Journal of Social Political Sciences
JSPS
Vol. 3, No. 3, August , 2022

THE UNITED STATE'S NATIONAL SECURITY PROTECTION FROM CYBER CRIME THREATS A CASE STUDY OF TIK TOK BANNING SUBMISSION BY THE PRESIDENT DONALD TRUMP IN 2020

Irma Indrayani, Tasya Maharani
International Relations Department Faculty of Social and Political Sciences
Universitas Nasional Jakarta, Indonesia
irma.indrayani@civitas.unas.ac.id

Abstract : In August 2020, President of the United States Donald Trump issued an Executive Order to the United States Ministry of Commerce to prohibit transaction activities through the TikTok application. The prohibition of this transaction then resulted in the notion of TikTok being banned because the President claimed that TikTok collects and sells personal data of its users to the Chinese Government. The multinational company ByteDance, which oversees TikTok, then denied this claim and prepared to sue the Trump Administration. However, based on the research that has been done, in fact, there is a Chinese National Intelligence Law, which requires companies to involve the National Intelligence Services in their operation. The results of the discussion will try to analyze the truth of Donald Trump's claims, and what kinds of dangers that might occur from the cyber-crime attacks so the use of national security theory is appropriate as a basis analysis..

Keywords: *Tik Tok Banning, Cyber Crime, National Security.*

Submission	:	May, 23rd 2022
Revision	:	June 19th 2022
Publication	:	August 30th 2022

INTRODUCTION

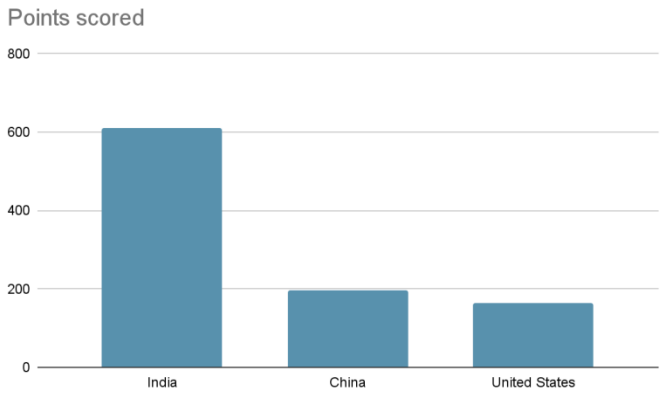
On August 6, 2020, President Donald Trump issued an Executive Order 13942 to prohibit transaction activities through the TikTok and WeChat applications. This Executive Order was later granted on September 18, 2020 by the United States Department of Commerce. The reason itself is to protect national interests, foreign policy, and the economy that may be threatened due to the possibility of data collection and theft by the Chinese Communist Party (U.S. Department of Commerce, 2020). Two days later on September 20, 2020, all transactions related

to the TikTok and WeChat apps, constituents, or app codes through app stores—such as the Play Store and App Store—have been banned. As of November 12, TikTok will be banned domestically in the United States (U.S. Department of Commerce, 2020).

TikTok and WeChat are software applications from China with different functions. WeChat is intended for chatting, and TikTok is an entertainment application that allows users to record videos with lots of music provided by the creator, the ByteDance Company. The ease of accessing and using TikTok makes many people of all ages download and use it actively. Apart from entertainment, many people use TikTok as a media to promote, create, and share a few moments in their lives with other users. Another reason why TikTok is so famous is because every user and the videos they create have an equal chance of going viral or famous (even if they don't have a famous person background).

The focus of the discussion in this article is on the blocking issue of TikTok in the United States. Although the Ministry of Commerce has officially approved the discourse of blocking two applications, namely TikTok and Wechat, the author thinks that TikTok is a trending platform and is widely used by various groups around the world. Furthermore, TikTok is expected to have a dangerous impact, not only on the security of its users, but on a broader scale, namely national security. If Donald Trump's accusations regarding the issue of theft of its user data and information are really carried out through the application, then millions of users are at risk of becoming victims of cybercrimes carried out by the ByteDance company, or more broadly China itself.

Previously India has also done the same thing. India's Ministry of Information and Technology has blocked 59 Chinese apps on the grounds that these apps steal and secretly transmit user data illegally. The Indian government also stated that applications from China threaten India's sovereignty and integrity, defense and security, and disrupt public order (BBC News, 2020). In 2019, India was the country with the highest number of TikTok downloaders in the world, reaching 611 million downloads, followed by China with 196.6 million downloads, and the United States with 165 million downloads (Chapple, 2020).



Graphic 1.0 Countries with the highest TikTok downloaders (2019)

Based on this data, it is known that the United States is one of the countries that use the most TikTok applications in the world. Furthermore, in the official legal report that TikTok filed against the Trump Administration, TikTok currently has 100 million active users in the United States with 1,500 workers and 10,000 new workforce recruiting plans across the US states (TikTok, 2020). TikTok's domestic profit in the United States is also no joke, which was around US$500 million in June 2020 (Yunan & Dotan, 2020).

The number of downloaders and active users who still use the TikTok application is a concern for the United States. The use of non-transparent data and information dissemination as well as the existence of China's National Intelligence Act are of great concern to the US in protecting its national security. The threat of cybercrime which has mushroomed in recent years is also not impossible. This study will further analyze the truth of Donald Trump's claims regarding TikTok and the threat of cybercrime that might occur if these claims are true. However, whether Donald Trump's claim is true or not, it seems China does have great power to interfere with the process of running this application. Furthermore, it is also necessary to examine how this case will move forward under the leadership of the Joe Biden Administration after the Trump Administration ends in January 2021

Based on this background, this paper focuses on the possibility of theft and sale of TikTok user data to the Chinese National Intelligence Service, as alleged by Donald Trump regarding the existence of the Chinese National Intelligence Law. Because this case occurred at the end of Trump's tenure, the time limitation in this research is from August 2020, the period when the ban was proposed, until January 2021, when Trump's term of office is over. However, to see the continuity and change in the direction of this case, the researcher added how this case

continued after Joe Biden came to power. This study aims to explain and identify how much control China has over the state and its people with the issuance of the Chinese National Intelligence Law. Even things as simple as watching or using a short video app can threaten and violate someone's privacy. Realizing this, Trump took preventive action by proposing to block TikTok domestically in the US, although this clearly received public criticism.

Furthermore, the research analysis explains the controversial articles on the Chinese National Intelligence Law which are very likely to threaten the national security of any country. In addition, although it seems difficult to accept, this research offers a solution so that this case can be accepted in a neutral way, as well as being a consideration for each individual to be more careful in keeping their personal data on the open-internet. Although not realized directly, data theft via the internet is real and can harm someone in any way. Thus, the preposition of this research is that the existence of tiktok may threaten US national security because of the Chinese National Intelligence Law.

LITERATURE REVIEW

Conceptual Studies on Security

Over the years, thinkers in the study of International Relations have tried to develop the concept of security because of its abstract and very broad meaning. The concept of security is one of the most important concepts in international relations, as explained by Arnold Wolf that, "…security is a crucial concept in international relations, [...] States and nations will tend to perceive differently their 'acquired values' and the degree of the danger they face…" (Lai et al., 2011, 1). Walter Lippmann also stated a similar statement that "a nation is secure to the extent to which it is not in danger of having to sacrifice core values if it wishes to avoid war, and is able, if challenged, to maintain them by victory in such a war" (Cox & Stokes, 2012, 51).

The definition of security concepts as stated above actually leads to security and military threats; mainly war. As Richard Ullman wrote as follows, "… traditional security conceptions have been too narrow and military oriented" (Ulman, 1983, 129). Thus, Ullman hereby emphasizes that the concept of security is not an absolute concept, but must be fulfilled by other elements in order for its value to be balanced. Furthermore, Richard Ullman also analyzes those issues such as scarcity of resources for human needs will be the main focus in discussing the concept of security in the post-Cold War era.

In line with Richard Ullman's statement, Ken Booth further revealed that after the Cold War, the discussion of security concepts became increasingly complex. These discussions, among others, cover the following issues:

"... the growth of complex interdependence, the erosion of sovereignty, amazing advance in communications, the declining utility of force, the degradation of nature, huge population growth, the internationalization of the world economy, the spread of global lifestyle, constant technological innovation, the dissemination of modern weaponry, the growing scope for non- state actors and so on" (Booth, 1991, 313-314)

The problems raised by Ken Booth then lead to new, broader issues—mainly regarding technological developments. The development of the era makes innovation in technology increasingly difficult to monitor and control. In fact, often these new technologies that come out make ordinary people overwhelmed and never feel enough. The scariest thing about technologies is that they are limitless. The possibility to create as well as the possibility to update is increasingly available, not only in good updates, but also in the direction of individual interests. Technology is also about its users. The world is not only a place for good and idealistic people, but also interested people who are willing to do whatever it takes to get their wants fulfilled—and technology may be the way. A previous study related to this theory was entitled "From Banning to Regulating TikTok: Addressing concerns of national security, privacy, and online harms" by Dr Jufan Wang in a report by The Foundation for Law Justice and Society, in association with the Center for Socio-Legal Studies and Wolfson College, University of Oxford. In this study, researchers analyze the possible impact if the US is really serious about blocking TikTok and the regulations that may be issued regarding this application. The research, which is based on the theory of national security, states that blocking TikTok is the easiest solution for long-term goals, such as data security, privacy, and preventing disinformation. However, the threat of blocking TikTok that will be carried out by the US will certainly scare a number of companies, because it will have a domino effect for other countries to do the same. The difference of these researches, this study focuses on the discussion based on Donald Trump's accusations against the possibility of theft of US public data, using the concepts of security, national security, and cyber security.

Cyber Security

Talking about technology cannot be separated from the existence of the internet or cyberspace. Public Safety Canada defines cyberspace as "the electronic world created by interconnected networks of information technology and the information on those networks. It is a global common where people are linked together to exchange ideas, services and friendship" (Public Safety Canada, 2018,

34). Based on this definition, it can be concluded that cyberspace is an abstract space that is not limited and includes all kinds of human nature from all over the world and all kinds of layers of society. These limitations in terms of interoperability, efficiency and freedom have clearly brought the countries of the world to their own fear and are trying to overcome the threats that may be caused by the cyber community. On this basis, a security concept related to cyber threats and crimes emerged, or what is known as the concept of cyber security.

With the same source, the definition of cyber security according to Public Safety Canada is "... protection of digital information and the infrastructure on which it resides" (Public Safety Canada, 2018, 7) Information protection as meant is protection against data theft and personal identity, fraud, propaganda, data misuse, fraud, and so on in cyberspace. However, one thing that is certain about cybersecurity is that it is very difficult to accurately identify the perpetrator of an attack (Buckland et al., 2015, 12). Perpetrators will easily cover up their own identity by impersonating someone else. In addition, the issues of cyber threats are also easy to be forgotten by the public due to the speed of information circulating in cyberspace itself.

National Security

National security is defined as a strategy to protect the country as a whole from threats that are considered to be harmful to the elements of the state (government, territory, people, and sovereignty). The main aspect and must exist in national security is security in terms of the military with the aim of protecting the existence of the country itself. But at the same time, the military is no longer the only element to secure national security. In today's era, the use of military weapons with the intention of destroying the human population is tantamount to showing how low the level of development in society and awareness to build the future is (Treinovskis & Jefimo, 2012, 43) Therefore, apart from the military, national security also includes aspects; environmental security, energy security and natural resources, economic interests, human security, homeland security, and cyber security (Holmes, 2015, 19) Because the elements of national security are numerous and do not only cover geopolitical, economic, and military affairs, the policies taken to maintain national security include not only defense policies, but also the country's domestic and foreign policies (Holmes, 2015, 23).

METHOD

The author uses qualitative research methods to answer and explain the truth of Donald Trump's claims on TikTok, as well as the possibility of the TikTok application being used as a medium to carry out cyber crimes. The qualitative

approach is also called the humanistic approach, because qualitative research occurs in situations where behavior and events involving humans interact naturally (Creswell, 2014, 327). The purpose of using this research is to produce descriptive data in the form of words or verbal from the observed behavior.
Furthermore, the data collection method chosen is a secondary data collection with document-based and internet-based datas. Document-based data collection methods were taken from documents in the form of books and research journals which were then reprocessed according to research needs. Meanwhile, internet-based data collection methods are taken from statistical webs and news portals both domestically and internationally so that the validity of the data used is really actual. This kind of data method has advantages because the data is easy to obtain and the researcher is easy to review for matters related to the substance of the research.

RESULT AND DISCUSSION

As explained in the introduction, TikTok is a Chinese app made by the ByteDance Company. TikTok started its first launch outside of China in May 2017. ByteDance Company, which handles TikTok, has opened branches in several major countries of the world, such as the United States (Los Angeles and New York), London, Paris, Berlin, Dubai, Tokyo, Singapore, Mumbai, Seoul and Jakarta (TikTok, 2020).
To run the application, it is no secret that the creator will collect information from the user itself. This is done so that the application can make it easier to adjust the interests of its users. TikTok—like other apps—does the same thing. It should be clarified that, by downloading, creating, and accessing a TikTok account, users voluntarily allow the creator to collect data for the benefit of the company and the users themselves. Some of the user information collected by TikTok is as follows (TikTok, 2020).

1. Registration information including age, username, password, language, email, and telephone number.
2. Profile information such as name, profile photo, location, and other social media accounts.
3. User-uploaded content, including photos, videos, comments, etc.
4. Payment information such as PayPal, Visa, etc.
5. Telephone numbers and social media contacts to find/find other people.
6. Information that users share in the questionnaire (gender, age, likes, preferences, etc.).
7. Phone model and operating system used.

Then apart from TikTok itself, the creator also makes it possible to retrieve user information from (TikTok, 2020):

1. Other social media linked to the application, such as Instagram, Twitter, Facebook, and Google,
2. Third-party services, for example; advertising,
3. Other users, and
4. Other sources from publicly accessible sources.

After knowing what information TikTok collects, then after that it is about whom the above information can be given. Based on what is written on the official website, the following are the possible persons/entities to whom personal data of TikTok users can be provided (TikTok, 2020):

a. Business partners (advertising, analytics and marketing),
b. If there is a possibility that TikTok will go bankrupt and be sold, merged, or transferred to another company.
c. Legal reasons, for example: court.
d. Other reasons with the direct permission of the user.

With the data that TikTok has collected, United States Secretary of State Mike Pompeo emphasized that millions of TikTok users are at risk of transferring personal data into the hands of the Chinese Communist Party (Tidy, 2020). ByteDance as the company that handles TikTok has clearly denied these claims many times, until in the end, ByteDance sued the Trump Administration to the high court for not accepting these claims and over the issue of blocking TikTok in the United States. TikTok insists that its company is very transparent about what they collect and what they don't. TikTok has also written time and time again that user security is the company's number one priority (TikTok, 2020).

Cases of theft or data breaches are not new and are not impossible. Previously, several application companies had been caught stealing information about their users' personal data. For example, an online shopping application from Indonesia, Tokopedia, has conceded 91 million user data and was sold for US$5,000 on a dark web site in May 2020 (CNBC Indonesia, 2020). Then the alleged case of data sales that recently happened was the case of selling Muslim Pro application data to the United States military. Although this accusation was denied by Muslim Pro, quoted by CNN Indonesia, Muslim Pro is one of hundreds of mobile phone applications that make money from selling user location data to third parties (CNN Indonesia, 2020).

In the scope, scale, and general occurrence, cases of data theft can result in submitting an online loan request using someone else's personal identity. This is easy to do because usually, the seller will sell a package that contains complete information in the form of; name, address, what bank is used, internet banking password, identity number, and so on (CNN Indonesia, 2018). On a broader scale, such as the theft of data from the Muslim Pro application and Donald Trump's accusations regarding TikTok, this is to monitor state policies through small things that people usually neglect to pay attention to.

TikTok as a National Security Threat to the United States

The era after the Cold War, especially after the tragedy of the September 11 attacks in the United States, has marked a shift in the concept of security from previously only military and security issues with the main actor being the state, becoming wider with various actors playing a role in international relations. Something that initially sounds impossible and is declared good in fact does not always work as expected. The speed of technological development is one of the biggest elements of the threat to national security in the life of the state. The existence of cyberspace or the internet in human life has brought a new chapter in the abstract and dynamic discussion of national security. The ease of accessing the internet makes people forget the importance of maintaining their identity because the internet is often associated as an anonymous space. However, the sheer number of cases that show the theft and sale of data is a reminder to humans that the internet can also be a threat to human security, or on a large scale, national security.

The fact that TikTok has the ability to collect user data is one of many examples of cyber crime issues. Perhaps, the personalization and information that TikTok collects are things that are commonly collected by other social media. However, the interesting thing about operating this app is that all activities carried out by the TikTok app—or the Chinese app in general—must be monitored by the country of origin.

This is in line with the Chinese National Intelligence Law which was promulgated on June 27, 2017 and has been in effect since July 2017. This law was created on the basis of increasing the protection of China's national security from the threat of terrorism and cyber-crime under President Xi Jinping's administration. With the promulgation of the Intelligence Act, it opens up great risks not only for the United States and overseas residents who do business or study in China, but also the entire population of China itself (Reuters, 2017).

There are several controversial articles related to this Law, including Article 7 which states that "all organizations, companies, or residents are obliged to support, assist, and cooperate with the work of the state intelligence agency as stated in the law". Then Article 14 states that "state intelligence work agencies, when legally carrying out their work, can demand that organizations or citizens who are related can provide the necessary support, assistance and cooperation". Continued in Article 16 which authorizes security officials to ask questions of individuals as part of collecting intelligence data, to examine their materials and files. Article 16 is clarified in Article 17, which stated that, these officials can confiscate means of communication, transportation, buildings, and other individual facilities including government organizations and agencies.

With the existence of this Intelligence Law, every activity carried out by citizens, foreign nationals, companies, and even organizations domiciled in China, are all monitored by the Chinese State Intelligence Agency for reasons of national security safeguards (Tanner, 2017). This clearly reduces the freedom of its citizens to interact in society because what happens in their activities in cyberspace will be monitored by intelligence.

TikTok is a Chinese company, which under the Act, is required by law to involve the Chinese Government in its operations. Although TikTok already has several branch offices in several countries, the head office of TikTok (ByteDance) is in China. This means, there is a possibility that the data of TikTok users is used by the Chinese Intelligence Service to maintain the national security of its own country.

The United States' action in blocking TikTok on its territory is the right thing to do. Even though ByteDance has denied these claims several times, there is still a possibility that these claims are true because this Intelligence Act has actually been operational. Furthermore, this issue also concerns the poor relations between China and the United States recently. The two of them seemed to want to prove their strength by looking for the opponent's weakness to protect their own—which made sense.

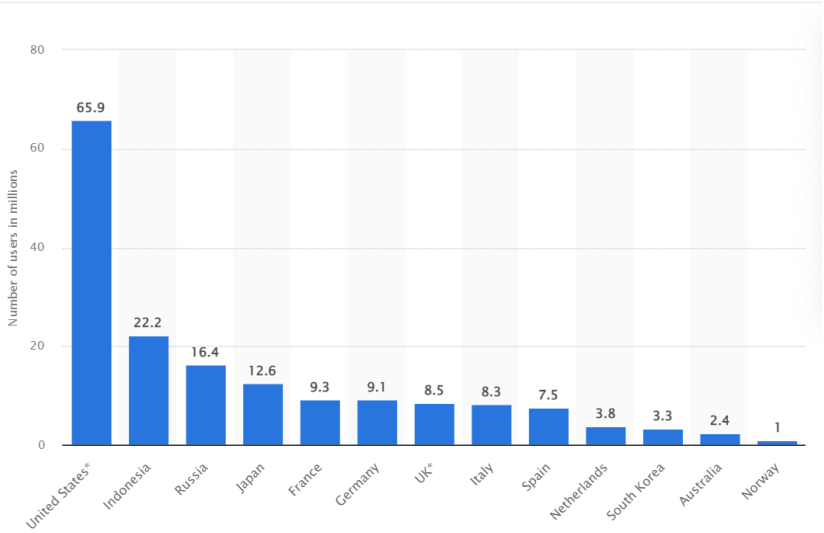
Although this action of the United States has many pros and cons for its people because after all, the public may not experience the impact of this data theft directly. However, it is the state's obligation to protect the national security and human security of its own country. In addition, whether we realize it or not, blocking TikTok is one of the United States' efforts to protect the human rights of its citizens from the threat of data theft in cyberspace.

Furthermore, if TikTok insists on continuing to operate in the United States, the US Department of Commerce asks TikTok to transfer its technology to US companies, Oracle and Microsoft to then open a new company called TikTok Global—including Canada, New Zealand, and Australia (Reuters, 2020). With this technology transfer discourse, TikTok (ByteDance) is required to seek approval from the Chinese Government. As a result, this

blocking discourse not only affects the United States' national security activities, but also leads to business and political activities. But despite that, the United States is known to have its own interests in buying and selling proprietary technology rights to protect its national security and economy (Baranson, 1976, 150).

Continuation of the Case in the Joe Biden Era

Until 2020, the United States occupies the first position with the largest number of TikTok users in the world with 65.9 million active monthly users (Graphic 1.0) (Ceci, 2022). So with this case, it is clear that there is a lot of opposition, especially from the TikTok Creator community. The first judge to hear the case, Wendy Beetlestone in Pennsylvania, thought blocking TikTok would threaten the creators with losing sponsorship income or other opportunities they could get. Then a second judge, Carl Nichols in Washington, also expressed his disapproval of the president's lawsuit. According to Nichols, Trump abused his power for economic gain with the intention of bringing this hugely popular app out of business.



Graphic 2 Counties with the highest TikTok users

Until the trial held on December 7, 2020, there has been no solid result on who won in this case. However, based on the two judges' statements and the circumstances that occurred until two years later, TikTok which was supposed to be slated to stop operating on November 12, 2020; seems to still be able to breathe easy. The case was ultimately not resolved until Donald Trump's Presidency ends on January 20, 2021 (Reuters & Shepardson, 2020). After Joe Biden took office, the Ministry of Commerce asked the Federal Court to withdraw the case of blocking and banning transactions via TikTok and WeChat on June 22, 2021. Furthermore, the Biden Administration ordered the Department of Trade to expand the scope of supervision of the application for 120 days (Shepardson, 2021).

President Joe Biden then decided to re-investigate and continue the case, but in a more coherent way than Trump's accusations. Biden argues that, if applications from China can really threaten America's national security, then the threat is no longer in the technology and trade sectors, but also the military, economy, and

democracy itself. Therefore, the Minister of Trade Gina Raimondo stated, a rigorous analysis of evidence and data is needed to examine applications developed by foreign countries, especially China. In the future, it is difficult to predict whether ByteDance will be asked to transfer its data to the US, or if TikTok will be fully transferred, the case is still under discussion by actors (Shepardson, 2021).

CONCLUSION

In August 2020, Donald Trump submitted an Executive Order to the United States Department of Commerce, to stop any transaction activity and close the operation of the TikTok and WeChat applications in his country on national security grounds. Donald Trump suspects that TikTok collects personal information from its users and provides it to the Chinese Communist Party. The author focuses the discussion on the issue of blocking TikTok because the author considers TikTok to be an application that is currently trending and is widely used by all ages. Furthermore, in September 2020, the Ministry of Commerce approved this order and TikTok will be officially blocked in November 2020.

Some of the important points of this research are first, the fact that there is a possibility of national security threats with TikTok application. The reason is in line with China's Intelligence Law which states that every activity of individuals, companies, even organizations, must involve the State Intelligence Agency in carrying out its activities. With this Act, all people who occupy Chinese land, all of their activities will be monitored by the State Intelligence Service. Second, the United States' decision to block Chinese applications is the right thing from America perspective for national security reason. The possibility of theft of user data through applications is proof that the meaning of this security concept has shifted; from what was originally only the military whose actor was the state, to many aspects that were never imagined before and with other actors who were not the state. Although the case is not yet fully resolved under President Trump, the Biden Administration will nevertheless continue to look for ways to keep TikTok in control in the United States in a legal way, along with the fact that this app has taken root in people's lives and has become a job for many people. Third, the author confirms that the concepts of security, national security, and cyber security are relevant as the theoretical basis of this case. That the shifting of security concepts including one of them, cyber security, can be a threat to every country and individual, even through something as simple as a mobile phone application.

REFERENCES

Baranson, J. (1976). Technology Exports Can Hurt Us. Foreign Policy Journal, 25.

BBC News. (2020, June 29). India bans TikTok, WeChat and dozens more Chinese apps. BBC. Retrieved September 21, 2020, from https://www.bbc.com/news/technology-53225720

Booth, K. (1991). Security and Emancipation. Review of International Studies, 17(4).

Buckland, B. S., Schreier, F., & Winkler, T. H. (2015). Democratic Governance Challenges of Cyber Security. DCAF Horizon, (1).

Ceci, L. (2022, May 13). • TikTok user base in selected countries 2020. Statista. Retrieved June 3, 2022, from https://www.statista.com/statistics/1202979/number-of-monthly-active-tiktok-users/

Chapple, C. (2020). TikTok Crosses 2 Billion Downloads After Best Quarter For Any App Ever. Sensor Tower. Retrieved November 27, 2020, from https://sensortower.com/blog/tiktok-downloads-2-billion

CNBC Indonesia. (2020). Kacau Banget! Kok Bisa Sih Data Tokopedia Bocor? Retrieved November 26, 2020, from https://www.cnbcindonesia.com/tech/20200704112811-37-170183/kacau-banget-kok-bisa-sih-data-tokopedia-%20bocor

CNN Indonesia. (2018, December 27). Risiko Ketika Data Pribadi Dicuri. Retrieved November 26, 2020, from https://www.cnnindonesia.com/teknologi/20181226210103-185-356593/risiko-ketika-data-pribadi-dicuri

CNN Indonesia. (2020). Muslim Pro Buka Suara, Bantah Jual Data ke Militer AS. Retrieved November 26, 2020, from https://www.cnnindonesia.com/teknologi/20201123140024-185-573352/muslim-pro-buka-suara-bantah-jual-%20data-ke-militer-as

Cox, M., & Stokes, D. (Eds.). (2012). US Foreign Policy. OUP Oxford.

Holmes, K. R. (2015). What is National Security? The Heritage Foundation: Index of U.S. Military Strength.

Lai, Y. M., Hughes, C. W., & Hughes, C. (Eds.). (2011). Security Studies: A Reader. Routledge.

Public Safety Canada. (2018). Canada's Cyber Security Strategy. Public Service Canada.

Reuters & Shepardson, D. (2020, December 28). U.S. government appeals order blocking TikTok restrictions. Retrieved March 25, 2022, from https://www.reuters.com/business/media-telecom/us-government-appeals-order-blocking-tiktok-restrictions-%202020-12-28/

Reuters. (2017, June 27). China passes tough new intelligence law. Retrieved November 26, 2020, from https://www.reuters.com/article/us-china-security-%20lawmaking-idUSKBN19I1FW

Reuters. (2020, August 29). China's new tech export controls could give Beijing a say in TikTok sale. Retrieved November 27, 2020, from https://www.reuters.com/article/us-usa-tiktok-china-idUSKBN25Q05Q

Shepardson, D. (2021, July 12). Biden administration asks courts to dismiss government appeals of TikTok ruling. Retrieved March 25, 2022, from https://www.reuters.com/business/retail-consumer/us-asks-court-dismiss-government-appeal-tiktok-ruling-%202021-07-12/

Tanner, M. S. (2017, July 20). Beijing's New National Intelligence Law: From Defense to Offense. Lawfare. Retrieved November 26, 2020, from https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense

Tidy, J. (2020, August 3). TikTok: What is the app and how much data does it collect? BBC. Retrieved November 26, 2020, from https://www.bbc.com/news/technology-53476117

TikTok. (2020). About Us: Our Mission. TikTok. Retrieved November 26, 2020, from https://www.tiktok.com/about?lang=en%20accessed

TikTok. (2020). Legal: Privacy Policy. TikTok. Retrieved November 26, 2020, from https://www.tiktok.com/legal/privacy-policy

TikTok. (2020, August 24). Why we are suing the Administration | TikTok Newsroom. Newsroom | TikTok. Retrieved November 21, 2020, from https://newsroom.tiktok.com/en-us/tiktok-files-lawsuit

TikTok. (2020, August 24). Why we are suing the Administration | TikTok Newsroom. Newsroom | TikTok. Retrieved November 26, 2020, from https://newsroom.tiktok.com/en-us/tiktok-files-lawsuit

Treinovskis, J. T., & Jefimo, N. (2012). State National Security: Aspect of Recorded Crime. Journal of Security and Sustainability Issues, 2(2).

U.S. Department of Commerce. (2020, September). Commerce Department Prohibits WeChat and TikTok Transactions to Protect the National Security of the United States. Retrieved September 10, 2020, from https://www.commerce.gov/news/press-releases/2020/09/commerce-department-prohibits-wechat-and-tiktok-transactions-protect

Ulman, R. (1983). Redefining Security. International Security, 8(1), 129.

Yunan, Z., & Dotan, T. (2020). TikTok's U.S. Revenues Expected to Hit $500 Million This Year. The Information. Retrieved November 21, 2020, from https://www.theinformation.com/articles/tiktoks-u-s-revenues-expected-to-hit-500-million-this-year%20accessed