Forum: Economic and Social Council

Issue: Discussing TikTok's worldwide abolition in light of personal government abuse

Officer: Sofia Jifkins Arellano

Table of Contents

Introduction

The debate about the potential worldwide abolition of TikTok, in light of personal information abuse by governments, has become a significant global concern. TikTok has transcended being just an entertainment app to become a key element of the world's digital culture. Its rising popularity has deeply changed interpersonal interactions, content sharing, and self-expression in the virtual world. However, this unprecedented influence has raised serious concerns about user data security and privacy.

The main worry is the potential for ByteDance, TikTok's China-based parent company, to be compelled to share data with the Chinese government, raising fears of widespread surveillance and espionage. This issue goes beyond individual privacy to broader implications in national security and geopolitics.

The tension between global digital platform expansion and national privacy and security regulations has led various countries to consider restrictive measures or outright bans of TikTok. This discussion englobes data security, ethical and legal dilemmas about free speech, privacy rights, and data sovereignty in an increasingly interconnected world.

The TikTok concern is highly relevant for the United Nations Economic and Social Council (ECOSOC) delegates, covering crucial topics like international cooperation, information governance, and digital-era human rights. It highlights the need to balance user privacy protection, national security, and free speech in a rapidly evolving digital environment. This topic challenges nations to consider how to manage digital platforms' influence while preserving personal information integrity and security, posing both technological and political challenges.

Definition of Key Terms

ByteDance

The Chinese company that owns TikTok.

Data Privacy

The rights of individuals to control their personal information and how it's used.

Cybersecurity

The practice of protecting systems, networks, and programs from digital attacks.

National Security

The protection of a nation from threats, especially in the context of foreign surveillance.

Digital Sovereignty

A country's authority over digital data and infrastructure within its borders.

Surveillance Capitalism

The monetization of personal data by tech companies.

Influencer Economy

The rise of content creators who influence consumer behavior.

Viral Trends

How certain content rapidly gains widespread popularity on TikTok.

For you page

Section inside Tik Tok app where users can watch recommended videos for them, according to their personal preferences, which are identified and memorized by the algorithm.

Historical Context

Origins of Tik Tok

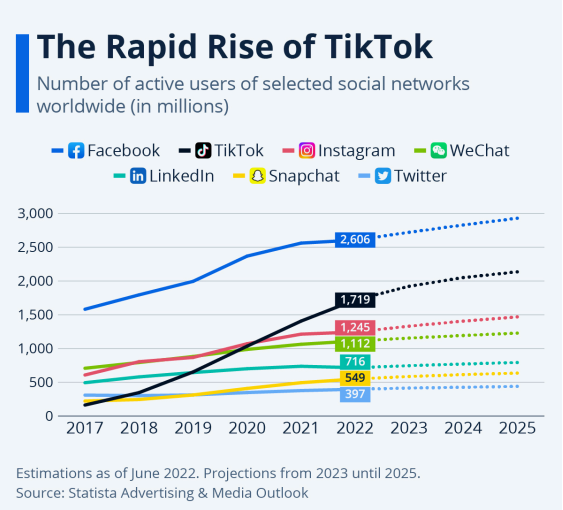
TikTok's emergence, unlike most content and social media networks, did not originate as a single innovation that evolved to its present state. In fact, its history began with three distinct applications. The first was Musically, launched in Shanghai in 2014. Though a Chinese-owned property, Musically had strong ties with the United States and garnered a substantial audience, which was key to its success. Its concept mirrored the one of the current TikTok, serving as a platform for creating and sharing short-duration audiovisual content. Later, in 2016, the prominent Chinese tech giant ByteDance introduced a similar entertainment service called Douyin. Within a year, it achieved a remarkable milestone of 100 million users in China and Thailand. Observing this immense popularity, ByteDance decided to expand under an enhanced brand name, TikTok. Thus, in 2018, ByteDance acquired Musically, assimilating its knowledge, data, and user base, and launched the new brand as TikTok.

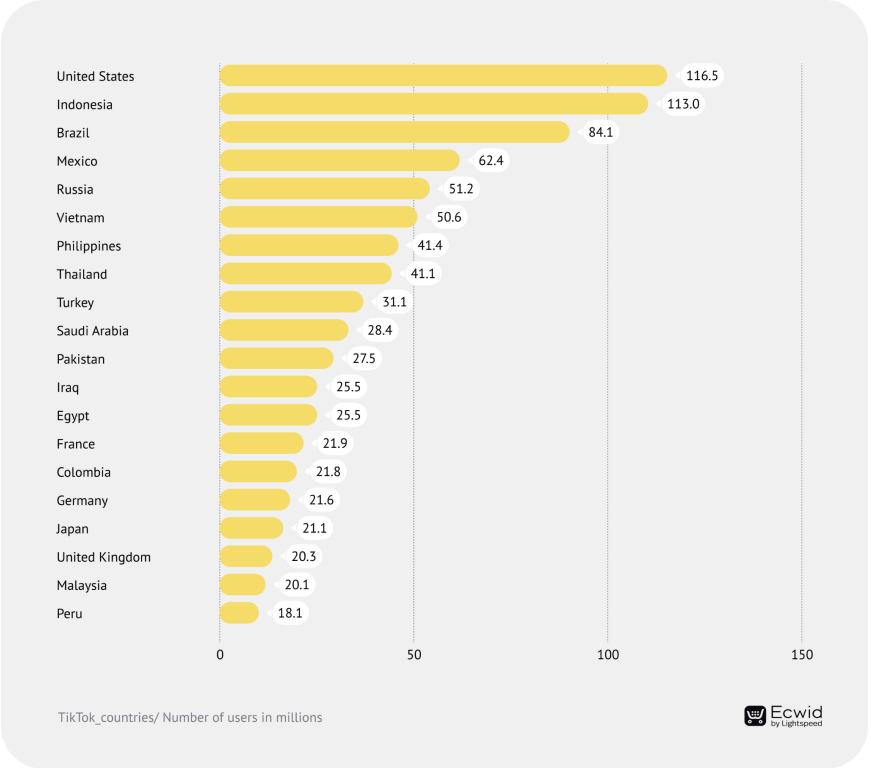
The Fame and Functioning of Tik Tok

A key aspect that makes TikTok so appealing to users is its use of an exceptionally powerful algorithm. This algorithm swiftly learns and adapts to each user's content preferences, far more rapidly than other similar applications. Users can choose from a vast array of song snippets and filters, all available for free. Most of the audiovisual content consumption occurs on the "For You Page," where the algorithm presents tailored content, anticipating the users' preferences based on their past views and searches. This page also features content that the algorithm predicts

could go viral, motivating users to create content in the hope that their videos might spread rapidly across the app, regardless of their number of followers.

TikTok has experienced one of the most rapid user growth rates in history, marking a significant shift in the social media and entertainment app industry due to the use of algorithms to enhance effectiveness.





The emergence of governmental concerns

The extraordinarily rapid growth of TikTok has raised concerns among capitalist politicians. The primary concern was spurred by the realization that a Chinese app was swiftly becoming an integral part of their populations' daily lives. There were also growing worries about the power this could give to the Chinese government, owning a company that, with a powerful algorithm, can compile private data from millions of users. Consequently, based on both factual and speculative arguments, there has been a solidifying belief in recent years that banning TikTok could mitigate potential threats to consumers and the governments of these countries.

Country and Block Positions

United States

In 2023, the administration of Joe Biden, President of the United States of America, issued a notice to ByteDance. They communicated that if the company was not sold, TikTok might face a ban in the U.S.A. due to data privacy and national security concerns. The White House also expressed support for draft legislation in the House of Representatives, which would grant the federal government the authority to regulate or ban technology produced by certain foreign countries, such as TikTok. Not waiting for these threats to materialize, the federal government and various states have already banned TikTok on government devices.

In conclusion, The United States' position, as reflected in the congressional scrutiny of TikTok and legislative actions, is one of concern over national security and data privacy, particularly regarding the potential for foreign espionage by China through the app. Furthermore, concurrently, the country is looking to renew Section 702 of the Foreign Intelligence Surveillance Act (FISA), which permits warrantless surveillance of non-U.S.

citizens abroad, indicating a dual approach of guarding against foreign threats while utilizing its own surveillance capabilities.

India

India's stance against TikTok became starkly evident in June 2020 when it banned the app alongside dozens of other Chinese applications following a border clash with China. The Indian government cited concerns over the sovereignty and integrity of the country, pointing to threats posed by these apps to its national security and defense. This move was part of a broader strategy to counteract perceived aggressions and to safeguard the personal data of its citizens from foreign surveillance and exploitation.

Australia

The Australian Information Commissioner is investigating allegations against TikTok regarding privacy breaches and unauthorized data scraping in Australia. These concerns include the use of a tracking tool, known as a pixel, to collect internet history and personal information from individuals, even those that had not installed the app. TikTok has countered these allegations, asserting that their use of pixels is in line with industry standards, voluntary for advertising clients, and compliant with Australian privacy laws. The company also highlighted that Australian user data is securely encrypted and stored in the United States and Singapore.

The Australian Federal Attorney-General Mark Dreyfus emphasized the importance of TikTok's cooperation with the inquiry, while the opposition expressed deep concerns about TikTok's data practices, especially given its connections to the Chinese Communist Party and China's intelligence laws. The case underscores broader issues of online privacy and the need for legislative reforms in Australia's Privacy Act expected in 2024, aiming to protect individuals against emerging technological threats.

Canada

Canada, too, raised alarms over the security of personal data collected by TikTok, leading to a ban of the app on government devices in February 2023. Canadian officials pointed to risks to privacy and security as the primary motivators for this decision, mirroring actions taken by other Western governments wary of the app's data handling practices and its compliance with local data protection laws.

Pakistan

Pakistan has intermittently banned TikTok, citing reasons related to immoral and indecent content. However, underlying these content-related concerns are broader issues of data privacy and security. Although the bans have been temporary, the ongoing scrutiny of TikTok in Pakistan puts an emphasis on the complex challenges the platform faces in balancing regulatory compliance with freedom of expression, alongside ensuring the protection of user data from potential misuse.

European Union

In response to the concerns over the security and privacy of user data, the European Commission, the executive arm of the EU, took decisive action in 2023 by banning TikTok from staff devices, citing cybersecurity concerns. This move, as reported by Reuters in February 2023 ("EU Commission bans TikTok from staff phones"), was a precautionary measure to protect against potential data breaches and unauthorized access to sensitive information. It highlighted the EU's proactive stance in addressing the risks posed by foreign-owned digital platforms to its internal cybersecurity posture.

Case Studies

TikTok's Hefty Fine for Child Data Privacy Violations in Europe

On September 15th 2023, TikTok was fined over 368 million dollars by European regulators for not adequately protecting children's personal information. The fine was imposed by the Data Protection Commission (DPC) in Ireland, which found that TikTok nudged users towards privacy-intrusive settings during account registration and video posting, particularly concerning because child users' profiles were set to public by default. These actions posed risks to children under 13 accessing the platform between July 31, 2020, and December 31, 2020. The DPC also highlighted issues with a family pairing setting that allowed non-child users to pair with child accounts and disable direct messaging limits.

TikTok disagreed with several aspects of the decision, particularly the fine's magnitude, stating that the investigated settings had already been changed and most issues addressed. TikTok has since made accounts for users aged 13-15 private by default and removed the option for any user to comment on videos created by 13-15-year-olds. Changes to family pairing features include screen time limits and content filtering tools. The DPC has ordered TikTok to comply with the rules within three months, and TikTok has committed to further strengthen protections for teenagers.

This incident follows TikTok's 2019 settlement of $5.7 million for violating the U.S.'s Children's Online Privacy Protection Act (COPPA), highlighting ongoing concerns about children's data privacy on the platform.

Timeline of Events

- **2016**

    - **September**: TikTok, known as Douyin in China, is launched by ByteDance for the Chinese market. The international version, TikTok, is launched later.
- **2018**
    - **May 25**: The European Union's General Data Protection Regulation (GDPR) comes into effect, setting a new standard for data protection and privacy, impacting tech companies globally, including TikTok.
- **2019**
    - **February:** TikTok pays a $5.7 million fine to the U.S. Federal Trade Commission (FTC) for illegally collecting personal information from children under 13, raising concerns about data privacy and protection on the platform.
- **2020**
    - **June:** India bans TikTok along with 58 other Chinese apps citing national security and data privacy concerns, marking one of the first significant bans against the platform.
    - **August:** Then-U.S. President Donald Trump signs an executive order to ban transactions with TikTok unless ByteDance divests its U.S. operations, citing national security concerns.
- **2021**
    - **June:** TikTok announces "Project Texas," a partnership with Oracle to store U.S. user data on domestic servers, aiming to address U.S. government concerns over data privacy and security.
- **2022**
    - **March:** Russia's invasion of Ukraine leads to increased scrutiny over TikTok and other social media platforms regarding the spread of misinformation and propaganda.
    - **December:** The U.S. Congress passes a spending bill that includes a provision banning TikTok from federal government devices, reflecting ongoing concerns over the platform's data security.

- **2023**
    - **February:** The European Commission bans TikTok on staff devices due to cybersecurity concerns, reflecting broader apprehensions within the EU regarding data privacy and security on social media platforms.
    - **March:** Canada announces a ban on TikTok from government-issued mobile devices, citing similar data security concerns.

Relevant UN Treaties and Resolutions

Universal Declaration of Human rights

The Universal Declaration of Human rights (UDHR) articulates fundamental human rights, including Article 12, which protects against arbitrary interference with one's privacy, family, home, or correspondence. This foundational document, while not legally binding, has influenced subsequent human rights treaties.

International Covenant on Civil and Political Rights

The International Covenant on Civil and Political Rights (ICCPR) is a key international treaty that obliges participating countries to respect the civil and political rights of individuals, including the right to privacy under Article 17. This provision is critical in the context of digital privacy and data protection.

Convention on the Rights of the Child

The Convention on the Rights of the Child (CRC) is the most widely ratified human rights treaty and addresses children's rights, with Articles 16 and 34 focusing on protecting children's privacy and safeguarding them from exploitation, pertinent to social media platforms' responsibilities.

United Nations Resolution on the Right to Privacy in the Digital Age

Adopted initially in 2013 and updated in subsequent years, this resolution calls on states to respect and protect privacy rights in the digital era, emphasizing concerns over mass surveillance and data protection.

Non-UN Treaties and Instruments

Budapest Convention on Cybercrime

As the first international treaty aiming to address Internet and computer crime, the Budapest Convention harmonizes national laws, improves investigative techniques, and facilitates cooperation among nations to combat cybercrime effectively.

General Data Protection Regulation

The General Data Protection Regulation (GDPR) is a comprehensive regulation by the European Union (EU) that sets stringent data protection and privacy standards for all individuals within the EU and the European Economic Area (EEA). It affects companies worldwide, dictating how they process and handle personal data.

Previous Attempts to Solve the Issue

Legislative and Executive Actions by Countries

Several countries, as previously mentioned, have taken national actions against TikTok, ranging from banning the app on government devices to outright bans. These actions are primarily motivated by concerns over

data privacy, national security, and the potential for foreign government surveillance.

TikTok's Efforts to Address Concerns

TikTok has made efforts to increase transparency and trust among its user base and governments. For example, the company initiated "Project Texas," a plan to store American users' data on servers managed by Oracle (an American multinational computer technology company), aiming to mitigate fears over data access by the Chinese government.

International Discussions on Digital Privacy and Security

On the international stage, discussions about digital privacy, data protection, and cybersecurity within forums such as the United Nations, the European Union, and other international bodies have indirectly addressed concerns relevant to TikTok and other social media platforms. While not aimed at TikTok specifically, these discussions contribute to shaping policies and regulations that impact how social media companies operate globally.

Regulatory Measures and Data Protection Laws

The implementation of stringent data protection regulations, such as the EU's General Data Protection Regulation (GDPR), sets high standards for personal data handling by tech companies, including social media platforms like TikTok. These laws aim to protect individuals' privacy and limit unauthorized data sharing, offering mechanisms to address potential abuses.

Public and Academic Scrutiny

Public discourse, academic research, and investigations by journalists have played a crucial role in highlighting the issues associated with TikTok and other social media platforms. This scrutiny has led to a better

understanding of the challenges and has pressured companies and governments to seek solutions.

Possible Solutions

In addressing the issue of TikTok's concerns about personal government abuse, a final resolution should aim at establishing a comprehensive framework that balances the safeguarding of digital privacy and personal data with the promotion of freedom of expression and innovation. This resolution should involve the coordination of UN member states, international organizations, tech companies, and civil society to ensure a multifaceted approach to digital governance that respects individual rights and state sovereignty. Before proposing specific clauses, delegates should consider the following questions to ensure the feasibility and effectiveness of the proposed solutions:

1. Has a similar approach been implemented in other contexts or with other platforms?
2. Has it been successful in enhancing data protection without stifling digital freedom?
3. Can we provide pragmatic examples of successful implementation?
4. Is the solution feasible across different political and legal systems?
5. Does it comply with the UN Charter, particularly concerning respect for national sovereignty and non-interference?
6. Does the solution respect the principle of state sovereignty while promoting international cooperation on digital privacy?

Considering these guidelines, possible solutions could be based on the following concepts:

- Development and Adoption of International Digital Privacy Standards: Encourage the drafting and adoption of a comprehensive set of international standards for digital privacy and data protection, akin to the GDPR, but with global applicability. These standards would aim to protect individuals' data from unauthorized use and

government surveillance, ensuring a balance between security and privacy.

- Implementing a Global Framework for Digital Platform Accountability: Propose a framework that holds digital platforms accountable for their data practices, including transparency in data collection, storage, and sharing. This framework could also include mechanisms for users to control their data and for independent audits of platform practices.

- Encouraging State Cooperation in Digital Education and Awareness Campaigns: Support initiatives that enhance public awareness and education on digital literacy, privacy rights, and safe internet usage. This could involve creating educational materials, conducting workshops, and launching campaigns that inform users about how their data is used and how to protect it.

- Promoting Research and Development in Privacy-Preserving Technologies: Advocate for increased investment in technologies that enhance privacy, such as encryption and secure data storage solutions. Encourage collaboration between states, academic institutions, and the private sector to advance these technologies.

As a friendly reminder, when drafting clauses and preparing for discussions, it is crucial to adopt a diplomatic and constructive stance that seeks to build consensus among UN member states and other stakeholders. An overly aggressive approach may hinder cooperation and lead to deadlocks. Therefore, we are expecting that delegates propose solutions that have a significant impact on enhancing digital privacy and security while aligning with the principles of the UN Charter and promoting international collaboration.

Bibliography

United Nations. (1948). *Universal Declaration of Human Rights*.

Office of the High Commissioner for Human Rights (OHCHR). (1966). *International Covenant on Civil and Political Rights*.

UNICEF. (1989). *Convention on the Rights of the Child*.

United Nations. (2013). *Resolution adopted by the General Assembly on 18 December 2013,*

Office of the High Commissioner for Human Rights (OHCHR). (2011). *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework*.

Council of Europe. (2001). *Budapest Convention on Cybercrime*.

European Commission. (2016). *General Data Protection Regulation (GDPR)*.

Australian Associated Press. (n.d.). *TikTok privacy breach allegations under spotlight*. Australian Associated Press.

Leonard, M. (2023, September 15). *TikTok fined over $368 million by European regulators for children's data privacy*.

Fouquet, H., & Nienaber, M. (2023, February 28). *European Parliament to ban TikTok from staff phones, EU official says*. Reuters.