RESEARCH ARTICLE

European Journal of Communication and Media Studies
www.ej-media.org

TikTok's Conflict of Interest with the US Government: Between Big Data Security and Economics (2017-2023)

Mansur Juned, Siti Maryam, Syahrul Salam, and Rahmadini Agung Ayu Utami

ABSTRACT

State capabilities in securing cyberspace will determine national security in the real world because cyber data is related to conventional information. This condition makes cybersecurity a complex domain because of its virtual nature, but it can impact aspects in real space. This complexity is also because all parties can access cyber, causing conflicts such as competition for big data interests. This study aims to determine the dispute between TikTok and the United States government over the security of its users' data, especially users from the United States. The United States accuses TikTok of misusing US user data for Chinese intelligence. However, TikTok has denied the allegations. The qualitative method used in this research is based on data collection techniques through a literature study with secondary data support. As a result, TikTok requires user data for product and service development purposes. While the United States is more than that, big data users are a national asset determining their global economic position. There is no hard evidence to suggest that TikTok provided the Chinese government with the data of users from the United States. This paper also views the US government's interest as an extension of the local private sector. This view is based on the finding that TikTok's profits and popularity are far above their all-American competitors.

Keywords: Big data, economy, geopolitics, TikTok, United States.

Published Online: September 04, 2023

ISSN: 2736-5522

DOI: 10.24018/ejsocial.2023.2.4.23

M. Juned*
University of Pembangunan National Veteran Jakarta, Indonesia.
(e-mail: mansurjuned@upnvj.ac.id)
S. Maryam
University of Pembangunan National Veteran Jakarta, Indonesia.
(e-mail: sitimaryam@upnvj.ac.id)
S. Salam
University of Pembangunan National Veteran Jakarta, Indonesia.
(e-mail: syahrulsalam@upnvj.ac.id)
R. A. A. Utami
University of Pembangunan National Veteran Jakarta, Indonesia.
(e-mail: rahmadiniaau@upnvj.ac.id)

Corresponding Author

I. INTRODUCTION

The rapid development of the cyber world also affects the study of IR. Cyber studies in IR now play an equally important role as conventional social science studies. The vastness of space and the ease of access to cyberspace allow actors in the conventional realm to engage in the cyber realm. The ability of states to secure the cyber realm will determine their national security in the real world because it is related to conventional information.

Cybersecurity is the management of techniques to safeguard the integrity of networks, programs, and data from unauthorized access to protect users or organizations in cyberspace (Seemma *et al.*, 2018). According to the International Telecommunication Union, cybersecurity seeks to ensure the attainment and maintenance of security properties of organizations and user assets against cybersecurity risks. General cybersecurity objectives include availability, integrity (encompassing authenticity and non-repudiation), and confidentiality (Seemma *et al.*, 2018).

The object of securitization in cybersecurity also includes intangible elements, such as the protection of social values, and tangible elements, such as the security of the national infrastructure. This condition makes cybersecurity a complex domain because of its virtual nature, but it can impact aspects in real space. In addition, cybersecurity issues can also have consequences on other aspects, such as ethical consequences related to economic losses due to data theft, physical losses as when critical physical systems are breached, such as power grids, and violations of privacy rights (Christen *et al.*, 2017).

The very open cyber world has provided opportunities for non-state actors to play a more active role in public policy than in the conventional world. The false territorial boundaries in cyberspace also increase the potential for conflict between actors because all parties have the same rights to freedom of information in cyberspace. One of the cyber conflicts that often occur is data security issues. The era of digitalization has made data appear as an essential asset in natural resources (Picciano, 2014). Data is now a contested asset due to its wide range of uses, creating the concept of big data.

Big data is large and complex data, and its processing cannot be done by conventional techniques (Maryanto, 2017). The big data characteristics are large size (volume), processing speed in line with the rapid growth of data (velocity), diverse data from structured to unstructured (variety), data certainty (veracity), and the value of data benefits (value) (Islah, 2018). Big data can be a source of information that supports company development, monitors political support distribution, and facilitates public administration organization. Big data is proliferating along with the increasing digital economy needs. The digital economy significantly impacts the country's economic growth (Zhang *et al.*, 2022) and affects the country's performance towards small and medium enterprises. The development of the digital economy also has a further impact on changes in consumer preferences and interests.

A cybersecurity conflict related to big data interests has occurred recently between the United States government and the well-known Chinese application TikTok.On August 6, 2020, President Donald Trump issued Executive Order 13942 to prohibit transaction activities through the TikTok and WeChat applications. This Executive Order was later granted on September 18, 2020, by the United States Department of Commerce. Through the FBI and the Federal Communications Commission, the United States government stated that TikTok is an application that is dangerous to the security of its users' data. Both mentioned that TikTok's parent company, ByteDance, could share TikTok user data, such as browsing history, location, and biometric identifiers, with the Chinese authoritarian government (Chan & Hadero, 2023). This allegation is based on the implementation of the Cyber Security Law in China since 2017. The national law mandates all Chinese companies to hand over all relevant personal data to the Chinese central government for national security purposes.

TikTok is the most popular entertainment-based social media app in the world today. TikTok has rapidly increased users in the United States over the past two years. When compared to its competitors, TikTok has the advantage of offering several easy access and other more exciting features. However, this ease of access is considered an opening for the United States government for cybercrime.

The conflict between app company TikTok and the United States government is the tip of the competing interests over control of big data related to public personal data. In today's information age, data is a commodity that sustains human life. Many aspects of life depend on the internet, so data is now a valuable asset. The practical value of the data has led to technological innovation, where personal data supports the performance of cyber technology. Users who share their personal data with Internet services, such as social media or search engines, will benefit from more optimized services. The data provided will help the machine process the user's activities on the internet, so they will find it easier to get what they are looking for. On the other hand, this study also looks at the enormous benefits TikTok has gained from its popularity, which has led to digital economy competition with other competing applications from America, such as Facebook and Instagram.

Using personal data for the convenience of online activities has resulted in challenges for the security of users' personal data. One such challenge is the international transfer of data. According to Romanosky, transferring users' data can be done anywhere if the personal data is adequate (Romanosky *et al.*, 2023). The issue of transferring personal data is also related to how application service providers regulate the access control of users' data. Puspa *et al.* (2020) argue that this problem can be handled by providing control settings for who can see users' personal data and what data can be seen. This can lead to consumer trust as they feel safe when sharing information.

The development of application technology based on artificial intelligence (AI) improves social media performance, such as TikTok. The ease of use of the application site is obtained from the personal data that users share. According to Fitria (Halim *et al.*, 2022; Nasution *et al.*, 2022), the factors of convenience, comfort, fun, feature facilities, security, privacy, and efficiency offered by TikTok have a positive effect on the intention of its users to use the application.

However, from a national security aspect, TikTok is seen as threatening the domestic national security of the United States. TikTok is considered dangerous, not only for the safety of its users but on a broader scale, namely national security. The United States government addressed the possible threat by drafting legislation aimed at protecting national, foreign policy, and economic interests that may be jeopardized by the possible collection and theft of TikTok user data by the Chinese government through the National Intelligence Service (Indrayani & Maharani, 2022).

Based on this background, this paper will discuss the conflict of interest between TikTok and the United States government in the cyber domain. Both are policymakers who have their views on data security. This paper argues that big data is a national asset that determines the status quo of the United States in the global economy. It also views the US government's interests as an extension of the local private sector. This view is based on the finding that TikTok's profits and popularity are far above all their competing apps. The concepts used are cybersecurity and digital economy to examine how these two actors understand data security based on their respective interests.

II. METHOD

This research uses qualitative methods, an approach that aims to explore and understand the meaning of individuals or groups related to social issues (Creswell & Poth, 2018). The research data will be narrowed down to big data, cybersecurity, TikTok, and US government policies obtained based on literature study techniques. The data sources used are primary data in the form of official United States government documents and secondary data such as books, scientific journals, news articles, official government documents, and research reports.

III. TikTok

TikTok is a technology subsidiary of ByteDance headquartered in Beijing with branch headquarters in Los Angeles and Singapore and offices in New York, London, Dublin, Paris, Berlin, Dubai, Jakarta, Seoul, and Tokyo. As its main feature, TikTok specializes in short videos lasting from 3 seconds to 10 minutes. This feature sets TikTok apart from other social media, making it a short video-based social media services pioneer.

The TikTok app's development mission is to spread the creativity of its users to bring happiness (TikTok, n.d.). Combining the task with the unique main display in short videos has successfully brought TikTok to market popularity. Based on the results of the Business of Apps survey (Halim *et al.*, 2022), TikTok was the most popular application in 2022. The second to fourth positions are filled by Meta apps, namely Instagram, Facebook, and WhatsApp, and the last position is CapCut, which is still affiliated with TikTok. TikTok has rapidly increased users in the United States over the past two years. This trend has made TikTok the most popular app, with 99 million downloads.

Apps developed by Chinese companies have characteristics that make them superior to Western apps. They are considered successful in monopolizing various features by packaging them in one application to make them more practical for their users. TikTok also applies this innovation. This application facilitates its users to be creative through short videos, enjoy entertainment, interact with other users, and trade simultaneously.

TikTok has a feature called For Your Page (FYP). FYP is a system of algorithms that supports curation on TikTok displays so that users can connect to content that matches their interests. The FYP algorithm has made TikTok users feel comfortable spending time on the application compared to other applications, such as Instagram (Stokel, 2023).

The next advantage is that TikTok is also more accessible than other applications. The FYP algorithm allows TikTok users to access the app without creating an account. FYP can work by detecting the account settings and devices used by users. This technology allows TikTok users who do not have an account to enjoy viewing short videos that match their interests without registering first.

TikTok's features make it one of the most popular social-commerce apps today. The FYP feature helps buyers easily find items they might like and helps sellers find buyers. Another digital economic activity is that TikTok provides a gift feature, a gift from the audience to an account that is live streaming, and the gift can be cashed in.

The explanation above shows that the algorithm is crucial for TikTok's current advantage. TikTok's algorithm allows users to connect to content that matches their interests without following the accounts directly. This technology has successfully made TikTok users more effective and efficient, saving them time and giving them more internet satisfaction than its predecessor, Instagram. TikTok can display changing content in real time, even if the user is just passively scrolling the screen. TikTok's algorithm system is called the interest graph. Whereas Instagram works based on the social graph. This system displays ad suggestions based on the assumption that the user has the same interests and purchasing behavior as other users connected to them (Stokel, 2023).

Algorithms are the primary way social networks attract and keep us paying attention. However, despite its advantages, the algorithm technology is viewed negatively because it jeopardizes users' data. TikTok collects user information such as name, age, and language. It also includes location data, data from the clipboard, contact information, site tracking, and all the data its users upload and the messages they send through the app (Jacobson, 2023). This information drives TikTok's algorithm. This concern extends to the national security level because the user data was suspected to be provided to the Chinese government. The United States feared that the Chinese communist government was forcing ByteDance to hand over their user data, including sensitive data, from US citizens (McDonald & Soo, 2023). However, TikTok CEO Shou Zi Chew denied the allegations. He said his company has never given or received a request to hand over US users to the Chinese government and would not honor it if such a request were made (Shepardson, 2023). This conflict shows that cyberspace is becoming a new arena for competing interests between multinational corporations and states.

IV. US GOVERNMENT POLICY ON TIKTOK

In November 2017, ByteDance, the parent company of TikTok, acquired an ownership stake in the entertainment app Musical.ly. Musical.ly is an entertainment social media company launched in 2014 and headquartered in Shanghai. The founders of Musical.ly are Chinese programmers Alex Zhu and Luyu Yang. Musical.ly is one of the few apps originating from China that has gained popularity in the United States. After the successful acquisition, ByteDance merged Musical.ly with TikTok in 2018.

One year later, US lawmakers issued an order to investigate TikTok for a national security investigation. According to the Commission on Foreign Investment in the United States (CFIUS) review report, TikTok's acquisition of Musical.ly did not pass CFIUS clearance (Roumeliotis *et al*., 2019). CFIUS is an authority tasked with reviewing potential national security risks in various deal processes by foreign parties acquiring US companies. The CFIUS investigation was based on concerns that TikTok would implement censorship of sensitive content, particularly politically. In addition, CFIUS also questioned how TikTok manages the storage of its users' data.

The then President of the United States, Donald Trump, issued a mandate entitled "Executive Order on Addressing the Threat Posed by TikTok." In the order, Trump declared a national communication and information technology emergency. Trump ordered to take further action against the TikTok app. TikTok is asked to find a new owner by finding an American company willing to buy part of their shares; the goal is to prevent ByteDance from becoming the primary owner within 45 days of the mandate being issued. If TikTok cannot fulfill the request, an alternative last resort is to close its offices in the United States within the same period.

Trump claims this direction was decided because the spread of applications developed and owned by Chinese companies is considered to continue to threaten the national security, foreign policy, and economy of the United States. In addition to concerns about the security of Americans' personal information, TikTok is also suspected of potentially providing access for the Chinese Communist Party to track the location of US Federal employees and contractors, create personal information documents for extortion, and conduct espionage against local companies.

Trump also received reports that TikTok censored some content relating to protests in Hong Kong and the treatment of ethnic Uyghurs and other Muslim minorities. It is also suspected that the TikTok app could be used for disinformation propaganda campaigns that benefit the Chinese Communist Party, such as untrue conspiracy theories about the origins of the COVID-19 virus. So, to prevent espionage, Trump banned US Federal officials from using TikTok (Trump, 2020).

Microsoft and Walmart had joined forces to negotiate jointly with TikTok over the issue of TikTok share ownership. The negotiations culminated in Oracle and Walmart as the US companies proposing to purchase the shares. Business-wise, Walmart is more favorable to TikTok because it has e-commerce features as its advantage to help TikTok Shop's social-commerce grow. Meanwhile, Oracle is a company that provides cloud storage services. Oracle Cloud has been ByteDance's data center since 2021 and is based in the United States and Singapore (TikTok, n.d.).

Trump's exclusive mandate could not be implemented to its fullest extent as he stumbled into a political case and failed to run for president of the United States in his second term. The planned share purchases by Walmart and Oracle have been postponed indefinitely. The change in the president of the United States made the newly elected president, Joe Biden, have to review the exclusive orders issued by the previous leader so that the share purchase negotiation process had to be stopped.

Under Biden's leadership, the United States changed its policy towards TikTok. Joe Biden halted legal proceedings to stop TikTok from operating in the United States. Instead, the US Department of Commerce reviewed various apps' design and development systems based in hostile countries, including China (BBC, 2021).

On June 9, 2021, Joe Biden signed an executive order lifting the ban on 10 Chinese app companies operating in the United States, including TikTok (Sorongan, 2021). The document, titled "Executive Order on Protecting Americans' Sensitive Data from Foreign Adversaries," outlined alternative actions the United States could take to review the Chinese companies. Biden replaced the explicit mention of the brands of the apps in question with the term "software applications originating from the jurisdiction of adversary countries" (The White House, 2021, p. 1). Biden also believes an evidence-based approach is needed to ensure these apps pose a latent cybersecurity danger to the United States.

In reviewing these applications, there are several criteria that serve as indicators for consideration of the presence of potential risks, including: ownership, control, or management by persons supporting the military, intelligence, or proliferation activities of a foreign adversary; use of connected software applications to conduct surveillance that enables espionage, including through a foreign adversary's access to sensitive or classified government or business information, or sensitive personal data; ownership, control, or management of connected software applications by persons subject to coercion or co-optation by a foreign adversary; suitable, control, or management of connected software applications by persons engaged in malicious cyber activities; the lack of thorough and reliable third-party audits of connected software applications; the scope and sensitivity of the data collected; the number and sensitivity of users of connected software applications; and the extent to which identified risks have been or can be addressed by independently verifiable measures (Biden, 2021).

On December 13, 2022, Senator Marco Rubio and US lawmakers Mike Gallagher and Raja Krishnamoorthi introduced a new bill to ban TikTok and ByteDance from operating in the United States (Feiner, 2022). The bill is called "The Averting the National Threat of Internet Surveillance, Oppressive Censorship and Influence, and Algorithmic Learning by the Chinese Communist Party Act" or the ANTI-SOCIAL CCP Act. The bill states that the legislation is designed to protect Americans from threats from certain foreign adversaries who use social media companies to surveil Americans, learn sensitive data about Americans, or spread influence campaigns, propaganda, and censorship. The bill defines terms such as "entity of concern" and lists criteria that indicate that a foreign social media platform is overly subject to the control of a hostile foreign government. The bill also contains a broader scope than the previous leader's order that specifically mentioned the TikTok app brand and Chinese state entities. The hostile state entities of concern in this bill are not just limited to China but also include other countries that practice ideologies contrary to the United States, such as Russia, Venezuela, Cuba, and North Korea (Sherman, 2022).

The bill is still under discussion and has yet to be authorized by President Joe Biden. In the Senate, the CCP Anti-SOCIAL Bill has majority support, signaling that the bill is likely to be approved. The Chinese hot air balloon case, suspected of being a tool for espionage activities against US residents, is considered a consideration that passed the CCP Anti-SOCIAL Bill to be accepted by Biden.

V. Discussion

Cybersecurity must go beyond protecting the information or information system resources of a person or organization. Cyber security is also about protecting all users who utilize resources in the cyber environment and protecting any other assets, including those of society at large, that are exposed to risk due to vulnerabilities stemming from the use of technology. Cybersecurity is increasingly critical due to the increasing reliance on computer systems, including smartphones, televisions, and the various small devices that make up the Internet of Things.

The issue between TikTok and the United States is a conflict of interest between multinational companies and the state. There is a difference of interest between the cybersecurity of the state and private companies. States allocate more cybersecurity for administrative purposes, while private companies focus on allocating software development and testing (Romanosky *et al.*, 2023).

In addition, the author also sees private interests in the legal action against TikTok. Musical.ly is one of the few apps originating from China that has become popular in the United States. Musical.ly is the only Chinese social media company with an extensive network outside China (Carson, 2016). The fact that the company that acquired Musical.ly, ByteDance, is a start-up shows China's business power is in a golden age. China can position its products as a giant in the global market even though geopolitical tensions with the United States are heating up. This phenomenon is a new challenge for the United States in maintaining its status quo (Yu, 2022).

TikTok's technological superiority has also allowed its growth to exceed the sales of Western entertainment social media apps in the global market. This growth rate is not only based on sales involving the number of users but also in terms of less time cost. TikTok has quickly gained popularity over Instagram and Facebook in under three years since its launch into the international market. The time users spend playing TikTok in a day is also longer than Instagram and Facebook (He *et al.*, 2021, p. 679).

These advantages show that TikTok is a software application that can solve the problems faced by users in social media so that it can meet their needs. The activities of social media users are based on the motivation of specific needs such as leisure, interactive social, self-expression, economic benefits, and care. When a social media application service can meet all these needs, users feel comfortable and satisfied. In addition, the FYP system in TikTok also has the advantage of filtering the information users desire based on their favorite preferences. The idea results from TikTok's innovation in studying the content homogeneity system. Western social media makes the appearance of limited and passive interaction between users. TikTok developed this innovation using a personalization system.

The FYP system isolates TikTok users in an algorithm that spoils them with homogeneous or similar information. However, at the same time, users are also still receiving trending information that is happening around them without the need to try more. Another advantage of TikTok is that it makes the phone a walking studio. Previously, no social media application accommodated the creativity of young people in the field of dance. TikTok is the first app to make such a breakthrough (Xu *et al.*, 2019).

To meet users' needs, TikTok innovates by utilizing information from users, such as social media features such as search fields, hashtags, like and dislike buttons, comment fields, and sharing buttons to discover the trends of information users want to consume. The information collected by TikTok also becomes a set of knowledge for TikTok's algorithm to generate information shared with other users as a sign that the information is in vogue with their social media contacts, even if they do not want the information on their page. It is this process that the United States finds problematic. From a business perspective, TikTok is interested in detecting all necessary forms of user activity to develop its service features. As a company, its orientation is to secure consumer trust. Developing their cyber tools is aimed at securing the company's valuable assets, and user data is one of them. TikTok recognizes that their concept's creativity and expression must be protected, as well as privacy. Using an app also means giving trust to the app provider. As such, TikTok provides open access to its software security mechanisms and strives to educate its users through transparency.

In terms of privacy, the information collected by TikTok aims to provide valuable and relevant experiences for its users. TikTok also requests that users read the provisions of the privacy rules to be aware of their mechanisms. Information requested by TikTok includes phone numbers; birthdays; addresses; payment information; likes, shares, search history; device type and ID; and location. The purpose of its use accompanies all of this information. TikTok also mentions that their device encryption keys are stored in a management system operated by a security team based in the United States (TikTok, 2021). To build user trust, TikTok offers a provision allowing users to copy their data anytime. This includes profile information, activity, and app settings. TikTok works with HackerOne to protect its devices from the risk of cyberattacks.

The mechanism of using user data by TikTok is an example of the utilization of big data by the business and technology world. In the Internet of Things era, big data is used as a sophisticated process that improves the performance of business and technology companies to map the direction of their business more precisely. The big data processing process aims so that every business, organization, and individual who uses it can benefit through insight related to decision-making and appropriate action. TikTok implements this process by collecting their users' personal data (Pujianto *et al.*, 2018). User personal data is big data that contains detailed user information so that the FYP algorithm system can make decisions to display impressions that match user interests.

TikTok has emphasized that it has never provided or received a request to share the personal data of users originating from the United States with the Chinese government (Aljazeera, 2023). Nor would TikTok honor such a request. Similarly, the Chinese government has denied the US allegations, saying it has never and will never request data from TikTok's American users (Tan, 2023).

TikTok's policy of requesting users' personal data is a form of tech companies' interest in the cyber domain. Private companies invest in developing secure infrastructure. They prioritize shareholders and consumers and do as much research as possible to meet their needs (Khaniejo & Sinha, 2018). TikTok's personal data request policy is reasonable from a business perspective. Consumers using digital technologies provide opportunities for companies to increase consumer engagement and the responsibility to protect their data. Personal data collected from users is valuable to help companies understand consumer problems and discover unmet needs. Thus, companies can develop products and services and filter advertisements to make them more personalized and in line with consumers' interests (Anant *et al.*, 2020).

There is no solid evidence of data theft of US TikTok users by the Chinese government (Allyn, 2023). TikTok is open about the storage of their users' personal data. They state that user data is stored in storage locations located in the United States and Singapore, and plan to open a data center in Ireland (TikTok, 2021)

The United States government still views TikTok as a national security threat. Discussions on Restricting the Emergence of Security Threats, the Risk Information and Communications Technology Act (RESTRICT Act), or Senate Bill 686 are ongoing. The RESTRICT Act would provide a legal basis for the US commerce ministry to monitor the flow of transactions and information of foreign technology companies originating from hostile countries that could pose security concerns for the national security of the United States or its citizens.

TikTok's threat to US national security is not only related to the security of American users' personal data but also includes threats to the national economy and geopolitics. The US government has asked TikTok to divest ByteDance or face severe sanctions and a ban on operations (Allyn, 2023). This move is related to the US government's interest in controlling the big data of its users. The data property is an inevitable trend in international development (Niu & Hong, 2021).

Conflicts of interest between China and the US today, mainly since China's economic rise, generally focus on how the two countries can protect each other's primary power sources, such as companies and people. Their conflict is also inseparable from the control of cyberspace, such as the digital economy, changes in domestic political perspectives on cyberspace, big data, technological advances, and trade wars that have occurred in recent years. In this condition, the involvement of multinational private companies plays a vital role in the conflict because of the company's significant contribution to the domestic economy (Juned *et al.*, 2022). The big data phenomenon has led to a trend where intelligence operators worldwide collect ordinary data en masse and use algorithms to weed out the data. Such capabilities allow modern private companies to collect consumer behavior data and exploit it into profitable value. As a result, communications today have significant economic value.

National security adjusts state laws and bureaucracies in response to rapid technological and geopolitical developments. These developments relate to the explosion of personal data processing and transfer that now underpins much of the global economy. Foreign competitors, especially China, have begun to target the US economy through cyberspace. Rapid developments make it difficult for the government to respond quickly to potential problems with data exports (Horowitz & Check, 2022). US policymakers adopted the RESTRICT Act to protect their strategic position in the market and industry (Gray, 2021).

VI. Conclusion

TikTok and the United States have different interests in using users' big data. As a technology company, TikTok needs its users' personal data for product development and customer satisfaction. Meanwhile, the United States government is interested in maintaining the privacy of its citizens' data and national security. The conflict between TikTok and the United States is a competition that goes beyond the cyber domain. The conflict also extends to geopolitics and economic interests. However, when looking at the position of the US government as a policy maker, this paper views the US government's interests as an extension of the local private sector. This view is based on the finding that TikTok's profits and popularity are far above their all-American competitors.

Although there is no hard evidence that TikTok doubles as Chinese intelligence, the United States still considers TikTok dangerous. Government agencies need help to keep up with the ability of technology companies to keep pace with the rapid data growth. Today, data has significant strategic value and plays a vital role in the global economy. TikTok's popularity rivals US products, which could improve China's economy.

References

Aljazeera. (2023). *TikTok CEO to tell legislators app 'never shared' data with China*. https://www.aljazeera.com/economy/2023/3/22/tiktok-ceo-to-tell-legislators-app-never-shared-data-with-china.

Allyn, B. (2023, March 23). *TikTok CEO says company is "not an agent of China or any other country."* NPR. https://www.npr.org/2023/03/21/1165210054/tiktok-ceo-to-lawmakers-americans-data-not-at-risk.

Anant, V., Donchak, L., Kaplan, J., & Soller, H. (2020, April 27). *The consumer-data opportunity and the privacy imperative*. McKinsey & Company. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative.

BBC. (2021, June 9). *Donald Trump-era ban on TikTok dropped by Joe Biden*. https://www.bbc.com/news/technology-57413227

Biden, J. (2021, June 9). *Executive order on protecting Americans' sensitive data from foreign adversaries*. The White House. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/06/09/executive-order-on-protecting-americans-sensitive-data-from-foreign-adversaries/.

Carson, B. (2016, May 8). *How a failed education startup turned into Musical.ly, the most popular app you've probably never heard of*. Business Insider. https://www.businessinsider.com/what-is-musically-2016-5.

Chan, K., & Hadero, H. (2023, March 7). *TikTok's CEO in Washington: Why app's security risks keep raising fears*. AP News. https://apnews.com/article/tiktok-ceo-shou-zi-chew-security-risk-cc36f36801d84fc0652112fa461ef140.

Christen, M., Gordijn, B., Weber, K., van De Poel, I., & Yaghmaei, E. (2017). A review of value-conflicts in cybersecurity. *The ORBIT Journal*, *1*(1), 1–19.

Creswell, J. W., & Poth, C. N. (2018). *Qualitative inquiry & research design: Choosing among five approaches* (4th edition). SAGE.

Curry, D. (2023, May 4). *Most popular apps (2023)—Business of apps*. https://www.businessofapps.com/data/most-popular-apps/

Feiner, L. (2022). *Lawmakers unveil bipartisan bill that aims to ban TikTok in the U.S.* CNBC. http://cnbc.com/2022/12/13/lawmakers-unveil-bipartisan-bill-that-aims-to-ban-tiktok-in-the-us.html.

Gray, J. E. (2021). The geopolitics of 'platforms': The TikTok challenge. *Internet Policy Review*, *10*(2), 1-26.

Halim, F., Augustinah, F., Vidyanata, D., Sherly, S., & Sudirman, A. (2022). Determinants of intention to use the TikTok application among Generation Z. *Ideas: Jurnal Pendidikan, Sosial, Dan Budaya*, *8*(3), 721-727.

He, X., Hua, K., Ji, C., Lin, H., Ren, Z., & Zhang, W. (2021). *Overview on the growth and development of TikTok's globalization*. *Proceedings of the 2021 3rd International Conference on Economic Management and Cultural Industry (ICEMCI 2021)*, 666–673.

Horowitz, B., & Check, T. (2022). *TikTok v. Trump and the uncertain future of national security-based restrictions on data trade*. *Journal of National Security Law and Policy*, *13*(1), 61-111.

Indrayani, I., & Maharani, T. (2022). THE United State's national security protection from cyber crime threats: A case study of TikTok banning submission by the President Donald Trump in 2020. *Journal of Social Political Sciences*, *3*(3), 268–280.

Islah, K. (2018). *Peluang dan tantangan pemanfaatan teknologi big data untuk mengintegrasikan pelayanan publik pemerintah* [Opportunities and challenges of using big data technology to integrate government public services]. *Jurnal Reformasi Administrasi: Jurnal Ilmiah untuk Mewujudkan Masyarakat Madani*, *5*(2), 130-138.

Jacobson, D. (2023, March 23). *Should governments ban TikTok? Can they? A cybersecurity expert explains the risks the app poses and the challenges to blocking it*. The Conversation. http://theconversation.com/should-governments-ban-tiktok-can-they-a-cybersecurity-expert-explains-the-risks-the-app-poses-and-the-challenges-to-blocking-it-202300.

Juned, M., Bainus, A., Saripudin, M. H., & Pratama, N. (2022). The dynamics of the USA and China relations in the cyberspace: Struggle for power in a global virtual world in building a global cyber regime. *International Journal of Business and Globalisation*, *30*(3/4), 396–414.

Khaniejo, N., & Sinha, A. (2018). *Economics of cybersecurity, Part II: Stakeholders* (Report). Center for Internet and Society. https://cis-india.org/internet-governance/files/economics-of-cyber-security-part-ii.

Maryanto, B. (2017). Big data dan pemanfaatannya dalam berbagai sector [Big data and its utilization in various sectors]. *Media Informatika*, *16*(2), 14-19.

McDonald, J., & Soo, Z. (2023, March 24). *Why does US see Chinese-owned TikTok as a security threat?* AP News. https://apnews.com/article/tiktok-bytedance-shou-zi-chew-8d8a6a9694357040d484670b7f4833be.

Nasution, R. A., Prayoga, Y., & Halim, A. (2022). The influence of ease of use, privacy, security and efficiency on shopping decisions using the TikTok shop. *Daengku: Journal of Humanities and Social Sciences Innovation, 2*(6), 895-902.

Niu, H., & Hong, J. (2021). International law thinking on data security in TikTok incident. *Proceedings of the 7th International Conference on Humanities and Social Science Reseqarch (ICHSSR 2021),* 268–271.

Picciano, B. (2014). *IBM BrandVoice: Why big data is the new natural resource*. Forbes. https://www.forbes.com/sites/ibm/2014/06/30/why-big-data-is-the-new-natural-resource/.

Pujianto, A., Mulyati, A., & Novaria, R. (2018). Pemanfaatan big data dan perlindungan privasi konsumen di era ekonomi digital [Utilization of big data and consumer privacy protection in the digital economy era]. *Majalah Ilmiah Bijak*, *15*(2), 127–137.

Puspa, D., Soegiharto, A., Nizar Hidayanto, A., & Munajat, Q. (2020). Data privacy, what still need consideration in online application system? *Jurnal Sistem Informasi*, *16*(1), 49–63.

Romanosky, S., Schwindt, K., & Johnson, R. (2023). *Comparison of public and private sector cybersecurity and IT workforces* (Report). RAND Corporation. https://www.rand.org/pubs/research_reports/RRA660-7.html.

Roumeliotis, G., Yang, Y., Wang, C., & Alper, A. (2019, November 1). *Exclusive: U.S. opens national security investigation into TikTok - sources.* Reuters. https://www.reuters.com/article/us-tiktok-cfius-exclusive-idUSKBN1XB4IL.

Seemma, P. S., Nandhini, S., & Sowmiya, M. (2018). Overview of cyber security. *IJARCCE*, *7*(11), 125–128.

Shepardson, D. (2023, March). *TikTok CEO: App has never shared US data with Chinese goverment*. https://www.nasdaq.com/articles/tiktok-ceo:-app-has-never-shared-us-data-with-chinese-goverment.

Sherman, J. (2022, December 28). *New bill proposes banning TikTok in the U.S.*. Lawfare. https://www.lawfaremedia.org/article/new-bill-proposes-banning-tiktok-us.

Sorongan, T. P. (2021, July 9). *Sengit! AS serang China, 10 perusahaan masuk daftar hitam* [Fierce! US attacks China, 10 companies blacklisted]. CNBC Indonesia. https://www.cnbcindonesia.com/news/20210709135451-4-259594/sengit-as-serang-china-10-perusahaan-masuk-daftar-hitam.

Stokel, W. C. (2023, February). *Instagram is becoming as uncool as Facebook—And it has only itself to blame*. Business Insider. https://www.businessinsider.com/why-instagram-cant-compete-tiktok-videos-algorithm-influencers-engagement-2023-2.

Tan, C. (2023, March). *China says "never" demanded TikTok hand over American user data*. Nikkei Asia. https://asia.nikkei.com/Business/China-tech/China-says-never-demanded-TikTok-hand-over-American-user-data.

The White House. (2021). Executive Order 14034—Protecting Americans' sensitive data from foreign adversaries. https://www.govinfo.gov/content/pkg/DCPD-202100490/pdf/DCPD-202100490.pdf.

TikTok. (n.d.). *About TikTok*. Retrieved July 17, 2023, from https://www.tiktok.com/about?lang=en.

TikTok. (2021, March 5). *Privacy and security*. https://www.tiktok.com/safety/en-us/privacy-and-security-on-tiktok/.

Trump, D. J. (2020, August 6). *Executive order on addressing the threat posed by TikTok*. Trump White House. https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-addressing-threat-posed-tiktok/.

Xu, L., Yan, X., & Zhang, Z. (2019). Research on the causes of the "Tik Tok" app becoming popular and the existing problems. *Journal of Advanced Management Science, 7*(2), 59–63.

Yu, C. (2022, September 22). *Chinese apps gain popularity globally.* Chinadaily.com.cn. https://www.chinadaily.com.cn/a/202209/22/WS632b3b2ba310fd2b29e79043.html.

Zhang, J., Zhao, W., Cheng, B., Li, A., Wang, Y., Yang, N., & Tian, Y. (2022). The impact of digital economy on the economic growth and the development strategies in the post-COVID-19 era: Evidence from countries along the "Belt and Road". *Frontiers in Public Health, 10*(856142), 1-17.