The TikTok controversy: its impact on international security

Gloria Sicilia Lozano | Master in the Security Studies Program, Georgetown University, Fulbright Scholarship.

Theme

The potential impact of TikTok on Western security has raised concerns regarding data collection, algorithmic control and potential interference by the Chinese government. Although ByteDance, the parent company of TikTok, has proposed the establishment of local data centres, these measures do not effectively address the fundamental risks that leave European society susceptible to potential Chinese influence. In light of this evolving technological and geopolitical landscape, it is imperative for the EU to maintain unwavering commitment to protecting its citizens and its interests.

Summary

TikTok, the popular social media application, has sparked concerns due to its potential for compromising Western security. Claims have been made asserting that the Chinese government possesses the capability to use the app for data collection, exertion of algorithmic control and interference with personal devices. As a response to these concerns, ByteDance has put forward a proposal to store user data on European soil.

While this project aims to create a firewall with China, it fails to address the key vulnerabilities that expose TikTok users to potential interference by the Chinese Communist Party (CCP). Considering both technological and legal standpoints, it remains feasible for the Chinese government to retain access to user information and the content they are exposed to. Such a situation holds the potential to yield grave consequences for the sovereignty of EU countries.

To date, a total of 12 countries have fully or partially banned the use of this app. The primary reasons cited encompass concerns over national security, espionage, as well as infringements upon the data protection and privacy of their citizens and their administrations.

Within a landscape marked by growing foreign interference, disinformation campaigns, and geopolitical tensions, TikTok assumes the guise of a novel digital threat, capable of being weaponised for strategic objectives. As highlighted by both in the Strategic Compass for Security and Defence (2022) and the European Economic Security Strategy (2023), the EU must adapt to address the new technological and geopolitical realities. To achieve this, the EU must assert its leadership in data protection regulation, defending the privacy and security of its member states.

Analysis

Introduction

TikTok's resounding success positions the app as a key player in the information age. Beyond amassing a wealth of data that holds immense value and relevance for various entities and nations, the app also wields the power to shape the content encountered by its users. Furthermore, questions have arisen about the application's ability to compromise its users' devices. Consequently, apprehensions have emerged regarding the app's potential use by the CCP. Notably, Afghanistan, India and Pakistan have enforced nationwide bans on the app, while countries such as Belgium, Canada, Denmark, France, New Zealand, Norway, Sweden, Taiwan and the US have restricted its use among government officials.

To address these concerns, ByteDance, the parent company of TikTok, has put forth plans for the creation of localised data centres, Project Clover in Europe and Project Texas in the US. These data centres, located in Ireland and Norway for European data storage and in Texas for US data, will entail significant investments of €1.2 billion and €1.5 billion, respectively. The infrastructure will be managed by the software company Oracle, a strategic move aimed at fortifying security measures and introducing an added layer of control.

However, these facilities will only store legally 'protected data', leaving the remainder of users' information exposed. Consequently, a significant amount of data could continue to be collected and exploited in alignment with the interests of the Chinese government. The limited separation between the private sector and the CCP, coupled with China's Personal Information Protection Law of 2021, which grants the government access to personal and non-personal data held by domestic companies under the principles of national security, would still require ByteDance's compliance in the event of government requests, presenting a significant threat to TikTok users.

Moreover, the risk of CCP interference the content users are exposed to persists, thereby influencing their behaviour. Numerous studies have already documented the negative impact on mental health, especially among teenagers. Instances of intoxication, acts of violence and reckless conduct arising from viral challenges and trends have been widely reported, as has the proliferation of hate speech, which profoundly impacts society.

The US position

Amidst mounting concerns regarding potential threats to national security, the US persists in pressuring ByteDance to divest from TikTok or face the prospect of a nationwide ban. Boasting a user base of 113 million in the US, this is the second time TikTok encounters such a threat from the federal government. In 2020, then-President Trump attempted similar measures, but his efforts were blocked by the federal courts. However, the current Administration enjoys bipartisan support and the consensus of US lawmakers, who share apprehensions over potential CCP exploitation of the app. In fact, on this occasion, the White House also has the backing of the Federal Bureau of Investigation (FBI). Christopher Wray, Director of this agency, testified before the House Homeland Security Committee, declaring that the Chinese government could leverage

the collected data and exert control over recommendation algorithms and device software. Additionally, the Director of Cybersecurity at the National Security Agency (NSA), Rob Joyce, has expressed concern over TikTok's capacity to wield substantial societal influence. A congressional hearing on TikTok took place in March 2023, during which CEO Shou Zi Chew's testimony failed to convince the Committee regarding the app's security and independence.

The most fervent critics argue that the claim of the CCP using TikTok for espionage lacks supporting evidence. Moreover, they assert that a nationwide ban would constitute a clear violation of the First Amendment of the US Constitution. It should be noted that there are numerous applications, such as Meta and Google, that also collect large amounts of data, and in 2013 Edward Snowden exposed the collaboration between major tech companies and the US Government in accessing personal information of citizens. They also point out that TikTok generates an excessive amount of data, making its processing difficult. Additionally, they highlight that the main concern stems from the fact that TikTok, as the first non-Meta-owned application to achieve such remarkable prominence, belongs to a nation deemed an adversary.

While a nationwide ban on the app remains distant, several legislative proposals have been presented, aiming to endow the executive branch with new powers to prohibit foreign technologies associated with countries deemed adversarial and posing a threat to national security. Among these proposals, the Restriction of Emerging Threats That Endanger Information and Communications Technology (RESTRICT) Act stands as the most significant, garnering support from a bipartisan group of senators and receiving endorsement from the White House. If enacted, this legislation would empower the Department of Commerce to review any foreign technology deemed a risk to national security. Reactions to this proposal have varied from support to concerns regarding the potential concentration of excessive power within the executive branch. Regardless, this development underscores a new era marked by heightened resolve in foreign policy vis-à-vis China.

It is evident that both the Democratic and Republican parties have aligned their positions on this matter. This growing consensus arises from the Republican Party's view of China as a clear adversary, which increasingly aligns with the Democratic Party's acknowledgment that, despite internal divisions, China represents both competition and a challenge to the international order. Secretary of State Antony J. Blinken affirmed this stance in a 2022 statement from the Department of State, and it is further reflected in the Biden Administration's newly adopted strategy known as 'Invest, Align, and Compete'. This strategy adopts an increasingly assertive stance across economic, military, diplomatic, and technological domains.

However, the economic consequences that may result from the measures adopted by the Biden Administration, some being a continuation of the previous government, remain uncertain. On one hand, the Tax Foundation has estimated that the decoupling of the US and Chinese economies could lead to a US$55.7 billion decrease in GDP and the loss of 173,000 jobs. On the other hand, the White House has reiterated, both through National Security Advisor Jake Sullivan and in the G7 Statement in Hiroshima, that its

goal is to de-risk and diversify in order to increase security and resilience, with decoupling being pursued only in specific sectors deemed critical to national security.

The EU position

In February 2023 the EU followed in the footsteps of the US and banned the use of TikTok. With a user base of 150 million in Europe, this ban applies to devices registered with European institutions, including the European Commission, the Council of the EU, the European Parliament, the European External Action Service and the European Court of Auditors. This measure, described as necessary for data protection without explicitly referring to the CCP, affects both professional and personal devices hosting EU applications. Beyond this, the EU has not announced any further steps towards a complete prohibition of the application.

The US has been demanding that the EU establishes a coherent strategy regarding China. While some EU member states and officials have taken a firmer stance against China, others have remained neutral, distancing themselves from the US discourse, as demonstrated by French President Emmanuel Macron during his last official visit to the PRC.

Nevertheless, in recent years, the EU has established various mechanisms to regulate data protection, combat misinformation and address the challenges posed by emerging technologies.

The EU currently operates under a robust regulatory framework, spearheaded by the General Data Protection Regulation (GDPR) enacted in 2016. This comprehensive framework already encompasses rules and mechanisms to govern the handling of data by organisations, both within and outside the EU. Of particular relevance to TikTok are the specific provisions pertaining to underage users, considering their substantial presence on the platform, the transparency standards in data processing, necessitating the completion of a Data Protection Impact Assessment (DPIA), and the strict requirements in the case of international transfers of European data. The GDPR demands the disclosure of the types of data collected, the purpose of processing, the recipients of the data and any potential international data transfers. Importantly, recipient countries are expected to offer an adequate level of protection or implement appropriate safeguards in line with the GDPR's provisions.

Published in 2022 the Digital Services Act (DSA) seeks to foster a secure digital environment and introduces the requirement for large platforms with over 45 million users, such as TikTok, to conduct annual risk assessments. Building upon the DSA, the EU released a list of 19 digital platforms in April 2023, including TikTok, subjecting them to enhanced scrutiny and annual audits commencing from August of the same year when the law comes into effect.

The Digital Services Act (DSA) published in 2022, aims to ensure a safe digital space and establish the conducting of annual risk assessments for large platforms with over 45 million users, such as TikTok. In April 2023, the EU published, under the DSA, a list of

19 digital platforms, including TikTok, which must undergo stricter controls and annual audits starting from August of this year when the law comes into effect.

Furthermore, the EU's 2022 Code of Practice on Disinformation serves as a critical instrument in the battle against disinformation, setting forth a framework comprising 44 commitments and 128 specific measures. TikTok has faced accusations of content censorship related to human rights issues in China, including the Xinjiang internment camps and the Uighur genocide. Additionally, a report released by NewsGuard in 2022 revealed instances of misinformation dissemination through TikTok's search engine, directly contradicting the principles outlined in the aforementioned code.

In May 2023 the fourth EU-US Trade and Technology Council (TTC) ministerial meeting was held, placing emphasis on the regulation of emerging technologies, the defence of human rights and the preservation of democratic values in a changing digital environment. Consequently, the TTC has dedicated specific sections to highlight the significance of transparent and accountable digital platforms, with a focus on protecting minors and addressing the menace of Foreign Information Manipulation and Interference (FIMI) against European principles. Both the EU and the US strive to make progress towards establishing a shared framework for the identification and mitigation of FIMI activities.

Most recently, the European Economic Security Strategy, presented in June 2023, seeks to strengthen the EU's economic security amidst emerging geopolitical and technological complexities. This strategy includes measures aimed at protecting critical infrastructure –both in the physical and cyber realms– mitigating risks associated with dual-use technologies, countering economic coercion by third countries and fortifying the EU's Single Intelligence Analysis Capacity (SIAC) for threat detection. Additionally, the development of the STEP platform is underway to mitigate strategic dependencies in the technological domain.

Recommendations

In the face of growing political tensions, the EU is recalibrating its stance on China. Despite existing differences among member states, recent EU actions indicate a greater sense of unity and cohesion in its approach to foreign policy and collective security. The EU's High Representative, Josep Borrell, has noted nuanced disparities in how to engage with the CCP, allowing for a reassessment of EU policy on this front. On one hand, the EU published the Strategic Compass for Security and Defence in March 2022, classifying China as a 'partner for cooperation, economic competitor, and systemic rival'. This recognition acknowledges China's capacity to disrupt the international order, challenge our interests and undermine our values. On the other hand, the EU's actions in recent years, as outlined in the preceding section, primarily target both Russia and China, albeit without explicit mention, as highlighted by European Commission President Ursula von der Leyen.

In light of TikTok and the Clover Project, it is imperative to rigorously enforce our legislation. To mitigate the risks associated with the penetration of new technologies, especially those from systemic rivals, the EU should pursue three main lines of action.

First, a comprehensive analysis of the app and its possible backdoors is necessary. This analysis should be entrusted to a reputable and independent public or private institution, including a declassified report that would serve as a negotiating tool with ByteDance. Moreover, a conclusive report would enable the European Data Protection Board (EDPB) to evaluate TikTok's adherence to GDPR and the DSA, as well as the principles enshrined in strategic documents published in recent years. These measures are essential to ensure TikTok's compliance with security standards and to safeguard the interests of its users. Furthermore, considering additional safeguards such as periodic audits or enhanced monitoring mechanisms can be contemplated to ensure ongoing compliance with regulations. If required, exploring potential updates or amendments that specifically address the challenges posed by TikTok and similar applications should also be considered.

Secondly, it would be necessary, although redundant, for TikTok to sign an agreement with EU authorities explicitly acknowledging that EU legislation supersedes any commitments made by TikTok, including those involving the Chinese government. Under no circumstances should TikTok transmit the data of European citizens, whether protected or unprotected, to third parties.

Thirdly, given the potential impact on Western security, it is recommended that the EU establish collaborations with intelligence and security agencies to obtain insights and guidance regarding potential threats associated with TikTok in this realm. Agencies such as Europol, the European Union Agency for Cybersecurity (ENISA), and the EU Intelligence and Situation Centre (EU INTCEN) could assume an increasingly prominent and pivotal role in actively monitoring TikTok's operations and identifying potential risks.

Conclusion

The EU must be fully aware of its current dependence on the US and China, as all major technology companies are predominantly based in these countries. Given Europe's substantial economic, demographic and technological-industrial influence, it finds itself in a critical juncture where securing global technology leaders on its own soil becomes imperative. This may necessitate tempering competition policies that have traditionally prevailed, thereby facilitating the development and establishment of such leading companies. Conversely, the EU should actively encourage diversification and provide increased support to European companies, presenting them as safer alternatives in line with its strategic objectives. Neglecting this imperative would amount to disregarding our own future and surrendering to irrelevance. Therefore, it is vital for the EU to take concrete measures to promote and attract the establishment of such companies within its borders, thereby contributing to their growth and enabling the attainment of robust technological autonomy on the global stage. These efforts will concurrently reduce reliance on foreign platforms and mitigate associated risks.