HB1141_USM_SENATE EEE.pdf

Education, Energy, and the Environment Committee
House Bill 1141
State Information Technology - Prohibited Applications and Websites
March 30, 2023
Favorable with Amendment

Chair Feldman, Vice Chair Kagan and committee members, thank you for the opportunity to share our position on House Bill 1141. The bill bans all products by ByteDance Ltd. and TenCent Holdings Ltd. from all state-owned information technology, including all devices and networks.

While the University System of Maryland (USM) understands the importance of protecting information and technological systems from foreign government hacking and monitoring, 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 complete ban of all products by ByteDance Ltd. and TenCent Holdings Ltd. does not allow the necessary flexibility to refine security and privacy measures to the needs of unique university communities.

Scope of the Bill

The bill requires the ban of all applications and websites developed by ByteDance Ltd. and TenCent Holdings Ltd. on all state owned or leased "information technology" (as defined in the State Finance and Procurement Article, Section 3.5-301 of the Maryland Code). Section 3.5-301 of the Maryland Code defines Information Technology as:

"Information technology" means all electronic information processing, including:

(1) maintenance;
(2) telecommunications;
(3) hardware;
(4) software; and
(5) associated services.

This would essentially require that USM institutions block any application and/or website by ByteDance or TenCent Holdings from all information technology and networks owned, operated, or leased by an institution or its agents. This also requires a ban on all applications and/or websites from the statewide education and research networks that the USM operates for groups across the state. By requiring the ban on statewide education and research networks, the effect of the ban will go far beyond the original public sector scope and impact private institutions as well as any other organization that partners with Maryland's research and education networks. This could have a harmful effect on interinstitutional collaboration on our statewide education networks. Lastly, it would impact the use of applications and websites by ByteDance and TenCent Holdings on personal devices that connect to an institutional or state network. That would impact on the experience of all students and guests of our institutions in addition to employees.

Impact of a Total Ban on USM Institutions

USM institutions and the communities we serve would be significantly impacted from an academic, operational and financial perspective by a total ban on applications and websites operated by ByteDance Ltd. and TenCent Holdings Ltd.

Educational Impacts

Within USM institutions, gaming platforms are at the heart of many video game design and data visualization classes. Video Game design classes rely on the ability to research and play games that are on the market. Students also use development tools provided by video game companies to develop new games. In particular, Unreal Engine, by Epic Games, is used across many USM video game programs and activities. Unreal Engine is an incredible tool for developing games, as well as non-game interactive and VR applications; and with source code, students can learn how game design engines work from the inside. Beyond video game classes, data visualization instruction also uses game-based data visualization tools to teach data analysis. Classes across the institutions also use voice and instant messaging tools such as Discord for formal class discussion and informal student to student discussions. Taking away these tools would harm video game and data visualization classes and take away a popular tool for class and student discussion.

Research Impacts

House Bill 1141 will impact research in several areas of the USM. While the bill allows for security research, it would block all other types of research. For example, UMBC uses the Unreal Engine, by Epic Games, for data visualization research. Unreal Engine is the only large-scale commercial-quality game engine available with full programming source code. The Unreal Engine is the underlying framework for the UMBC Imaging Research Center's three plus year research project to build visualization solutions for clients such as the City of

Baltimore and US Military Intelligence. Banning applications and websites from ByteDance and TenCent Holdings would have a catastrophic impact on these data science / visualization research programs.

A total ban on TikTok would also block research such as:

- Dancing to the #challenge: The Effect of TikTok on Closing the Artist Gender Gap

  Yifei Wang, Associate Professor Jui Ramaprasad and co-author Anandasivam Gopal – Robert H. Smith School of Business
  https://today.umd.edu/could-the-next-viral-dance-challenge-help-narrow-musics-gender-gap

- Pitfalls of the TikTok Resume Trend

  Associate Professor Cynthia Kay Stevens – Robert H. Smith School of Business
  https://www.rhsmith.umd.edu/research/pitfalls-tiktok-resume-trend

- There's a long history of dances being pilfered for profit – and TikTok is the latest battleground

  Jill Vasbinder, Senior Lecturer in Dance https://umbc.edu/stories/theres-a-long-history-of-dances-being-pilfered-for-profit-and-tiktok-is-the-latest-battleground/

Marketing Impacts

A total ban of TikTok would have dramatic impacts on marketing across the USM. Many university admissions departments use TikTok to advertise programs to high school students. Institutions also use TikTok to reach our current students and alumni, promote events, solicit donations, and announce accomplishments. Lastly, our athletics programs utilize TikTok heavily to draw attention to our athletic teams, advertise upcoming games, and attract new athletes. A ban of TikTok would impact the USM's ability to engage with its community around the globe and grow its programs.

Entertainment Impact

The gaming impact on university communities would be tremendous. TenCent Holdings is one of the largest gaming conglomerates in the world. As shown above, they own part or all of nearly fifty different gaming companies, including many of the biggest titles in gaming and four of the five major e-sports environments. The University of Maryland, College Park has over 1500 students enrolled in intermural e-sports as well as intercollegiate esports

competition teams. All other USM institutions also have students participating in gaming and e-sports activities. In addition to student entertainment, many students use video games as a stress relief tool and mental health aid. Cutting off students from the game networks they have paid to participate in and are passionate about will have a dramatic impact on our communities.

Family / Social Impacts

Many members of the USM community rely on ByteDance and TenCent products for daily activities. A significant number of our Asian community members use WeChat to stay in contact with family in the US and abroad. E-commerce and financial services, offered by these companies, are also used for daily activities. A ban on the products of these two companies would result in cutting off many of the tools that our Asian community members use for daily life and contact with their families.

Discord is also broadly used by our students as a daily communication tool. Many student organizations use Discord to pass messages and communicate about campus events. Discord is heavily used for communication while playing video games and is the way that many students stay in daily contact with their friends around the globe. Cutting off Discord would significantly impact a tool that our students rely on to stay connected to their friends and peers.

Technical / Labor / Financial Impact

Trying to implement a total ban across all state-owned devices and networks would also be very challenging from technical, financial, and labor perspectives. We do not currently have technical capabilities in place across all our infrastructure to block all the apps related to ByteDance Ltd. and TenCent Holdings Ltd. Purchasing the hardware and software to implement such filtering would easily pass $1 million. These two companies also offer over 200 different products through the companies listed above. Even if we had the money and technology to implement the filtering, it would be very time consuming and technically challenging to implement filtering for every individual program and service. These two companies are also buying and developing new companies and solutions on a regular basis, so ongoing effort would need to be spent to maintain the blocks.

Conclusion

In the end, House Bill 1141, as written, will have a dramatic impact on many facets of recruitment, marketing, research, education, and the daily lives of our students and other community members. It would also be extremely expensive and technically difficult to implement. The USM acknowledges the risk to security and privacy that ByteDance Ltd. and

TenCent Holdings Ltd. pose to our communities and have plans in place to manage the risks in balance with the needs and resources of our communities.

The USM respectfully requests an exemption from the proposed prohibitions detailed in House Bill 1141. The USM seeks solely to retain the flexibility to block the use of applications and websites by ByteDance Ltd. and TenCent Holdings Ltd. on critical infrastructure while still allowing the use of these applications and websites in low-risk areas of our institutions.

The Scope of ByteDance Ltd. and TenCent Holdings Ltd.

ByteDance and TenCent Holdings are conglomerates of companies that operate a vast array of applications and websites. Beyond TikTok and WeChat, the following are examples of the websites and applications operated by companies associated with ByteDance and TenCent Holdings:

ByteDance Ltd.	TenCent Holdings Ltd.
CapCut – Video Editing Software **Douyin** – Chinese Version of TikTok **Lark** – Enterprise Collaboration Tool **TikTok** – Video Social Media Network **Toutaio** – News Aggregation tool **Xigua Video** – Short and Mid Length Video / TV Content **Nuverse** – Video Game Company - Warhammer 40,000: Lost Crusade in 2021 - Marvel Snap **Gogokid** – English Language Training Tool **Moonton** - Mobile eSports game - Magic Rush: Heroes - Mobile Legends: Bang Bang - Mobile Legends: Adventure - Mobile Legends: Pocket - Sweet Crossing: Snake.io **Party Island** – Social Media App **Resso** – Social Music Streaming App - Music by Warner Music Group, Sony Music Entertainment, Merlin and Beggars Group, and others.	Social Media **TenCent QQ** – Chinese Instant Messaging **TenCent QZone** – Social Network / Blogging **Tencent Weibo** – Microblogging Service **WeChat** – Mobile Voice and Text Messaging **Discord** – VoIP and Instant Messaging Platform (Partial Ownership) Game Companies (100% Ownership by TenCent Holdings) **Epic Games** **Leyou** (Athlon Games, Digital Extremes, Splash Damage) **Riot Games** **Sharkmob** **Sumo Group** **Turtle Rock Studios** **Wake Up Interactive** (Soleil, Valhalla Game Studios) **Inflexion Games** **Fulqrum Games** **Game Companies (Partial Ownership of TenCent Holdings)** - TenCent Holdings has a partial ownership in over thirty-seven video game companies including major companies such as: **Supercell** **Epic Games** (including the Unreal Engine) **Ubisoft** **Roblox Corporation** **Television, Streaming, and Comics**

	• **TenCent Video** – Video / TV Online Streaming • **TenCent Comics** – Comic Books Online Steaming • **Iflix** – Malaysian Streaming Service • **Huya Live, DouYu, Kuaishou and Bilibili** – Live Game Video Streaming **Music** • **QQ Music and JOOX** – Social Music Streaming App • **TenCent Music** • **Spotify** (Collaborative / 10% Stake) **E-Commerce** • **JD.com** – Payment System Similar to Paypal • **PaiPai Second Hand** – Similar to EBay **Healthcare and Insurance** • **WeChat Intelligent Healthcare** • **Tencent Doctorwork** • **AI Medical Innovation System (AIMIS)** **Other** • **Sogou** – Internet Search Engine • **QQ Haiwai** – Real Estate Listing Service • **TenCent Credit** – Credit Scoring Service

About the University System of Maryland

The University System of Maryland (USM)—one system made up of twelve institutions, three regional centers, and a central office—awards eight out of every ten bachelor's degrees in the State of Maryland. The USM is governed by a Board of Regents, comprised of twenty-one members from diverse professional and personal backgrounds. The chancellor, Dr. Jay Perman, oversees and manages the operations of USM. However, each constituent institution is run by its own president who has authority over that university. Each of USM's 12 institutions has a distinct and unique approach 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, with the flagship campus in the Washington suburbs. The USM includes Historically Black Colleges and Universities, comprehensive institutions, research universities, and the country's largest public online institution.

USM Office of Government Relations - Patrick Hogan: phogan@usmd.edu

TikTok Protecting US National Security Interests[1

Uploaded by: David Carroll

Position: UNF

Protecting U.S. National Security Interests

TikTok's Chinese heritage has raised concerns about whether TikTok poses a national security threat.
We've been working to address those concerns through an initiative called Project Texas.

🎵 TikTok

What is Project Texas?

- Project Texas is an initiative to make every American on TikTok feel safe, with confidence that their data is secure and the platform is free from outside influence.

- We've been implementing Project Texas to remove doubts about potential external or foreign influence, create a secure enclave to protect U.S. user data, and put additional safeguards on our content recommendation and moderation tools.

What is USDS?

- TikTok U.S. Data Security ("USDS") is tasked with managing all functions and elements of the TikTok platform related to U.S. data and content.

- This structure brings heightened focus and governance to our data protection policies and content assurance protocols to keep U.S. users safe.

- Teams within USDS are dedicated to delivering on our commitments, and span functions like Safety, Legal, Engineering, Finance, HR, User Ops, Security Compliance, and more.

March 2021	May 2022	June/July 2022	August 2022	October 2022	December 2022	January 2023
Project Texas Kick-off	USDS department formalized	100% of new user traffic routed to Oracle and stored there exclusively	Oracle begins reviewing the TikTok app source code	Access to TikTok Oracle Cloud Environment cut off from non-USDS personnel	USDS Trust & Safety team established to oversee U.S. content moderation	First Dedicated Transparency Center opens in Maryland for source code inspection

Did you know?

- ByteDance is a private, global company. Nearly 60% is owned by global institutional investors, 20% is owned by the company's founders, and 20% is owned by 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.

Did you know?

- TikTok does not log keystrokes

- TikTok does not collect precise location in the U.S.

- TikTok does not track your search and browsing behavior across the internet

- TikTok does not build a "shadow profile" on our users to serve ads

- TikTok does not use face or voice prints to identify individuals

Components of Project Texas

TikTok

Organizational Design – Protecting Against Outside Influence

- TikTok U.S. Data Security is a special purpose subsidiary that oversees all elements of the U.S. TikTok platform related to data and content.
- TikTok USDS will be governed by an independent board made up of U.S. Government vetted and approved directors, each with significant national security experience.
- The USDS board will report directly to CFIUS, with no reporting lines to TikTok or ByteDance leadership.
- USDS officers will be vetted and approved by CFIUS; they will report to the USDS board, with no reporting lines to TikTok or ByteDance leadership.
- Employees of USDS will be vetted and hired in accordance with requirements—including restrictions on country of origin—put forth by CFIUS. They will have no reporting lines to TikTok or ByteDance leadership.

Technology Assurance – Preventing Backdoors and Content Manipulation

- All software and code entering the secure enclave through protected gateways will be inspected by Oracle and a third party source code inspector. Code that has not been inspected and approved cannot operate in the environment.
- Oracle will review and approve all TikTok app code, compile the app, and deploy it to the app stores, maintaining chain of custody for assurance.
- The U.S. TikTok app validated and compiled by Oracle will only be able to communicate with code in the Oracle environment that has also been inspected and approved by Oracle and a third party code inspector.
- The code that powers TikTok's recommendations—the For You Feed—will be inspected and tested to ensure that it recommends content solely on content-neutral user behavior and established and auditable promotion and filtering decisions, such as featuring World Cup content or ensuring that multiple videos from the same creator don't run back-to-back.
- 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 Enclave for the U.S. App – Putting U.S. Data Out of Reach

- Today, all new U.S. user data is stored in the protected Oracle cloud environment with tightly controlled, rigorously monitored gateways.
- Only approved USDS personnel has access to U.S. user data in the Oracle cloud.
- All business functions requiring access to U.S. user data will be housed in USDS.
- There will be limited situations—vetted and agreed to by the U.S. Government—where 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 environment 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 environment.

Compliance Monitoring and Oversight – Holding Us Accountable

- All elements of the TikTok app and backend code will be subject to multiple layers of outside oversight and monitoring, including source code inspection, overall compliance monitoring in USDS operations, content audits, and more.
- Every third party that is a part of this process will have reporting obligations directly to CFIUS.
- CFIUS will have discretion to do site inspections, request audits, and appoint additional monitors.
- Failure to adhere to the commitments in the agreement could result in additional mitigations or a total shutdown of the U.S. service.

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.

Trust & Safety at TikTok

♪ TikTok

TikTok is an entertaining and joyful place because of the work we put into keeping the platform safe.

How we keep TikTok safe

12 Community Guidelines

40^k 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

In 2022*

327 million videos removed for violating our Community Guidelines

96% were removed proactively before they were reported

93% were removed within 24 hours

90% were removed before they had a single view

180 million total accounts removed

60 million suspected under 13 accounts removed

*Jan–Sept 2022

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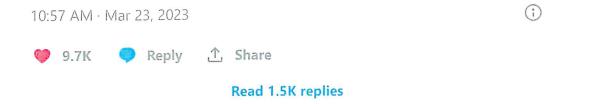
TikTok also denied lawmakers' assertions that the CEO of TikTok's parent company, ByteDance, is a member of the Chinese Communist Party. He is not, the company said.

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.