Centre for International
Governance Innovation

Policy Brief No. 221 — January 2026

# Rethinking TikTok Regulation in Canada

Matt Malone and Oren Tsur

## Key Points

- Since its launch in 2017, TikTok has become an enormously popular app in Canada — and the source of many privacy and security concerns.
- Recently, the Canadian federal government restricted the operation of TikTok Technology Canada Inc., based on the findings of an undisclosed national security review taken under the auspices of the Investment Canada Act (ICA), while still permitting the app run by TikTok Pte. Ltd. to collect, use and analyze Canadians' data. This dual approach overlooks key opportunities for Canada to strengthen its digital sovereignty with respect to the identified concerns.
- There are four forms of more effective regulation, including: text and data mining (TDM) exceptions; mandatory access to TikTok application programming interfaces (APIs); required disclosure of TikTok source code to the government; and stricter data localization requirements of data collected by the app.

## The Unprecedented Popularity of TikTok

In September 2025, several Canadian privacy regulators unveiled a long-awaited report on TikTok's "collection, use and disclosure of the personal information of individuals in Canada." That investigation revealed just how popular the app had become, with 14 million Canadian monthly users. It also noted that approximately 500,000 underage users — those below the age of 13 (and 14 in Quebec) — are removed from the app each year (412,241 in 2021; 506,363 in 2022; and 579,306 in 2023). Prior to their removal, those children are the focus of targeted ads and tailored content recommendations (Joint Investigation 2025). The investigation revealed how important government policy regarding the app is to many Canadians.

## About the Authors

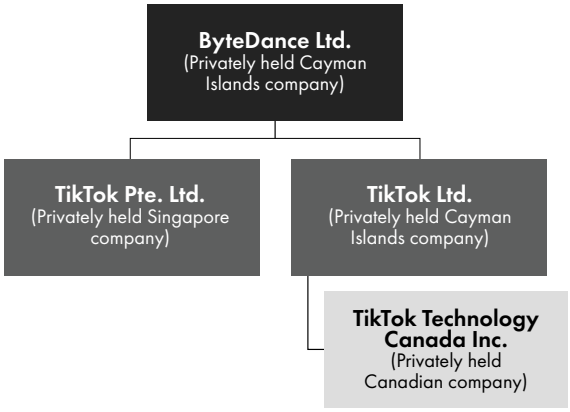
Matt Malone is a fellow at the Balsillie School of International Affairs and the Founder of Open by Default, which is hosted by the Investigative Journalism Foundation.

Oren Tsur is an assistant professor (senior lecturer) in the Department of Software and Information Systems Engineering at Ben Gurion University, where he heads the Natural Language Processing and Social Dynamics Lab.

# TikTok's Corporate Structure in Canada

Figure 1 provides a quick overview of the corporate structure of TikTok in Canada (relevant details of ownership are discussed in later sections).

### Figure 1: Corporate Structure of TikTok in Canada




*Source:* Authors.

This company began operating in Canada through the 2018 acquisition of Network Sense Ventures Limited and was later rebranded TikTok Technology Canada Inc. It "sells advertising space to consumer brands, governments, and other Canadian organizations that wish to advertise on the TikTok Platform" and engages in lobbying (both directly in Parliament and also through publicity campaigns, including buying ads in influential policy venues such as Air Quotes Media).[1]

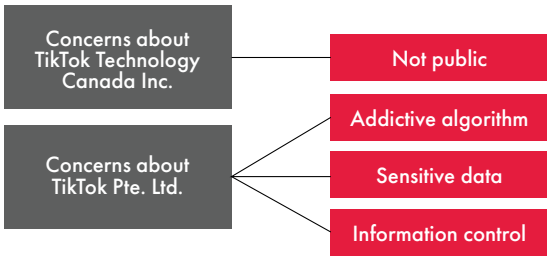
**TikTok Pte. Ltd.**: This company "is responsible for distributing the TikTok app in the Google Play Store and Apple App Store" (Office of the Privacy Commissioner of Canada 2025a). When TikTok Pte. Ltd. collects user data, it stores the data in Malaysia, Singapore and the United States (Virginia) (TikTok 2023b). Its authority to engage in this activity is regulated by federal and provincial privacy laws.

1 *TikTok Technology Canada Inc v Canada (AG), Minister for Innovation, Science and Economic Development and the Governor in Council*, Notice of Application, FC, T-3463-24 (filed 5 December 2024).

# Government Concerns

In various public fora, Canadian federal governments have expressed different concerns about TikTok Technology Canada Inc. and TikTok Pte. Ltd. (see Figure 2). These concerns can briefly be summarized as follows.

## Figure 2: Government Concerns About TikTok Technology Canada Inc. and TikTok Pte. Inc.




*Source:* Authors.

## Concerns About TikTok Technology Canada Inc.

As indicated above, little is known about the federal government's concerns regarding TikTok Technology Canada Inc. Publicly available information shared by the company and the government has revealed limited information (see Table 1 on the following page).

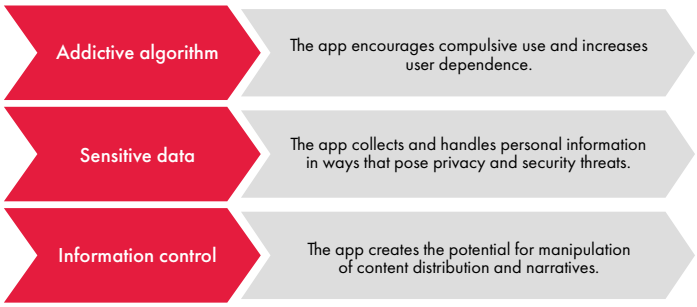
## Concerns About the TikTok Pte. Inc. App

Separate from the issues involving TikTok Technology Canada Inc., concerns have also been raised about privacy and security risks associated with the app operated by TikTok Pte. Ltd. These are well known. A September 2022 brief (released in June 2023) from the Privy Council Office's Intelligence Assessment Secretariat — reportedly used in the decision to ban the app on government-issued mobile devices — raised concerns in three main areas (see Figure 3).

### Addictive Algorithm

With TikTok's approximately 14 million Canadian users, roughly 40 percent of Canadians aged 16–29 use the app daily (compared with only four percent of Canadians over age 60) (TikTok 2025; Lockhart 2025). Ample research and scholarship have identified the effects of recommendation algorithms in using online behavioural data to shape beliefs, values and behaviour, in particular among young people (Coates et al. 2019; Himelboim and Golan 2023; Tolbert and Drogos 2019; Whittaker et al. 2021). While many examples of these impacts may seem benign, the Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions (the Hogue Inquiry) underscored how malicious actors also utilize these vectors to stoke social divisions (Medford-Kerr 2025; Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions 2025). For example, in 2024, the European Union reported — and TikTok confirmed — that a significant information operation involving "a large network of fake TikTok accounts" was involved in "pushing disinformation about Ukraine" (EU Disinfo Lab 2024). TikTok itself has published a list of "covert influence operations" that it has uncovered on its networks,

## Figure 3: Concerns about TikTok Pte. Inc. App




*Source:* Authors.

## Table 1: Findings

| Timeline | Events |
|---|---|
| 2018–2020 | During its first two years in Canada, required notices under the ICA were not provided to the federal government ("ICA notices"). |
| August 2020 | According to TikTok Technology Canada, the above delay was made known to the federal government. |
| September 2020–January 2023 | The Foreign Investment Review and Economic Security (FIRES) branch of Innovation, Science and Economic Development, with the agreement of officials from the Department of Canadian Heritage, agreed with TikTok Technology Canada Inc. to delay the filing time for the ICA notices. According to TikTok Technology Canada Inc., FIRES "took the position that it would be preferable for TikTok [Technology] Canada [Inc.] to delay filing" in light of events happening in foreign jurisdictions.[2] |
| February 2023 | FIRES contacted the company to inform them that "it would soon be requesting" the ICA notices.[3] |
| March 2023 | FIRES began issuing requests for information from the company. |
| June 2023 | TikTok Technology Canada Inc. submitted the final ICA notices. |
| September 2023 | The federal government issued a section 25.3 notice under the ICA, ordering a national security review of TikTok Technology Canada Inc., which included "a confidential summary of the national security concerns."[4] |
| March 1, 2024 | The federal government issued a policy statement on investment reviews in the interactive digital media sector that recognized how hostile state-sponsored and influence actors "leverage foreign investments in the interactive digital media sector to propagate disinformation or manipulate information in a manner that is injurious to Canada's national security" (Government of Canada 2024). |
| November 5, 2024 | The federal government announced it was ordering a "wind up" of TikTok Technology Canada Inc. The decision emphasized that "the government is not blocking Canadians' access to the TikTok application or their ability to create content" (Innovation, Science and Economic Development Canada 2024). |
| December 5, 2024 | TikTok Technology Canada Inc. initiated a judicial review of the decision. |
| December 12, 2024 | Dan Rogers, director of the Canadian Security Intelligence Service (CSIS), noted that CSIS, which participated in the ICA review, found "that there were national security reasons to be concerned with TikTok [Technology] Canada [Inc.]'s establishment" and that the larger assessment was "consistent" with the March 2024 policy statement.[5] |
| Present | TikTok Technology Canada Inc.'s judicial review remains ongoing, although there is little reason to expect it will succeed (Diab 2025). |

*Data source:* Global patent databases, accessed via Questel Orbit Intelligence, September 2025.
*Source:* Authors.

2 *TikTok Technology Canada Inc v Canada (AG), Minister for Innovation, Science & Economic Development and the Governor in Council*, Notice of Application, FC, T-3463-24 (filed 5 December 2024).

3 *Ibid.*

4 *Ibid.*

5 House of Commons, Standing Committee on Access to Information, Privacy and Ethics, Evidence, ETHI-145 (12 December 2024).

with many of those targeting the war between Russia and Ukraine but also political discourse in Cambodia, China, Ecuador, Indonesia, Iraq, Malaysia, Serbia and Thailand (TikTok 2023a).

This is what misinformation and disinformation look like in practice: trust and persuasion are critical in the maintenance of trust in institutions, and values are central to identity and decision making; when values are shaped and intermediated by algorithms, trust can become fragile. In turn, the erosion of trust can generate polarization and hate and erode baseline social cohesion.

## Sensitive Data

User profiling based on data usage and consumption, as well as obtrusive permissions (required or set by default) such as location, contacts list, documents and media files, pose a significant threat. Concerns over these threats are alluded to in a number of official statements. For example, in February 2023, Treasury Board President Mona Fortier, in announcing the ban of the TikTok app from government devices, also noted that the data collection methods used by TikTok provided "considerable access to the contents" of users' phones (Treasury Board of Canada Secretariat 2023). Similarly, CSIS Director Rogers told Parliament that "social media platforms in particular are of interest to threat actors because of the data they generate and collect."[6]

Essentially, there are two main types of potential backdoors in TikTok. First, there are concerns about a built-in or intentional backdoor that is either known to TikTok's creators and exploitable by them or to a malicious actor such as the People's Republic of China (PRC). For example, the source code may include mechanisms that allow access to other data on a user's device, beyond what the app needs for normal operation. In some cases, this might even appear to be legitimate access because the user has granted permissions. Second, there are concerns about exploitation by third parties, such as foreign governments or non-governmental actors, who may find vulnerabilities in TikTok's servers. If successful, they could gain access to the same user data that TikTok normally collects. In this case, the backdoor does not come from the app's intentional design, but rather from weaknesses in its security that outside actors can exploit.

These backdoor access concerns are not theoretical concerns with respect to data use by TikTok itself or, among others, the PRC and the United States. TikTok has admitted to accessing user data to track journalists (Murphy 2022). As noted above, none of the data TikTok collects by and about Canadians is stored in Canada. Rather, according to a 2023 report from TikTok, it is stored in Malaysia, Singapore and the United States (Virginia) (TikTok 2023b).

**With respect to the PRC:** In recent years, Canada's national security and intelligence agencies and law enforcement entities have focused on the PRC. The Hogue Inquiry noted that the PRC poses "the most sophisticated and active cyber threat to Canada" — a view reiterated by the Communications Security Establishment Canada (CSE) (Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions 2025). Thus, the concerns regarding China are particularly pronounced. China has a "golden share" in ByteDance through one or more entities (De Mott 2023). Even though this minority share does not amount to "TikTok being owned by China" (approximately 58 percent of ByteDance Ltd., in the words of TikTok Technology Canada Inc.'s lawyers, is "owned by investors around the world"), this stake provides the state — through an array of data collection laws passed in recent years — with powers that give the Chinese government "the legal and physical capability to compel any Chinese entity or person to turn over information" (US Department of Homeland Security 2020).[7] Rogers has clearly noted these risks to Parliament. "Through its 2017 National Intelligence Law," he told a parliamentary committee in December 2024, "the PRC compels PRC citizens and entities to co-operate with PRC intelligence agencies upon request, which includes providing all information to the state and its intelligence apparatus." When asked if the data was likely to wind up in the PRC, he said this was "certainly foreseeable."[8]

**With respect to the United States:** Section 702 of the Foreign Intelligence Surveillance Act enables the intelligence community to engage in the quasi-warrantless collection of data of non-US

6 Standing Committee on Access to Information, Privacy and Ethics, *supra* note 5.

7 *Ibid*.

8 Standing Committee on Access to Information, Privacy and Ethics, *supra* note 5.

targets reasonably believed to be located outside the United States. If the US government wanted to access Canadian data collected by TikTok and stored in the United States, there would be little oversight or review of those practices.

### Control of the Information Environment

Concerns related to "information control" are wide-reaching, especially as they pertain to societal-level risks concerning profiling and manipulation. Platforms deploying algorithms to intermediate what users read can amplify content, narratives and threads, and users internalize the values of these messages. CSIS itself has recognized that the PRC is "increasingly using social media and the Internet for disinformation campaigns involving elections" (Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions 2025).

During the lead-up to the 2025 Canadian federal election, the Security and Intelligence Threats to Elections (SITE) Task Force, comprised of CSIS, CSE, Global Affairs Canada and the Royal Canadian Mounted Police, identified an information operation with alleged ties to the PRC that targeted the Liberal Party of Canada (LPC) leadership candidate Chrystia Freeland (Tunney 2025). During the election itself, SITE identified a campaign by WeChat's "most popular news account," which intelligence had linked to the PRC, against Prime Minister, LPC leader and LPC candidate for Nepean, Mark Carney. SITE identified that the goal of the campaign was "to influence Chinese communities in Canada" during the election (Privy Council Office 2025). Later during the same election, a deepfake of Carney announcing a ban on cars made before 2000 originated on TikTok and circulated widely (Saeed 2025).

One of the challenges in monitoring and assessing these influence campaigns is the multimodal nature of many social media platforms, in particular their "unique content and interaction structures" (Luceri et al. 2025). A lack of access to raw data from these platforms inhibits properly studying its effects. For example, in Canada, organizations such as the Media Ecosystem Observatory (MEO) use mostly processed data from social media platforms to examine "how information, stories, and influence move online today" (Pehlivan et al. 2025). MEO has noted it faces challenges with "platform restrictions" in accessing data (ibid.).

By its own accord, TikTok publishes limited information relating to transparency efforts, including "Community Enforcement Guidelines," "Government Removal Requests," internet protocol removal requests, efforts to combat child sexual exploitation and abuse, and more. Many of these reports are specifically tailored to jurisdictions, pursuant to regulatory requirements.[9]

## Revisiting the Policy Response

### Drawbacks of the Corporate Wind-Up

While the shutdown of TikTok Technology Canada Inc. has asserted Canada's sovereignty through the ICA in response to the concerns about injury to national security, it also has several significant drawbacks, in particular when it comes to Canada's enforcement capabilities (Malone 2025).

First, the wind-up order *weakens* the state's investigative power. In December 2024, the privacy commissioner of Canada, Philippe Dufresne, told Parliament that his investigations are "easier if the organization is in Canada."[10] Shutting down the app also seems likely to undermine commitments such as TikTok's partnership with Elections Canada during the 2021 election, a feature providing information on voting locations.[11]

Second, the wind-up order *diminishes* the ability of state actors to issue fines and hinders parties from seeking redress for harms and wrongs. In the event that fines are levelled against TikTok Technology Canada Inc. by a government actor, the ability to collect those fines or penalties may be seriously diminished. Similarly, if a party seeks to bring a claim against TikTok, they would be required to do so through a non-Canadian actor.

And, finally, the wind-up is *not in line with other actions*, such as government use of other ByteDance-owned tools. For example, CapCut, a video-editing app, is not banned on government-

9 See www.tiktok.com/transparency/en/reports/.

10 Standing Committee on Access to Information, Privacy and Ethics, *supra* note 5.

11 *Ibid*.

issued devices, and Canadian federal ministers have recently posted videos made using CapCut on social media. This is also true of other ByteDance-owned apps, such as Toutiao, a news and information app, as well as Lemon8, a lifestyle app. Similarly, other social media apps, such as Facebook, Instagram, LinkedIn, Snapchat and X, are permitted for download on government-issued devices, including those with a nexus to the PRC such as Weibo, a micro-blogging site that is similar to X.

Perhaps most importantly, by remaining **shrouded in secrecy** at the same time it seemingly contradicts several other avenues of enforcement without clear justification (such as those proposed in this policy brief), the wind-up order has the effect of undermining public support and generating significant confusion and criticism.

While these drawbacks are real, these concerns are somewhat muted by issues of access to raw and meta data.

## Current and Potential Responses to Concerns About TikTok Pte. Ltd.

Because most of the concerns about TikTok have focused on the app, not the corporate entity, the federal government's (and provincial counterparts') response to TikTok Pte. Ltd. raises some additional questions. This is particularly true given that the public comments on the threats associated with TikTok generally relate to TikTok Pte. Ltd. A range of policy responses has been contemplated for TikTok Pte. Ltd, as demonstrated in Figure 4.

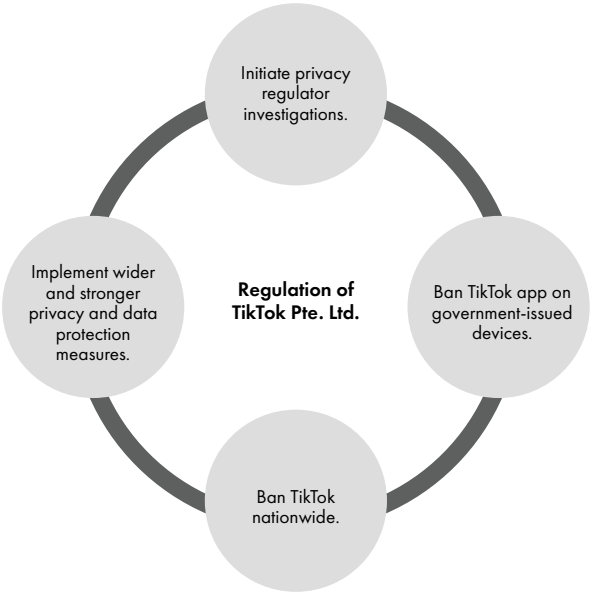
So far, TikTok Pte. Ltd. has largely escaped regulation. Currently, the government is engaged in the following regulatory or enforcement-related practices:

**Action: Initiate privacy regulator investigations**
Status: Under way/complete
Description: In October 2025, various privacy regulators in Canada completed an investigation into TikTok Pte. Ltd.'s compliance with privacy legislation (Office of the Privacy Commissioner of Canada 2025a). As a result of this investigation, TikTok Pte. Ltd. was required to utilize more age-assurance mechanisms.

**Action: Ban TikTok app on government-issued devices**
Status: Mostly complete
Description: Beginning in February 2023, the app has been banned by many Canadian government entities on government-issued devices. This approach is already in effect with respect to government-issued devices in most jurisdictions in Canada (mirroring the European Union and the United States).

**Action: Ban TikTok app nationwide**
Status: Not taken
Description: Several countries have proceeded with

Figure 4: Regulation of TikTok Pte. Ltd.




*Source:* Authors.

full bans, and such an approach may enjoy support in Canada. According to a study from The Dais, 52 percent of Canadians strongly or somewhat support a ban on TikTok, compared with 19 percent strongly or somewhat opposing one. The remainder have no opinion or knowledge of the issue (Lockhart 2025). While there are important questions about how such a ban would be implemented — whether through special legislation, as in the United States, or through the Emergencies Act — this option has not been seriously explored.

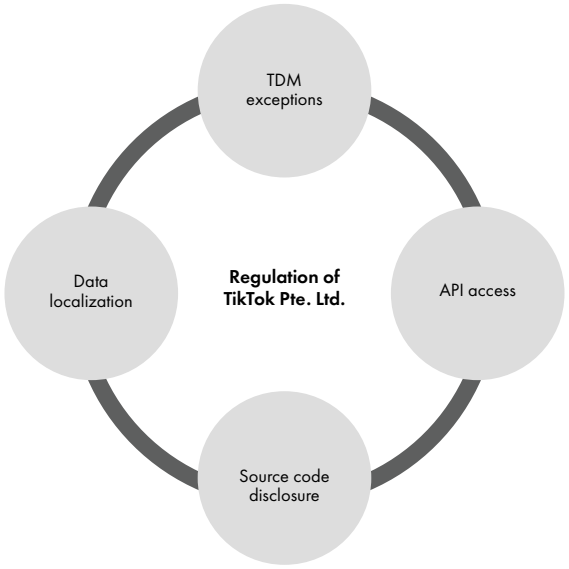
**Action: Implement wider and stronger privacy and data protection measures**
Status: Not taken
Description: Many of the solutions necessitated in the case of TikTok should be implemented in any reform to Canada's outdated privacy and data protection regime and the broader policy environment of government use of technology. These measures include:

- tightening the digital environment regarding the download and use of all social media apps on government-issued devices;
- providing order-making power for the privacy commissioner of Canada;
- raising the thresholds for private companies to collect and transfer data;
- imposing data localization requirements for companies of a certain size; and
- severely raising penalties for social media platforms that fail to take all reasonable measures to prevent children younger than 13 from using them (this would follow TikTok's own policies, although the privacy commissioner of Canada has noted that children younger than 13 "still make use of [the app] nonetheless") (Office of the Privacy Commissioner of Canada 2025a).

# Recommendations: Strengthening the Policy Response

The authors of this policy brief advocate for a more nuanced approach to regulation. If the problem is the intermediation by platforms and algorithms, then effective regulation should focus on these aspects. In addressing this problem, the core challenge, in all cases, is that both governmental and non-governmental bodies "have to rely on platforms to access data in the first place" (Brown 2023). Accordingly, the authors advocate for the following policy changes (see Figure 5).

## Figure 5: Regulation of TikTok Pte. Ltd.




*Source:* Authors.

## TDM Exceptions and API Access

As noted above, one of the main challenges that civil society actors such as the MEO and academic researchers, including the authors of this policy brief, face is platform restrictions with respect to data access (Pehlivan et al. 2025). In recent years, there has been a tendency by platforms toward restricting access (for example, Meta shutting down the CrowdTangle API used by journalists and X charging exorbitant fees for its API) (Fischer 2024; Murtfeldt et al. 2024). Often when platforms disable or restrict access, researchers are forced to resort to guerilla scraping, which presents not only data quality issues but also ethical concerns and potential liability issues (Pehlivan et al. 2025). This has given way to an unfortunate situation: While these platforms have an immense cultural impact, the accompanying threats they pose are not being adequately examined.

At present, there is a lack of a well-developed framework for engaging in such research. Among other things, this may require the government to establish a full-fledged open-source intelligence framework to provide adequate safe harbours for researchers. Ultimately, the current approach favoured by the government — as seen in the recent call to develop advanced technologies for open-source intelligence due diligence to address questions of research security — prohibits scraping that contravenes platform terms of service, even when they are government entities, government-funded researchers or public interest actors (Innovation, Science and Economic Development 2025).

Further, other corporate entities of TikTok in the European Economic Area, Switzerland, the United Kingdom and the United States already provide vetted researchers with access.[12] The disadvantage facing Canadian researchers inhibits meaningful research, even as the TikTok app becomes more central in shaping beliefs, values and behaviour, especially among youth. Instead, the government should compel data access for government and vetted researchers, as recommended by a parliamentary committee in 2025.[13] This would have the effect of bolstering SITE and other government entities' capacity, as well as non-governmental entities, such as civil society and academia, to engage in monitoring.

Precedents for such safe harbours already exist. For example, in the European Union and Japan, TDM exemptions for the purposes of scientific research help protect public interest researchers.[14] Likewise, the European Union's Digital Services Act requires "very large online platforms" and "very large online search engines" to "provide access to data to vetted researchers" who meet certain requirements — and to do so "without undue delay."[15] This includes, "where technically possible," access "to real-time data."[16] TikTok is designated as a "very large online platform" in the European Union, and, as such, is required to comply with this provision; however, its compliance with these requirements raised some concerns, and so any heavy-handed control by TikTok Technology Canada Inc. should be prevented — for example, mandatory sharing of research findings in advance, overly strict confidentiality obligations and similar measures (Chan 2024). One researcher noted that some data delivered was unreliable, indicating the need to strengthen the requirements — under penalty of fines — to allocate sufficient resources for this access (Darius 2024).

## Source Code Access

During the FIRES review, TikTok Technology Canada Inc. apparently made an offer to the federal government to provide source code. Although the federal government did not take TikTok up on that offer, the company is "hopeful that they will do so," and the authors of this policy brief believe that they should do so.[17] That offer should not only be accepted by the Canadian government, but it should also be mandated. Reviewing source code — the most recent stable version that was deployed to production, or even, if necessary, all versions deployed to production and material such

12 See https://developers.tiktok.com/products/research-api/.

13 Standing Committee on Access to Information, Privacy and Ethics, *supra* note 5.

14 EC, *Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC* [2019] OJ, L 130/92; *Copyright Act* (Japan) (Act No 48 of 6 May 1970, as amended up to 1 January 2022)..

15 EC, *Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act)* [2022] OJ, L 277/1.

16 *Ibid*.

17 Standing Committee on Access to Information, Privacy and Ethics, *supra* note 5.

as audit logs, algorithm change logs or performance logs — can help identify potential backdoors, vulnerabilities and other threats, intentional or not yet recognized. For example, TikTok Pte. Ltd. has admitted to spying on reporters and improperly accessing personal data (Office of the Privacy Commissioner of Canada 2025a). Privacy and security concerns can be much better observed through mandatory source code disclosures.

This approach would also put the transparency onus on TikTok Technology Canada Inc. For example, if the company refused to provide the code, that would make it — and not the Canadian government — the actor that chose secrecy. Moreover, this move is not without precedent, given that China has routinely asked foreign technology companies to provide source code (Volz 2016). While source code is undoubtedly sensitive as trade secrets, such status can be broken under Canadian law using public interest overrides — in other words, demanding disclosure when it is in the public interest.[18] However, given such sensitivity, it is reasonable that this access only be granted to the government itself.

While there are several apparent drawbacks, such as Chinese orders to Canadian companies to disclose source code, these precedents are already a real concern. Operationally, there is also currently no trade agreement in place that would prevent a demand for this type of access (as there is if the request were made to an American company, since the Canada-United States-Mexico Agreement provides that no state party to the agreement "shall require the transfer of, or access to, a source code of software owned by a person of another [state] ... as a condition for the import, distribution, sale or use of that software, or of products containing that software, in its territory."[19]

## Data Localization Requirements

Although it would have seemed unimaginable a short time ago to conflate these issues, the political sensitivities of the present moment in Canada mean that there are vivid concerns about Chinese and American access to the data TikTok Pte. Ltd. collects about Canadians. Data localization has potential benefits such as easing government authorities' access to data (for example, subpoena powers), while also reducing or averting access by foreign actors to data otherwise stored in their jurisdictions. In addition to these questions of lawful access, there are potential economic benefits that come from requiring platforms to establish infrastructure for their technologies in Canada, using Canadian products and employing Canadians.

Both the United States and the European Union require the default storage location of user data in their respective territories (Project Texas[20] and Project Clover, respectively) (Milmo 2023). Canada should do the same. Data localization is extremely popular in Canada. A 2021 survey noted that 75 percent of Canadians have concerns about an organization transferring their personal information outside of Canada (BC Freedom of Information and Privacy Association 2021). To be sure, countries using data localization to assert their sovereignty and control over their citizens' data are also using such demands to gain power. For example, such calls may serve not only as attempts to immunize domestic markets from global competition or to create incentives for foreign companies to invest locally, but they might also invite opportunities for the concentration of power and expansion of surveillance skills in ways that should be monitored closely (Yayboke, Ramos and Sheppard 2021).

# Conclusion

The influence of the TikTok app in shaping the beliefs, values and behaviours of Canadians cannot be dismissed and demands greater scrutiny. Right now, the most serious concerns about TikTok Pte. Ltd. have gone unaddressed. It should not befall the federal government alone to engage in this scrutiny. Canadian experts can help — but they need the ability to study TikTok's content ecosystem in real time. Without data-scraping protections as well as direct data access, governmental and non-governmental watchdogs are effectively flying blind. Opening up the app to scrutiny through mandated API

18 *Access to Information Act*, RSC 1985, c A-1, online: <https://laws-lois.justice.gc.ca/eng/acts/a-1/>.

19 *Canada-United States-Mexico Agreement*, 30 November 2018, c 19, art 19.16 (entered into force 1 July 2020), online: <www.international.gc.ca/trade-commerce/trade-agreements-accords-commerciaux/agr-acc/cusma-aceum/text-texte/19.aspx?lang=eng>.

20 See https://usds.tiktok.com/usds-about.

access and source code disclosure and stricter data localization requirements will enhance informed policy, academic insight and public accountability while the app remains in wide usage.

## Acronyms and Abbreviations

| | |
|---|---|
| APIs | application programming interfaces |
| CSE | Communications Security Establishment Canada |
| CSIS | Canadian Security Intelligence Service |
| FIRES | Foreign Investment Review and Economic Security |
| ICA | Investment Canada Act |
| LPC | Liberal Party of Canada |
| MEO | Media Ecosystem Observatory |
| PRC | People's Republic of China |
| SITE | Security and Intelligence Threats to Elections |
| TDM | text and data mining |

## Works Cited


BC Freedom of Information and Privacy Association. 2021. Various polls. www.ipsos.com/sites/default/files/ct/news/documents/2021-11/FIPA%20Tables-2021-11-15_0.pdf.

Brown, Megan A. 2023. "The Problem with TikTok's New Researcher API is Not TikTok." Tech Policy Press, March 1. www.techpolicy.press/the-problem-with-tiktoks-new-researcher-api-is-not-tiktok/.

Chan, Kelvin. 2024. "TikTok faces European Union scrutiny for possible breaches of strict new digital rulebook." Associated Press News, February 19. https://apnews.com/article/european-union-tiktok-digital-regulation-3fd249bbc9ff78a4401827c4b84b71a7.

Coates, Anna E., Charlotte A. Hardman, Jason C. G. Halford, Paul Christiansen and Emma J. Boyland. 2019. "Social Media Influencer Marketing and Children's Food Intake: A Randomized Trial." *Pediatrics* 143 (4): e20182554. https://doi.org/10.1542/peds.2018-2554.

Darius, Philipp. 2024. "Researcher Data Access Under the DSA: Lessons from TikTok's API Issues During the 2024 European Elections." Tech Policy Press, September 24. www.techpolicy.press/-researcher-data-access-under-the-dsa-lessons-from-tiktoks-api-issues-during-the-2024-european-elections/.

De Mott, Filip. 2023. "TikTok parent ByteDance has special stock owned by China's government. Here's how 'golden shares' give Beijing influence over the social-media giant." Business Insider, March 29. https://markets.businessinsider.com/news/stocks/tiktok-ban-bytedance-golden-shares-chinese-government-communist-party-board-2023-3.

Diab, Robert. 2025. "Why TikTok's challenge to the order to leave Canada will fail — and how." *Robert Diab* (blog), January 5. www.robertdiab.ca/posts/tiktok-challenge.

EU Disinfo Lab. 2024. "Massive Russian Influence Operation on TikTok and Beyond." Webinar, March 5. www.disinfo.eu/outreach/our-webinars/massive-russian-influence-operation-on-tiktok-and-beyond/.

Fischer, Sara. 2024. "Meta Shuts Down Data Tool Widely Used by Journalists." Axios, March 19. www.axios.com/2024/03/19/meta-shut-off-data-access-to-journalists.

Government of Canada. 2024. "Policy Statement on Foreign Investment Review in the Interactive Digital Media Sector." March 1. https://ised-isde.canada.ca/site/investment-canada-act/en/home/policy-statement-foreign-investment-review-interactive-digital-media-sector.

Himelboim, Itai and Guy J. Golan. 2023. "A Social Network Approach to Social Media Influencers on Instagram: The Strength of Being a Nano-Influencer in Cause Communities." *Journal of Interactive Advertising* 23 (1): 1–13. https://doi.org/10.1080/15252019.2022.2139653.

Innovation, Science and Economic Development Canada. 2024. "Government of Canada orders the wind up of TikTok Technology Canada, Inc. following a national security review under the *Investment Canada Act*." Statement, November 6. www.canada.ca/en/innovation-science-economic-development/news/2024/11/government-of-canada-orders-the-wind-up-of-tiktok-technology-canada-inc-following-a-national-security-review-under-the-investment-canada-act.html.

———. 2025. "Advanced technologies for open-source intelligence due diligence." Government of Canada, August 15. https://ised-isde.canada.ca/site/innovative-solutions-canada/en/advanced-technologies-open-source-intelligence-due-diligence.

Lockhart, Angus. 2025. *Survey of Online Harms in Canada 2025*. May. Toronto, ON: The Dais. https://dais.ca/reports/survey-of-online-harms-in-canada-2025/.

Luceri, Luca, Tanishq Vijay Salkar, Ashwin Balasubramanian, Gabriela Pinto, Chenning Sun and Emilio Ferrara. 2025. "Coordinated Inauthentic Behavior on TikTok: Challenges and Opportunities for Detection in a Video-First Ecosystem." arXiv, May 16. https://arxiv.org/pdf/2505.10867v1.

Malone, Matt. 2025. "While the U.S. Supreme Court deliberates a TikTok ban, Canada's own TikTok policy remains a mess." *The Globe and Mail*, January 15. www.theglobeandmail.com/business/commentary/article-while-the-us-supreme-court-deliberates-a-tiktok-ban-canadas-own-tiktok/.

Medford-Kerr, Marcus. 2025. "Dead or 'unalive'? How social platforms — and algorithms — are shaping the way we talk." *The Sunday Magazine*, July 27. www.cbc.ca/radio/sunday/algospeak-and-content-moderation-1.7594212.

Milmo, Dan. 2023. "TikTok unveils European data security plan amid calls for US ban." *The Guardian*, March 8. www.theguardian.com/technology/2023/mar/08/tiktok-european-data-security-regime-us-ban-social-video-app.

Murphy, Hannah. 2022. "TikTok admits tracking FT journalist in leaks investigation." *Financial Times*, December 22. www.ft.com/content/e873b98a-9623-45b3-b97c-444a2fde5874.

Murtfeldt, Ryan, Sejin Paik, Naomi Alterman, Ihsan Kahveci and Jevin D. West.. 2024. "RIP Twitter API: A Eulogy to Its Vast Research Contributions." arXiv, April 10. https://arxiv.org/pdf/2404.07340.

Office of the Privacy Commissioner of Canada. 2025a. "Consolidated Issue Sheets on the Wind Up of TikTok Technology Canada, Inc." April 8. www.priv.gc.ca/en/privacy-and-transparency-at-the-opc/proactive-disclosure/opc-parl-bp/ethi_20241210/is_20241210/.

Office of the Privacy Commissioner of Canada. 2025b. "Joint investigation of TikTok Pte. Ltd. by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Office of the Information and Privacy Commissioner for British Columbia, and the Office of the Information and Privacy Commissioner of Alberta." September 23. www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2025/pipeda-2025-003/.

Pehlivan, Zeynep, Saewon Park, Alexei Sisulu Abrahams, Mika Desblancs-Patel, Benjamin David Steel and Aengus Bridgman. 2025. "Building a Media Ecosystem Observatory from Scratch: A Data Infrastructure for Cross-Platform Analysis." arXiv, June 12. https://arxiv.org/pdf/2506.10942.

Privy Council Office. 2025. "Information operation on WeChat targeting the 45th General Election." Backgrounder, April 7. www.canada.ca/en/privy-council/news/2025/04/information-operation-on-wechat-targeting-the-45th-general-election.html.

Public Inquiry Into Foreign Interference in Federal Electoral Processes and Democratic Institutions. 2025. *Volume 1: Report Summary*. Final Report. January 28. https://foreigninterferencecommission.ca/fileadmin/report_volume_1.pdf.

Saeed, Henna. 2025. "PM Carney's deepfake: How to fact check and spot AI manipulation." CityNews, May 9. https://calgary.citynews.ca/2025/05/09/mark-carney-deepfake-how-to-spot-fake-videos/.

TikTok. 2023a. *Community Guidelines Enforcement Report.* December 13. www.tiktok.com/transparency/en-us/community-guidelines-enforcement-2023-3.

— — —. 2023b. "TikTok Facts: How we secure personal information and store data." News release, October 12. https://newsroom.tiktok.com/en-us/tiktok-facts-how-we-secure-personal-information-and-store-data.

— — —. 2025. "TikTok World Canada 2025: Driving Full-Funnel Growth with AI, Creativity and Community." News release, June 17. https://newsroom.tiktok.com/en-ca/tiktok-world-canada-2025.

Tolbert, Amanda N. and Kristin L. Drogos. 2019. "Tweens' Wishful Identification and Parasocial Relationships with YouTubers." *Frontiers in Psychology* 10: 2781. https:/doi.org/10.3389/fpsyg.2019.02781.

Treasury Board of Canada Secretariat. 2023b. "Statement by Minister Fortier announcing a ban on the use of TikTok on government mobile devices."Statement, February 27. www.canada.ca/en/treasury-board-secretariat/news/2023/02/statement-by-minister-fortier-announcing-a-ban-on-the-use-of-tiktok-on-government-mobile-devices.html.

Tunney, Catharine. 2025. "Freeland targeted by 'malicious' WeChat campaign with alleged ties to China: Threat task force." CBC News, February 7. www.cbc.ca/news/politics/freeland-wechat-malicious-activity-1.7454067.

US Department of Homeland Security. 2020. "Data Security Business Advisory: Risks and Considerations for Businesses Using Data Services and Equipment from Firms Linked to the People's Republic of China." December 22. www.dhs.gov/sites/default/files/publications/20_1222_data-security-business-advisory.pdf.

Volz, Dustin. 2016. "Apple refused China request for source code in last two years: lawyer." Reuters, April 20. www.reuters.com/article/business/apple-refused-china-request-for-source-code-in-last-two-years-lawyer-idUSKCN0XG28Y/.

Whittaker, Joe, Seán Looney, Alastair Reed and Fabio Votta. 2021. "Recommender systems and the amplification of extremist content." *Internet Policy Review* 10 (2). https://doi.org/10.14763/2021.2.1565.

Yayboke, Erol, Carolina G. Ramos and Lindsey R. Sheppard. 2021. "The Real National Security Concerns over Data Localization." Center for Strategic & International Studies. July 23. www.csis.org/analysis/real-national-security-concerns-over-data-localization.

## About CIGI

The Centre for International Governance Innovation (CIGI) is an independent, non-partisan think tank whose peer-reviewed research and trusted analysis influence policy makers to innovate. Our global network of multidisciplinary researchers and strategic partnerships provide policy solutions for the digital era with one goal: to improve people's lives everywhere. Headquartered in Waterloo, Canada, CIGI has received support from the Government of Canada, the Government of Ontario and founder Jim Balsillie.

## À propos du CIGI

Le Centre pour l'innovation dans la gouvernance internationale (CIGI) est un groupe de réflexion indépendant et non partisan dont les recherches évaluées par des pairs et les analyses fiables incitent les décideurs à innover. Grâce à son réseau mondial de chercheurs pluridisciplinaires et de partenariats stratégiques, le CIGI offre des solutions politiques adaptées à l'ère numérique dans le seul but d'améliorer la vie des gens du monde entier. Le CIGI, dont le siège se trouve à Waterloo, au Canada, bénéficie du soutien du gouvernement du Canada, du gouvernement de l'Ontario et de son fondateur, Jim Balsillie.

## Credits

Research Director, Digitalization, Security & Democracy Aaron Shull
Director, Programs Dianna English
Senior Program Manager Jenny Thiel
Publications Editor Christine Robertson
Graphic Designer Abhilasha Dewan



67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org

CIGI