappointed that no member of the committee seemed interested in the potential negative impact of a ban. "I felt so bad that no member spoke up," he said. "I'm going to have to lay off 5,000 of our tutors if TikTok gets banned, and millions of other businesses will also be impacted. Between 80 to 90 percent of our users discover us on TikTok."

TikTok also denied lawmakers' assertions that the CEO of TikTok's parent company, ByteDance, is a member of the Chinese Communist Party. He is not, the company said.

Other questioning drew TikTokers to rally to the company's defense. Several mocked Rep. Richard Hudson (R-N.C.) after he asked, "Does TikTok access the home WiFi network?"



But Patrick Jackson, chief technology officer at Disconnect, a data privacy company, said the question might have had a basis in fact. While it's hard to know exactly what Hudson was trying to ask (his office declined to comment), Jackson said he believes the congressman was attempting to question TikTok's CEO about a setting in Apple's iOS system where users are prompted to give apps permission to access other devices on their WiFi network.

"Most times it's harmless," Jackson said, "maybe it's a video app that wants to cast to your Chromecast, or send audio to your Sonos. By default, apps can only communicate to the internet, not to your local network."

Apps can exploit that access, however, if a user grants it. For instance, giving an app access to a printer may allow it to print a document without asking the user. And data about what other devices a user has on their WiFi network is valuable. Other apps such as Instagram and Signal also prompt the user to connect to their local network.

TikTok_Myth vs. Fact(1).pdf
Uploaded by: Kiley Smith
Position: UNF

TikTok Myth vs. Fact

Myth **TikTok's parent company, ByteDance Ltd., is Chinese owned.**

Fact TikTok's parent company ByteDance Ltd. was founded by Chinese entrepreneurs, but today, roughly sixty percent of the company is beneficially owned by global institutional investors such as Carlyle Group, General Atlantic, and Susquehanna International Group. An additional twenty percent of the company is owned by ByteDance employees around the world, including nearly seven thousand Americans. The remaining twenty percent is owned by the company's founder, who is a private individual and is not part of any state or government entity.

Myth **TikTok and ByteDance are headquartered in China.**

Fact TikTok, which is not available in mainland China, has established Los Angeles and Singapore as headquarters locations to meet its business needs. That is in keeping with ByteDance's approach to aligning business needs to the markets where its services operate. ByteDance does not have a single global headquarters.

Myth **There is a member of the Chinese government on ByteDance's board of directors.**

Fact This is not accurate. ByteDance's board of directors is comprised of five individuals, none of whom is a part of any government or state entity. 3 of the 5 are American. The board includes:

- Rubo Liang, ByteDance Chairman and CEO (Singapore-based)
- Arthur Dantchik, Susquehanna International Group (U.S.-based)
- Bill Ford, General Atlantic (U.S.-based)
- Philippe Laffont, Coatue Management (U.S.-based)
- Neil Shen, Sequoia (Hong Kong-based)

Four out of five of the board's directors represent ByteDance's investors on the board, and Rubo Liang, ByteDance CEO, represents the company and its employees.

Myth **The Chinese government has a "golden share" interest in ByteDance Ltd.**

Fact As is required under Chinese law, in order to operate certain news and information products that are offered exclusively in China, media licenses are required for those services. As such, an entity affiliated with the Chinese government owns 1% of a ByteDance subsidiary, Douyin Information Service Co., Ltd. This is a common arrangement for companies operating news and information platforms in China. This arrangement is specific to services in the Chinese market, and has no bearing on ByteDance's global operations outside of China, including TikTok, which does not operate in mainland China.

Myth vs. Fact

Myth **Employees of a ByteDance subsidiary in which the Chinese government owns a small stake can access Americans' user data.**

Fact As described above, Douyin Information Service Co., Ltd. operates only in mainland China, where TikTok is not available. Employees of that entity are restricted from access to U.S. user databases, with no exceptions. These databases are scanned daily and monitored for access to every data field.

Myth **Decisions about TikTok are made in Beijing.**

Fact This is not true. TikTok's CEO Shou Chew is a third-generation Singaporean who is based in Singapore; Mr. Chew oversees all key day-to-day and strategic decision making when it comes to TikTok. TikTok's senior leadership team is based in Singapore, the United States, and Ireland.

As would be expected with any subsidiary of a holding company, high level decisions around financial matters and corporate governance are made in concert with the ByteDance board and CEO. None of those individuals reside in mainland China. Three out five members of that board are Americans, and four out of five of them represent the interests of ByteDance's global investors. The fifth member of the board is the ByteDance CEO, who resides in Singapore.

Myth **TikTok manipulates content in a way that benefits the Chinese government or harms American interests.**

Fact TikTok is an entertainment app. The content on TikTok is generated by our community. TikTok does not permit any government to influence or change its recommendation model.

Myth **ByteDance censors TikTok content on behalf of the CCP or Chinese government.**

Fact There are no TikTok content moderators in China. Content moderation on TikTok is overseen by our U.S. and Ireland-led Trust and Safety team. All content is moderated based only on our publicly available Community Guidelines, which are also developed by our Trust and Safety team. Regardless of how content is flagged to TikTok—via formal or informal government request, by our automated systems at time of upload, or from community reports—no content is removed without going through our established moderation processes. TikTok does not remove content on behalf of any government except in compliance with legal process for content that violates local law. TikTok does not operate in mainland China.

Myth vs. Fact

Myth **Under its 2017 National Intelligence law, the Chinese government can compel ByteDance to share American TikTok user data.**

Fact TikTok Inc., which offers the TikTok app in the United States, is incorporated in California and Delaware, and is subject to U.S. laws and regulations governing privacy and data security. Under Project Texas, all protected U.S. data will be stored exclusively in the U.S. and under the control of the U.S.-led security team. This eliminates the concern that some have shared that TikTok U.S. user data could be subject to Chinese law.

Myth **TikTok stores U.S. user data in China, where multiple Chinese nationals, including possible members of the CCP, have access to it.**

Fact As of June 2022, 100% of U.S. traffic is routed to Oracle and USDS infrastructure in the United States, and today all access to that environment is managed exclusively by TikTok U.S. Data Security, a team led by Americans, in America. We have begun the process of deleting historic protected user data in non-Oracle servers; once that process is complete, it will effectively end all access to protected U.S. user data outside of TikTok USDS except under limited circumstances.

Myth **TikTok gathers as much data as possible, and the company takes a lax approach to the security of that data.**

Fact TikTok has been adopting a privacy and security-by-design approach when it comes to product roll-outs and the security of user data. When it comes to user data, we limit the types of data we collect, and we believe that we collect less data than our competitors. We disclose the data that we do collect, how we use it and with whom, and our privacy policies are regularly updated.

Today, in the United States, access to new protected U.S. user data is managed exclusively by TikTok U.S. Data Security, a team led by Americans, in America. Since October of 2022, all new protected U.S. user data has been stored in the secure Oracle infrastructure, not on TikTok or ByteDance servers. Access to that data is controlled by TikTok USDS. We have begun the process of setting up controlled gateways for all data coming into the environment and all data going out. These gateways are currently controlled by USDS, and they will soon be controlled by Oracle.

Myth vs. Fact

Myth **TikTok collects a significant amount of sensitive data on its users.**

Fact TikTok's privacy policy fully describes the data the company collects. There have been many inaccurate claims about our policies and practices that have gone unaddressed by the media. To be clear, the current versions of the TikTok app do NOT:

- Monitor keystrokes or content of what people type when they use our in-app browser on third party websites;
- Collect precise or approximate GPS location in the U.S.;
- Use face or voice prints to identify individuals.

In line with industry practices and as explained in our privacy policy, we collect information to help the app function, operate securely, and improve the user experience. We constantly update our app and encourage users to download the most current version of TikTok.

Myth **Douyin offers educational content, limits screen time, and creates a positive experience for teens, while TikTok does not.**

Fact Douyin and TikTok are separate apps that are run by separate teams and serve separate markets. Some reports have compared the Douyin experience for users under age 14 to the over 18 experience on TikTok. This is not a reasonable comparison; when compared to the TikTok experience for people under 13, TikTok has higher levels of moderation and curation to ensure a safe and appropriate experience. We've partnered with Common Sense, a third-party expert in assessing age-appropriate content, to moderate and curate content for that experience. TikTok users 17 and younger now have a default screen time limit of 60 minutes. TikTok also provides Family Pairing, a suite of tools families can use to help limit content and screen time in a way that makes sense for them.

Myth **TikTok takes a lax approach to minor safety & privacy in order to addict teens to its platform.**

Fact TikTok has taken numerous steps to help ensure that teens under 18 have a safe and enjoyable experience on the app, and many of these measures impose restrictions that don't exist on comparable platforms. Accounts registered to teens under 16 are set to private by default and are prevented from sending direct messages; content made by our users under 16 is ineligible for recommendation into the For You feed to further protect privacy and help ensure safety. We also prevent teens from receiving late-night push notifications and give parents and guardians the ability to create further restrictions on these notifications through Family Pairing.

Myth vs. Fact

Myth **TikTok is a go-to platform to buy illegal drugs.**

Fact TikTok has a zero tolerance policy for the sale, trade, promotion, use and the depiction of drugs, including controlled substances, for both organic and paid content. Apart from obvious satire, our policies governing content that depicts drugs do not have exceptions because of the harm and normalization that can follow.

On many platforms, direct messaging is the mechanism that is often used to sell drugs, and recruit for or promote criminal activities. However, unlike on other platforms, accounts on TikTok for users under age 16 do not have access to our direct messaging service.

Myth **ByteDance used TikTok data to surveil journalists and their precise locations.**

Fact A small group of ByteDance employees misused their access to TikTok user data in an effort to identify employees who leaked confidential company information to journalists. The aim of those employees, all within the internal audit department, was to investigate whether other employees leaked confidential company information to reporters, and if so, to identify those employees. As part of that investigation, they engaged in a misguided effort to determine whether suspected employees had previously been in the same approximate location as the reporters believed to have received the leaked information. TikTok and ByteDance condemned this effort in the strongest possible terms. As a result, three employees have been terminated, and one employee has resigned. However, to characterize it as an effort to spy on or surveil journalists is inaccurate.