

Sécurité publique  
CanadaPublic Safety  
Canada

Sous-ministre

Deputy Minister

Ottawa, Canada  
K1A 0P8**SECRET/CEO**

DATE:

File No:

RDIMS No:

**MEMORANDUM FOR THE MINISTER OF PUBLIC SAFETY****PRIVACY AND NATIONAL SECURITY CONCERNS WITH TIKTOK**

(Information only)

**ISSUE**

Recent reporting has sparked renewed interest in privacy and national security concerns associated with TikTok, and reignited calls by some American lawmakers to ban the app. The Privy Council Office's Intelligence Assessment Secretariat (PCO-IAS) published a Current Intelligence Brief on TikTok on September 16, 2022 (**TAB A**).

**BACKGROUND**


TikTok is a Chinese video-sharing social networking service owned by ByteDance, a Beijing-based Internet technology company founded in 2012.

With over 1 billion monthly users across more than 150 countries, TikTok dominates our modern information environment. It gained widespread use during the pandemic, and is known to be "as addictive as Vegas slots" due to its personalized video feed.

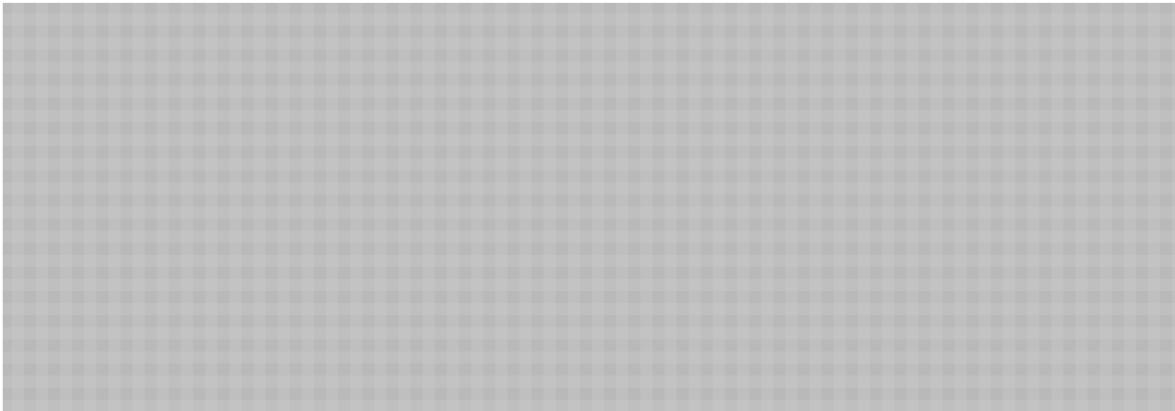
TikTok has come under scrutiny over the past few years due to privacy and security concerns. For example, in June, BuzzFeed reporting alleged that leaked audio from 80 internal TikTok meetings showed that U.S. user data had been accessed repeatedly from China. In October, Forbes reported that ByteDance planned to use the app to monitor the physical location of specific American citizens.

**CONSIDERATIONS**

*Canadian assessment*



**SECRET/CEO**

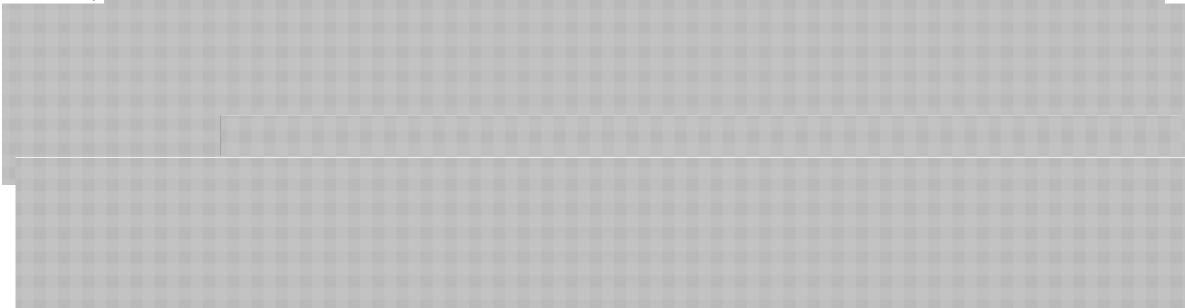


[REDACTED] As of 2022, there are over 8 million Canadian TikTok users, ranging from 55% of teenagers to members of Parliament. It harvests their data, offering false public and governmental reassurances about data sovereignty and security. [REDACTED]



*Investment Canada Act (ICA) Implications*

Through the purchase of a Canadian company, TikTok established an office in Toronto in 2019. [REDACTED]



*U.S. response*

On August 6, 2020, due to alleged privacy and national security concerns, former U.S. President Donald Trump announced through Executive Orders sweeping bans on U.S. transactions with China's ByteDance. These actions would have effectively required TikTok to shut down operations in the US as early as mid-September 2020.

In June 2021, President Biden replaced and revoked the orders, directing the Commerce Department to review apps tied to foreign adversaries. On June 24, 2022, U.S. Federal Communications Commissioner, Brendan Carr, wrote to the CEOs of Apple and Google requesting that their respective companies remove the application from their app stores. In the letter, Commissioner Carr states, "it is clear that TikTok poses an unacceptable national security risk due to its extensive data harvesting being combined with Beijing's

SECRET/CEO

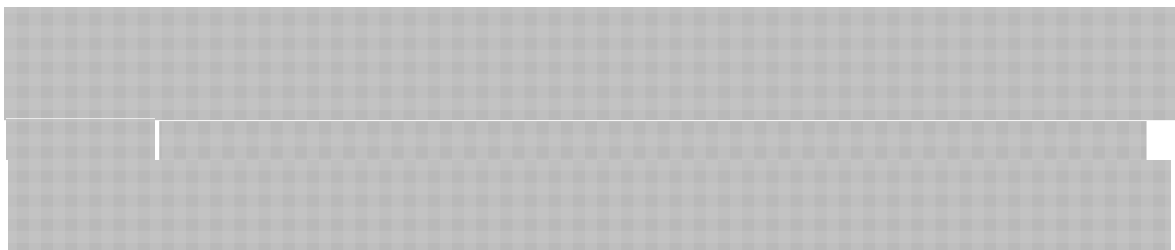
- 3 -

apparently unchecked access to that sensitive data.” More recently, the FCC commissioner was also quoted in an interview with Axios regarding TikTok that he does not “believe there is a path forward for anything other than a ban.”

In November 2022, FBI Director Chris Wray, appearing in front of American Lawmakers (House Homeland Security Committee), spoke to his organization’s national security concerns: “We do have national security concerns [...] about TikTok. They include the possibility that the Chinese government could use it to control data collection on millions of users or control the recommendation algorithm, which could be used for influence operations if they so choose, or to control software on millions of devices which gives the opportunity to potentially technically compromise personal devices.”

The Biden administration is reportedly considering an arrangement that would allow the app to continue operating in the U.S by, amongst other things, routing U.S. user traffic through servers maintained by Oracle Corp, which would also audit the app’s algorithms.




Opponents to this approach include Florida Republican Senator Marco Rubio, Wisconsin Republican House Representative Mike Gallagher, and Illinois Democrat House Representative Raja Krishnamoorthi. On December 13, 2022, these lawmakers introduced bipartisan legislation to ban TikTok from operating in the United States. The *Averting the National Threat of Internet Surveillance, Oppressive Censorship and Influence, and Algorithmic Learning by the Chinese Communist Party Act* would block and prohibit all transactions from any social media company in, or under the influence of, China, Russia, and several other foreign countries of concern. The Bill follows a series of state-level orders prohibiting TikTok on government devices—Utah and Texas banned the app from government-issued devices on December 12, 2022, on the heels of similar orders in South Dakota and Maryland. Open-source reporting in the U.S. deems the likelihood of the Bill’s passage to be low.



**SECRET/CEO**

- 4 -

**NEXT STEPS**

Public Safety, in partnership with partner departments and agencies,    


Should you require any additional information, please do not hesitate to contact me or Sébastien Aubertin-Giguère, Acting Senior Assistant Deputy Minister, National and Cyber Security Branch at 613-990-4976.

Shawn Tupper

Enclosures: (1)

Prepared by: NCSB-NCSD.



CURRENT INTELLIGENCE BRIEF

s.15(1) - Int'l

s.15(1) - Subv



ECONOMIC SECURITY AND TECHNOLOGY: TikTok Takeover

KEY TAKEAWAYS

- One billion people now use the social media platform TikTok. This viral growth is due to its personalized video feed, known to be "addictive as Vegas slots." Vulnerable users unwittingly expose their device and data to significant risks.
- TikTok dominates our modern information environment. It is diversifying beyond video, into search and music. TikTok's global reach makes it an appealing platform
- [Redacted]
- [Redacted]
- Despite assurances, there is growing evidence that TikTok's data is accessible
- [Redacted]

1. **Addictive Algorithm.** TikTok's competitive advantage is its artificial intelligence (AI)-enabled personal video feed. This individual recommendation engine is based on video likes and shares, comments, attentional response (how long you watch), and your device and account settings. With short videos, TikTok surpasses its peers at serving up viral content, holding user attention, and harvesting more data, which then further improves the customization and user experience (see image on next page). As per one cybersecurity analyst, "Every time you use the platform, the algorithm is updated with new data so it can understand you more precisely." As of August 2022, ByteDance now has to share this algorithm with the Chinese state.

Government-ordered mitigation is highly challenging and its long-term efficacy remains uncertain.

2. **Sensitive Data.** TikTok is the first Chinese-owned app to reach over a billion users beyond China, creating a globally-embedded and ubiquitous collection and influence

INFORMATION TIKTOK CAN COLLECT FROM ANDROID DEVICES

DATA COLLECTION BY THE TIKTOK APP

- **DEVICE MAPPING** TikTok gathers all apps installed on the phone, and retrieves all other running applications on the phone
- **LOCATION** TikTok checks device location once per hour
- **CALENDAR** Ongoing access
- **CONTACTS** If user denies access to contacts, TikTok asks again and again for access until given
- **EXTERNAL STORAGE** App requests external storage, standard with social media to store video, images, etc. However TikTok also retrieves a list of everything available in an external storage folder

DEVICE DATA TIKTOK CAN GAIN

- Wi-Fi SSID (Wi-Fi network name)
- Past configured Wi-Fi networks
- Device build serial number (unique number assigned by manufacturer to identify individual device)
- SIM serial number (unique identifier specific to SIM card)
- All accounts on device
- Active subscription information
- Integrated circuit card identification number (a global unique serial number that is tailored to your SIM card)
- Device ID (most likely advertising ID)
- Device IMEI (international mobile equipment identity - unique identifier of device)
- Device MAC address (media access control address) - unique identifier assigned to a network interface control
- Device phone number
- Device voicemail number
- GPS status information (updates on the GPS location)
- Complete clipboard access (password managers use clipboards)



Source: Internet 2.0

TECHNICAL ANALYSIS REVEALS...

**Your Data and Device, Exposed.** Third party technical analysis of TikTok software has revealed "dangerous" and commercially unnecessary device permissions and data access upon download (see image above). An Australian cybersecurity firm has concluded that most of TikTok's access and data collection is not required for the app to function, and only serves as a "data harvesting" tool. Further, Tiktok's location tracking, device mapping, external storage access, contacts and third-party applications data collection are also unnecessary and a cause for further concern. Separate technical analysis highlights that TikTok conceals its data collection, including where that user data actually goes. (U)

CIB 19/2022

platform for Beijing to exploit. The platform has access to information about an individual's device, location, contacts, content, preferences, and patterns. It also knows a users' name, age, gender, and interests. An updated privacy policy inform users that TikTok will also "collect biometric identifiers and biometric information," including users' face and voice. TikTok's business line expansion and adoption of new technologies practically ensures it will harvest greater variety of sensitive Western data.

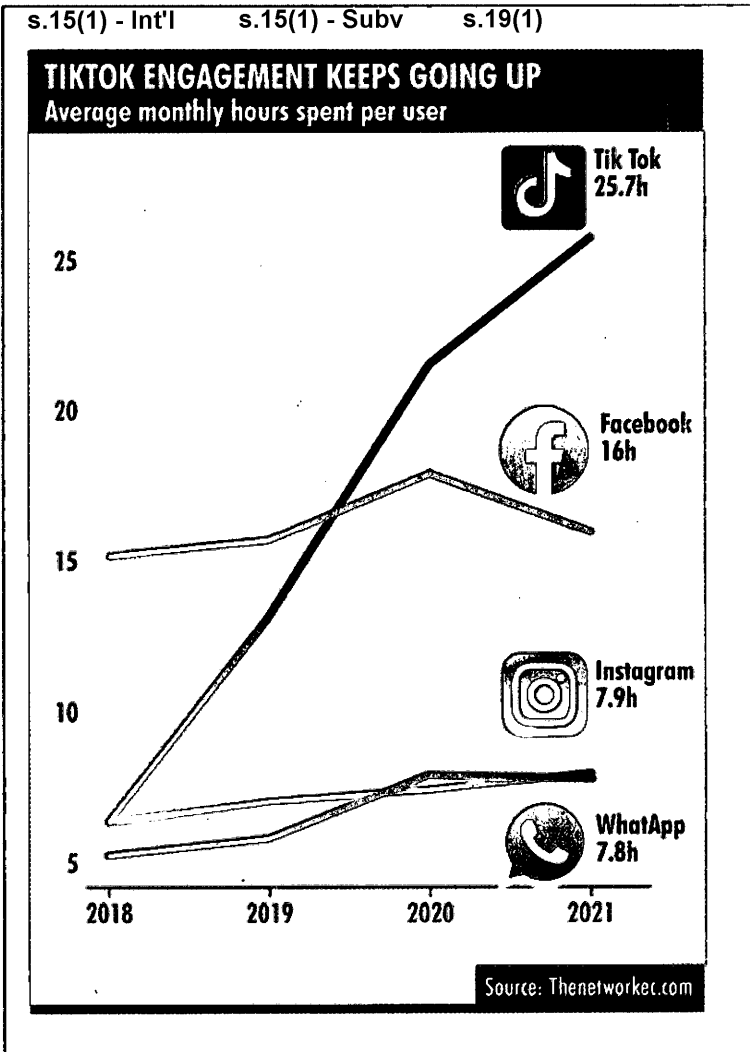
3. Control the Information Environment.

ByteDance's CEO has professed support for the CCP's propaganda agenda. Additional open sources reveal active TikTok censorship "on a range of political and social topics, while also demoting and suppressing content." Revelations from within ByteDance itself show AI-amplified content oversight and suppression, bolstering the work of 20,000 human content moderators. While Western social media applications are imperfect and can serve foreign disinformation agendas,

4. Origins and Western Response. ByteDance created TikTok in 2018, after acquiring U.S. platform Musical.ly. Although ByteDance was required to divest TikTok in 2020 by the Committee on Foreign Investment in the United States (CFIUS), that order is unenforced. U.S. mitigation efforts to protect user data are also unfulfilled, despite ByteDance's commitments. Multiple sources suggest that Western data remains accessible to China. A TikTok official admits: "Everything is seen in China." Deliberate deception is unclear, but there is a trust deficit due to the difference between ByteDance's words and its actions. In June 2022, the U.S. Federal Communications Commission (FCC) wrote to Apple and Google about the "serious national security threats" posed by TikTok, seeking its removal from their app stores: "It is clear that TikTok poses an unacceptable national security risk due to its extensive data harvesting being combined with Beijing's apparently unchecked access to that sensitive data". Other nations share these concerns, reacting with public cautions (e.g. Australia), to outright bans (e.g. India)

HIGH-RISK OUTLOOK

5. As of 2022, there are over 8 million Canadian TikTok users, ranging from 55% of teenagers to Members of Parliament. It harvests their data, offering false public and governmental reassurances about data sovereignty and security. TikTok—and its Chinese owner ByteDance—command the modern information environment.



Analyst: [Redacted]  
Director: [Redacted]

Assessment Base: This assessment is based on open source and classified reporting.

Consultations and Responsibilities: The judgements in this assessment are the responsibility of PCO-IAS. (C)

This assessment has been approved by:  
Martin Green  
Assistant Secretary to the Cabinet  
Intelligence Assessment  
(613-957-5107)