

Geopolitics, Privacy, and User Trust: TikTok

By Yuko Xiao

Author Biography

Yuko Xiao is a current senior studying at White Rock Christian Academy in Vancouver as a diploma candidate. She is passionate about cognitive science specifically the interconnectedness of economics, geopolitics and psychology. She plans to major in consumer behavior or cognitive science in university and hopes to contribute to society by improving decision-making processes, fostering sustainable consumer practices, and bridging cultural divides

Abstract

The paper uses a thorough review of the current literature, governmental materials, and information available on ByteDance as the major source for analyzing the link between geopolitical aspects, privacy concerns, and user engagement with businesses. The study found that the uncertainty surrounding TikTok's data usage and the ongoing tensions between China and the United States leads to a decline in user trust. This is particularly evident in the e-commerce sector, where individual privacy concerns directly affect customers' buying habits and commercial involvement. This phenomenon would directly impact TikTok's international e-commerce expansion, as well as user engagement on the platform; ultimately affect the platform's overall growth and revenue potential. The paper concludes with recommendations for enhancing data privacy on TikTok such as reducing data collection from minors, putting stricter regulations on third-party data access and being more transparent about their data policies.

Keywords: TikTok, Data Security, Geopolitical Tension, User Trust, Ecommerce, User Engagement, Business Engagement, China, United States.

Introduction

TikTok, a short-video sharing app by Beijing ByteDance Technology Co., has rapidly ascended to the top of the social media hierarchy with over a billion users. Besides the widely known function of creating short looping videos, it has also shown great dominances in the e-commerce sector. Currently, over 11% of U.S. households have made purchases via TikTok Shop since its launch in September 2023 (Earnest, 2024).

With TikTok's massive user base and a growing e-commerce aspect, both consumers and business owners have been paying more attention to data security today. In relation to this matter, the sale-off bill of TikTok in United States and China has attracted many arguments due to huge amounts of personal data that it collects: user locations, device details and behavior information. One possible concern of the US is how TikTok shares its data with third parties such as advertisers or even governments, which are sensitive issues given ongoing geopolitical tensions between the U.S. and China. Although the company claims that such collected information is used by its algorithms for calculations on personalized content in their platform, there can be no assurance that privacy will not be violated. Research findings have indicated that trust in the platform directly influences trust between venders and buyers (Wu et al., 2023). Therefore, it is worthwhile to analyze whether there is a correlation between engagement and trust to determine if there are economic benefits from a policy of enhanced data security and privacy measures.

Currently, there is a lot of research done regarding security and trust relationship. However, none of those papers specify what exactly that would mean to normal citizens. Questions like "Is data violation a concerning topic for the public, or is it driven more by political tension?"

or "Does China's political regime directly influence business engagement?" are rarely addressed. Addressing these questions can support normal citizens in engaging better with social media with a correct knowledge of technical security, as well as the interplay between data security, trust, and user engagement, ultimately leading to better business strategies on the platform.

Based on the political policies of China and United States and the severity of privacy concerns, this paper will answer the research question "How do geopolitical tensions and differing privacy regulations between China and the United States influence user trust and engagement on TikTok?" Through this analysis, the paper will provide valuable insights into how these factors shape consumer attitudes and engagement.

Literature Review

Political Systems and Data Security

With the base of TikTok being in China, it carries many data security concerns for the foreign countries. China's communist regime exerts a significant influence on the economic functions (including oversight, data control, and strategic policy implementations) implementing laws that are designed to enhance government access to data while ostensibly protecting user's privacy (Zhao & Feng, 2021). Their implementation often prioritizes state security over individual privacy.

Some of the current policies are:

- **Cybersecurity Law:** Mandates real-name registration, restricts anonymity, and requires companies to store data locally, making it accessible to government authorities for surveillance and security purposes. (China Cybersecurity Law, Article 24, 37)

- **Data Security Law:** Requires companies to classify data based on its importance and ensure that sensitive data is stored within China, preventing foreign access. (China Data Security Law, Article 21, 31)
- **Personal Information Protection Law:** Imposes stringent requirements on data processing, including obtaining user consent and ensuring data security. (China Personal Information Protection Law, Article 13, 51)

From observing the policies, it can be seen how TikTok could be perceived as risky by countries like United States. The data localization requirements restrict the free flow of data and complicate compliance with international regulations, increasing operational costs for U.S. companies. The Chinese government to access data stored locally under these laws raises concerns about the use of this information in cyber warfare and economic espionage (Strand, 2016). And lastly, control over data can be used strategically to assert geopolitical influence, as data is increasingly seen as a critical asset in international relations (Ciuriak, 2022).

However, this doesn't mean everything is negative; there is still a robust legislative framework for data protection and cybersecurity. Since the government has the right to access the data for their interests, it wouldn't make sense for them to allow any data leakage. Similarly, if the data of an operator does not relate to national or social matters as indicated in Cybersecurity Law, it may not be classified as "important" hence is protected from such collection by the government - although some people argue that this clause raises controversy (Hong & School, 2017). Lastly, they might even favor the fact that they are the only ones with the data and would therefore work hard to protect it. Thus there seems to be no great likelihood of these possible risks without immense political tension. However, for countries like USA, where democracy

prevails, there's still more caution because, except in extreme cases, the state has no authority to order companies release their data. In this context, the US recently incorporated a sell-off bill requiring TikTok be sold off within 270 days or face a nationwide ban thereby showing strong concerns over privacy and security (Fung, 2024). This suggests that this political regime could influence TikTok's international expansion, potentially undermining the trust of companies unable to ensure long-term data security and compliance, leading to decrease in engagement of business internationally.

It is also essential to consider the potential exaggeration from the U.S. institution on privacy risks due to the geopolitical tension. Research may focus on the worst-case scenarios rather than a balance interpretation of possibility in data misuse. Similarly, this exaggeration might rally public opinion and introduce potential bias.

General Privacy Concerns & TikTok Privacy Policies

Shifting the attention to privacy concerns for consumers, these concerns mainly arise from the ease of obtaining users' personal data and the sharing of user data with third parties for advertising purposes. Under the guise of behavior analysis for better platform functionality, users' behavior is constantly monitored by platform owners. This need for data sharing and disclosure complicates privacy research in this era (Wang et al., 2022). Trying to be as holistic as possible for this essay, three dimensions will be addressed: awareness concerns (how much the user knows about data collection), usage concerns (how the data is used by the platform), and leakage consequences (the extent of harm to the users).

Based on current studies, it is suggested that users have low awareness and understanding of TikTok's data security practices. TikTok's publicly demonstrated privacy policies outline that only basic information is collected, such as profile information, user content, messages, purchase information, network contacts, identity, location information, and image and audio information (TikTok, 2022). However, the document doesn't specify exactly how the data is used; most of the language in these policies is vague, commonly referencing the goal to "improve user experience," which doesn't offer clear insight into the data's actual use. It is even suggested in an interview on CNN's Anderson Cooper 360 with Ivan Tsarynny, CEO of Feroot Security, that TikTok could continue to access data even if the app is deleted, a capability that is not explicitly mentioned in the publicly available information on TikTok's privacy policy (Feroot, 2024). Nevertheless, few users actually read the policies.

Additionally, a significant portion of users recognize the potential dangers associated with TikTok. For example, a Pew Research study found that about six-in-ten Americans (59%) see TikTok as a major or minor threat to national security in the United States (McClain, 2023). This concern further highlights the issue of transparency in data collection and usage. The fact that users do not feel secure despite the publicly available information on TikTok's data security policies underscores the significance of a lack of clear communication. This unclear and often vague description of how TikTok handles security leads to increased worry among consumers. And when users are unsure about how their data is protected, it naturally result in a decrease in user engagement due to privacy concerns. However, it is worthwhile mentioning that though existing studies effectively document user's awareness of privacy concerns, they often lack empirical data that show how these concerns directly influence a specific

user's behavior. The exact action being influenced need further research. TikTok has often said that its data collection is primarily used to build algorithms and enhance the user experience. However, actions taken by its parent company ByteDance suggest there may be discrepancies between what it claims and what actually happens. TikTok claims that all U.S. user data is stored in data centers in the United States and Singapore, but a 2022 investigation by BuzzFeed revealed that ByteDance employees in China accessed non-public U.S. user data "many times" (Congressional Research Service, 2023). On top of that, TikTok CEO Chew cited research from the University of Toronto during his testimony, claiming that "TikTok does not publicly transmit data to the Chinese government."; but the researchers themselves disputed this, noting that their analysis "could not understand what happened to user data after it was collected and transmitted back to TikTok servers"(Congressional Research Service, 2023). This discrepancy suggests that ByteDance may not be fully adhering to its stated policies, raising questions about the actual usage of the data it collects. TikTok also grants access to numerous third-party entities with the lack of transparency about how these third parties manage and protect data. This raises concerns that user data may be improperly handled or sold without clear guidelines. Finally, there are concerns that the information collected by TikTok could be used to create politically biased information that China. The U.S. Congressional Research Service has said that there are concerns that TikTok could spread misinformation, propaganda, or censored content, which could lead to the formation of an "information cocoon" that could polarize society for China's own benefit (Congressional Research Service, 2023).

In discussing the consequences, this article will deliberately avoid the usual focus on specific case studies or enumerated

dangers. Instead, it will examine the types of information that can be accessed through TikTok and what this means for malicious Internet actors. Starting with profile information, TikTok collects and stores a variety of personal information, including your phone number, pictures and videos you post, like, or follow. This data can give a comprehensive picture of you, including your interests, social behavior, and basic personal information. Someone with access to this data can form a detailed profile of your identity and preferences. In addition to this, TikTok also records all message communications. This means that private messages a person exchanges with friends can be leaked, and someone can explore personal lives or vulnerabilities by accessing this information. The last and most worrying is location data, which allows someone to track an individual's exact location: includes where a person lives, work, go on weekends, and even daily life routines (for example, when a person takes a nap). This data is extremely valuable and, after being analyzed over time, can reveal a lot about life patterns. The potential harm associated with problems such as stalking, burglary, and other malicious crimes is significant.

Data security is a significant concern given the various issues discussed, however, these only become particularly pressing if these data were leaked. However, it is important to note that there is no clear incentive for the Chinese government or TikTok to deliberately leak this data, and there are no laws that openly permit the sale of such data without cause.

Impact of Privacy Concerns on Business & Consumer Engagement

Though data security for TikTok remains a less obvious concern for many users, it is becoming increasingly clear that consumers are growing more aware of how their data is collected, stored, and used. As this awareness spreads, privacy concerns will likely become a more significant factor in how consumers engage with e-commerce of TikTok.

This emerging market of TikTok, with its unique features such as the ability to stream and sell simultaneously, presents a vast opportunity. However, engagement is very important at this stage, and either businesses or consumers wouldn't want to join if the security of the market cannot be confirmed. It has been demonstrated that a significant 70% of respondents reported their purchase intentions were directly influenced by privacy concerns when using TikTok Shop (Putri et al., 2023). This highlights that if TikTok can maintain its consumers' trust and build a safe environment for it could be a major revenue spot for the company. However, this market is heavily built on trust, and historical data breaches have shown that privacy violations can lead to significant declines in users and business engagement. For example, the Cambridge Analytica scandal, where user information was accessed without consent and misused for political profiling and advertising, resulted in a short-term decline in daily active users and ad revenue for Facebook, along with hesitations from business partners (Brown, 2020). To avoid similar pitfalls, TikTok must prioritize data security, especially as its e-commerce platform is still in its growth stage, where competition is fierce, and trust is crucial. However, most current studies focus primarily on the U.S. and China, which may not fully represent the global population or encompass the regulatory environments of other regions.

Methodology

This paper does not incorporate primary research due to geopolitical sensitivities and access to Proprietary Information. From observing the difficulty to obtain firsthand data without encountering potential bias or legal constraint this paper utilizes only secondary sources. Specifically this research was conducted through an extensive review of existing literature, focusing on scholarly articles, government documents, and publicly available information.

from TikTok's original company ByteDance. The analysis is primarily based on critical review of these sources with primary experiment done by credible organization.

The analysis of geopolitical tension in this essay is approached as a market battle between China and the United States. By examining sources published by both the Chinese and U.S. governments, the essay explores how these tensions impact user and business engagement on TikTok.

The privacy regulation aspect is analyzed through a dual lens: publicly declared regulations and hidden practices used by TikTok. This includes an examination of TikTok's officially declared security policies and primary research conducted by organizations to uncover any undeclared data handling practices.

The sources prioritize government official document, followed by analyze of these material with research to find supporting academic paper. Sources are chosen based on the authorial credibility, applicability of the information and alignment with recent market. Data from those sources was extracted systematically. For example, legal documents addressing China's privacy concerns were carefully reviewed to specific law (e.g. Cybersecurity Law).

Discussion

The Extend of Influence of Geopolitical Tension and Privacy Regulation

The potential risks associated with geopolitical tensions surrounding TikTok are more concerning than the documented cases, making the full impact of these tensions uncertain. The primary security risk is the possibility of the Chinese government accessing user data, which could potentially be used maliciously against other countries. Although current evidence suggests

that actual misuse is unlikely, it is not impossible. Therefore, it is difficult to fully assess the extent of the influence, but it is clear that the situation is likely to become more concerning over time.

This uncertainty also slightly impacts the trustworthiness of the platform. As countries with growing concerns have already demonstrated actions such as potential shutdowns or regulatory crackdowns, this could deter business investments on the platform. This includes third-party investors, business partners, and influencers. Specifically, if influencers migrate to other platforms, they may take their followers with them, further reducing user engagement on TikTok.

The ambiguity surrounding TikTok's privacy regulations—particularly the lack of transparency about data handling—fuels significant trust issues. This uncertainty particularly affects TikTok's e-commerce sector, where users may engage with content (such as scrolling) but hesitate to make purchases due to privacy concerns. Over time, this decrease in market activity could lead to businesses exiting the platform due to declining consumer interest. Additionally, such ambiguity could attract businesses interested in exploiting user data, potentially causing TikTok to face a sharp decline in user engagement, similar to what happened with Facebook.

Looking into the future, while an outright regulatory ban remains possible, as seen with India's 2020 ban, this paper considers it generally unlikely. A more probable scenario involves the enforcement of stricter and more transparent privacy regulations, which may require TikTok to collaborate with a Western-based company to handle data. This belief is based on the idea that no country is eager to escalate political tensions; banning TikTok outright could potentially trigger a data access conflict between the U.S. and China. Additionally, TikTok's massive consumer base

and the many influencers who rely on the platform make a full shutdown less likely to gain public support. Lastly, ByteDance is unlikely to willingly withdraw from the U.S. market, given the platform's growing influence and potential in the e-commerce sector.

Recommendations

Based on the analysis of geopolitical tensions and privacy regulations, this section offers several recommendations.

1. **Limit data collection for children:**

Given that it is unlikely that TikTok can completely stop collecting personal data for its algorithms, this paper proposes that at the very least, the platform should limit the range of data collected from children. For instance, children under 16 should not be able to share location data or send their phone number, address, or contact information to strangers on the platform. This recommendation is based on the idea that individuals who may not have the resources to protect themselves if their data is compromised should minimize their online exposure. These additional protections for minors would help mitigate the data leakage risks discussed in the privacy concerns section. For example, it prevents the leakage of location data that could give malicious actors access to a child's daily routines.

2. **Adjust algorithm for younger user:**

Additionally, this essay suggests that the algorithm used to calculate personalized content should not be applied to children under 12-14 depending on timing of human development and sexual education in that specific region. This is due to belief that early exposure to algorithm-driven content could negatively impact cognitive and emotional development, especially around sensitive topics like sexuality. This approach would also provide

children with access to a broader range of information, thereby reducing the issue of information cocoons: which are associated with a lack of creativity and empathy. Moreover, not using the algorithm for younger children would minimize the platform's influence on their development, making parents more comfortable with allowing their children to use TikTok, which could potentially lead to increase user engagement.

3. **Regulated third-party access:** Current case studies and research indicate that the primary concern regarding data leakage comes from third-party platforms. Therefore, this essay recommends that when users access third-party platforms through TikTok, they should first be reconfirmed with their consent. TikTok should also implement strict regulations on the amount of information third parties can access. This essay argues that there is no justification for third-party platforms to have access to all personal profiles; instead, TikTok should retain control of the data and handle recommendations.
4. **Enhance transparency:** Most importantly, TikTok should openly and truthfully declare the amount of data they access, the regulations governing this data, and how it is used. If these aspects are addressed, this essay anticipates a significant improvement in user trust, which would likely lead to increased user engagement.

While some of the ideas like limiting data access for third parties may cause hesitation among some businesses and users, it is important to remember that TikTok's e-commerce sector is a long-term endeavor with substantial competition. This paper believes that losing some businesses and users that might misuse the platform is a worthwhile trade-off for creating a more secure platform and fostering engaged users.

In terms of consumer behavior, individuals are advised to limit the amount of personal information they share on TikTok. This is particularly important for younger users, who are more vulnerable to risks. Additionally, users should avoid discussing sensitive topics or sending private messages on the platform, as the current data transfer processes between platforms are opaque, and the potential consequences and ownership of data remain unclear. It is, of course, fine to engage on social media, but users should ensure they do not expose any information that could put them at risk. This advice is especially relevant in light of previous data breaches across social media platforms, which have exposed the vulnerability of users' private information, for example, the 2018 Cambridge Analytica scandal.

Conclusion & Future Research

In conclusion, the intersection of geopolitical tensions and varying privacy regulations between China and the United States plays a critical role in shaping user trust and engagement on platforms like TikTok and Douyin. As the platforms expand their reach in global markets, concerns over data security and privacy have become increasingly prominent. The current issue revolves around ByteDance retaining control over the data generated by TikTok. This situation that exacerbates geopolitical tension and raises concerns about potential privacy violations brings distrust and worry that potentially influence engagement in the market. The findings of this analysis support the main argument that geopolitical factors and privacy issues significantly impact TikTok's ability to maintain user and business trust. Specifically, ongoing geopolitical tensions raise significant concerns about TikTok's data security, deterring business investment and the lack of transparency in TikTok's data handling practices fuels trust issues, particularly

affecting its e-commerce sector, where users may hesitate to make purchases on the platform.

This whole analysis is built upon a very generalized concept, addressing the overall connection of geopolitical tension, privacy regulation and users & business engagement. However, it lacks specificity regarding particular communities (superficially discussed, in the case of minors) and does not delve into the duration of the impact or the specific types of engagement affected. These aspects would benefit from more detailed exploration, which could be achieved through primary research that targets these precise variables.

References

Ciuriak, D. (2022, March 11). The Geopolitics of the Data-Driven Economy. Papers.ssrn.com. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3770470

Congressional Research Service. (2023, March 29). TikTok: Recent Data Privacy and National Security Concerns. <https://crsreports.congress.gov/product/pdf/IN/IN12131>

Creemers, R., & Webster, G. (2021, August 20). Translation: Personal Information Protection Law of the People's Republic of China - Effective Nov. 1, 2021. DigiChina. <https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/>

Creemers, R., Webster, G., & Triolo, P. (2018, June 29). Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017). DigiChina; Stanford University. <https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/>

Earnest. (2024). Case Study: TikTok Shop Disruption Analysis with Credit Card Transaction Data. https://6513813.fs1.hubspotusercontent-na1.net/hubfs/6513813/Earnest%20Case%20Study_TikTok%20Shop%20Growth%20Analysis%20with%20Credit%20Card%20Transaction%20Data-1.pdf

Feroot. (2024, April 23). Beyond TikTok Tracking Pixels: CNN Anderson Cooper 360 interviews Ivan Tsarynny, CEO of Feroot Security. Feroot. <https://www.feroot.com/news/beyond-tiktok-tracking-pixels-cnn-anderson-cooper-360-interviews-ivan-tsarynny-ceo-of-feroot-security/>

Fung, B. (2024, April 24). Biden just signed a potential TikTok ban into law. Here's what happens next | CNN Business. CNN. <https://www.cnn.com/2024/04/23/tech/congress-tiktok-ban-what-next/index.html#:~:text=The%20bill%20that%20Biden%20signed>

Hong, Y., & School, Y. (2017). THE CROSS-BORDER DATA FLOWS SECURITY ASSESSMENT: An important part of protecting China's basic strategic resources. https://law.yale.edu/sites/default/files/area/center/china/document/dataflowssecurity_final.pdf

Lim, W. M., & Ting, D. H. (2012). E-shopping: An Analysis of the Uses and Gratifications Theory. *Modern Applied Science*, 6(5). <https://doi.org/10.5539/mas.v6n5p48>

McClain, C. (2023, July 10). Majority of Americans say TikTok is a threat to national security. Pew Research Center. <https://www.pewresearch.org/short-reads/2023/07/10/majority-of-americans-say-tiktok-is-a-threat-to-national-security/>

Nurdiana Putri, Yadhith Prasetya, Putu Wuri Handayani, & Fitriani, H. (2023). TikTok Shop: favorsHow trust and privacy influence generation Z's purchasing behaviors. *Cogent Social Sciences*, 10(1). <https://doi.org/10.1080/23311886.2023.2292759>

Strand, S. (2016). The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age. *Internasional Politik*, 74(4). <https://doi.org/10.17585/ip.v74.622>

TikTok. (2022). Privacy Policy | tiktok. TikTok.com. <https://www.tiktok.com/legal/page/row/privacy-policy/en#privacy-row>

Wang, Q., Zhang, W., & Wang, H. (2022). Privacy concerns toward short-form video platforms: Scale development and validation. *Frontiers in Psychology*, 13. <https://doi.org/10.3389/fpsyg.2022.954964>

Wu, W., Wang, S., Ding, G., & Mo, J. (2023). Elucidating trust-building sources in social shopping: A consumer cognitive and emotional trust perspective. *Journal of Retailing and Consumer Services*, 71, 103217. <https://doi.org/10.1016/j.jretconser.2022.103217>

Zhao, B., & Feng, Y. (2021). Mapping the development of China's data protection law: Major actors, core values, and shifting power relations. *Computer Law & Security Review*, 40, 105498. <https://doi.org/10.1016/j.clsr.2020.105498>