

National Threats and Responses Toward Digital Social Media: The Case of Global TikTok Regulations

LE YANG

Ph.D Candidate, School of Journalism and Communication, Tsinghua University

Visiting Scholar, School of Public Policy, Georgia Institute of Technology

Abstract

Since the United States' attempt to regulate TikTok in 2020 due to national security concerns, 32 countries have implemented various regulatory measures against the platform for different reasons. This study uses global TikTok regulations as a case study to investigate the types of social media threats perceived by nations and their corresponding regulatory responses. Employing thematic analysis, we examine the relationship between threat perceptions regarding TikTok and regulatory responses across different countries. Grounded in the dual attributes of content and data within social media, along with considerations of threats at both national and individual levels, we formulate a typology of national threats emanating from social media. The findings reveal that (i) countries perceiving threats to TikTok from national security-data concerns are more inclined to implement measures isolating it from critical devices, (ii) countries perceiving threats related to individual well-being-data are more prone to adopting privacy regulations, and (iii) countries perceiving threats linked to national security-content and individual well-being-content are more inclined to enforce complete bans or content regulations. These decisions are influenced by factors including domestic stability, religious convictions, and democratization.

Keywords:

Media regulation, global TikTok regulation, social media national threats, typology, media comparative studies

TikTok, a short-video application that combines the strengths of Toutiao¹ and

¹ Toutiao is a news and information content platform developed by ByteDance. It uses artificial intelligence algorithms to analyze user behavior and preferences, generating a customized feed of articles, videos, and other content based on individual interests.

Musical.ly², has disrupted the U.S. dominated social media market, becoming a popular app with over 1 billion daily active users. However, since 2019, the investigation by the U.S. Committee on Foreign Investment in the United States (CFIUS) into ByteDance's (TikTok's parent company) acquisition of Musical.ly, citing national security concerns. The Trump administration issued an executive order invoking the powers under the International Emergency Economic Powers Act (IEEPA) to limit TikTok's operations within the United States (Executive Order, 2020). And Biden administration signed "Government Device Ban on TikTok Act" (U.S. Congress, 2021). U.S. senators are still debating a nationwide ban on TikTok (McCabe & Kang, 2023). With the U.S. investigation and regulation of TikTok, 32 countries around the world have taken different regulatory measures to TikTok, as seen in the Table 1. Which has raised a series of questions about the social media application's impact and the reasons behind the global regulatory actions. Why are so many countries concerned about a social media platform primarily used for everyday entertainment? What factors contribute to the diverse range of restrictions imposed on the app? Why is the same social media application subject to varying regulatory measures across states? How do different countries view social media as a national threat? And what regulatory approaches will nations prefer to adopt in response to different social media threats?

Table 1 Different National Restrictions to TikTok (Until December 2023)

Restriction Status	Type	Description	Country	Number	Sum
Officially Restricted	Completely ban	National block	India,Azerbaijan,Kyrgyz,Afghanistan,Nepal,Somalia, Senegal	7	32
	No Tiktok on official devices	Prohibit install on government devices	America,Britain,Canada,France,Australia,Netherland,New Zealand,Denmark,Norway,Belgium,Estonia,Ireland,Japan,Korea,Latvian,Malta	16	
	Content Regulation	Improve content moderation	Vietnam,Kenya,Malaysia,Italy	4	
		Ban due to content violation and lift	Bangladesh,Jordan,Pakistan	3	
		Cooperate with content moderation	Thailand	1	

² Musical.ly was a social media platform for creating, sharing, and discovering short music videos. Users could choose from a library of songs, dialogues, and sound bites to create videos where they lip-synced, danced, or performed skits. In 2018, Musical.ly was acquired by ByteDance and merged into TikTok.

	Privacy Regulation	Fine for user data violation	America, Britain, Netherland, Turkey, Ireland	5	
		Improve user data protection	Vietnam	1	
		Participate in data localization	France	1	
Discussion without restriction	Completely ban	National block	Egypt, Philippines	2	3
	No Tiktok on official devices	Prohibit install on government devices	Philippines	1	
	Privacy Regulation	Investigate the use of user data	Colombia	1	
Others	TikTok cannot be used on German government devices from News sources, but no official announcement, and the German health minister still runs a TikTok account with 144k followers.			Germany	3
	After Russia made it a crime to spread fake news about its invasion of Ukraine, TikTok shut down it's video uploading and live streaming functions in Russia.			Russia	
	Indonesia shut down TikTok Shop for protecting local businesses, but later reinstated it.			Indonesia	

The global regulatory actions surrounding TikTok highlight complexities in digital media regulation, data protection, and geopolitical considerations, shaping the dynamics of national security in the digital era. These actions reflect the intricate interactions between economics and politics, the market and the state, as well as technology companies and governments. Additionally, TikTok's Chinese affiliation has symbolically positioned it as a representative of China, leading to questions about whether restrictions on TikTok are directed at the enterprise or the home country. This study aims to clarify the perception of social media national threats posed by nations and explore the relationship between those threat perceptions and regulatory responses through an analysis of TikTok's regulations worldwide, shedding light on the complexities of digital media regulation and its implications for national security in the digital age.

This study is organized into several sections. The first reviews existing research on TikTok regulations, focusing on factors influencing regulation and regulatory policy. The second section develops a theoretical typology of social media national threats perception, based on two threat objects (nation-state and individual) and two social

media attributes (content and data). The third part outlines data sources and method. The fourth section presents the research findings: (i) Data is emerging as the primary source of threats from TikTok to nations. (ii) Geopolitics play a role in the global regulations of TikTok. (iii) In response to data threats at the national level, countries are more likely to isolate TikTok from critical devices. In response to data threats at the individual level, countries are more inclined to adopt privacy regulations, often requiring TikTok to enhance user data protection through fines, and (viii) In cases where a country perceives TikTok's content as a threat, complete bans and content regulations are implemented, depending on their stability, religions and democracy level.

Literature Review

TikTok, as the globally popular short-video social media which parent company is a Chinese enterprise, marked the initial instance where the United States employed a National Security Emergency Executive Order to block a social media app (Executive Order, 2020). There is a bunch of researches about TikTok restriction from the perspective of China-U.S. exasperate competition. The prevalent viewpoint suggests that the U.S. government's forceful separation of TikTok from its parent company and the attempts to ban TikTok within the country are manifestations of the United States curbing China's rise in the digital domain (Goodin, 2020). Trump's Executive Order is an extraordinary measure that represents an externalization of excessive concerns and fears about China's growing strength (Dong, 2021). In terms of Trump's administration interests, the crackdown on TikTok was a specific measure of Trump's "America First" strategy, opening up a new battleground in the U.S.-China technology war (Pan, 2020). This crackdown also served the Trump administration's electoral interests (Meng & Li, 2020; Chen, 2022). Economically, TikTok's rise disrupted the prevailing status quo of traditional U.S. media enterprises dominating the international market. In 2022, TikTok became the world's third most popular internet service, posing competition against mainstream U.S. platforms like Meta (Facebook, Instagram) and Alphabet (Google, YouTube). This shift in dynamics made the U.S. internet industry and political factions believe that "the rise of Chinese internet companies threatened American businesses" (Meng, 2020), prompting the United States to prevent the Chinese company "ByteDance" from achieving globalization (Pan, 2020). In the broad national competition context, scholars also think TikTok posed a threat to America's dominant position in cultural and technological domains

(Kuang & Zhang, 2020; Cartwright, 2020).

Apart from the strong suppression of TikTok by the United States, India was the first country to completely ban TikTok. Against the backdrop of the 2020 border conflict between India and China, the Modi administration believed that TikTok engaged in activities detrimental to India's sovereignty and integrity, compromising data security and personal privacy. Consequently, India imposed a nationwide ban on over 60 Chinese applications, including TikTok (PIB Delhi, 2020). Regarding the research on India's ban on TikTok, scholars argue that India's ban had a clear tone of technological nationalism, perceiving TikTok's "Chineseness" as a result of populist sentiments expressed in India's "nationalism" discourse. (Song & Ray, 2023; Kumar, 2023; Mishra & Schroeder, 2022)

The United States' coercion for TikTok to divest and India's comprehensive ban on TikTok demonstrate that, within the geopolitical context, the development of platform enterprises is not solely determined by user-platform interactions but rather influenced by international relations (Kumar & Thussu, 2023). However, based on the Relationship Scorecard between China and major countries, it's evident that countries' decisions to restrict TikTok are not solely based on their relationship with China. As seen in the Figure 1, although Japan has significant negative relations with China, its restriction on TikTok is not extreme. Instead, Japan's ban on TikTok is limited to devices involving government confidential, slightly less strict than a general prohibition on using TikTok on government devices. Additionally, the Japanese government's statement emphasized that this action was "not directed at any specific country" (47NEWS, 2023). Furthermore, Pakistan, a country with relatively positive relations with China, had banned TikTok three times. Research comparing India, the United States, and Pakistan's reasons and measures for sanctioning TikTok revealed that Pakistan's primary concern was content morality, the United States focused on national security, and India emphasized data privacy (Riaz, 2020). Thus, it's evident that countries may have differing perceptions of TikTok threats, leading to different approaches in their responses.

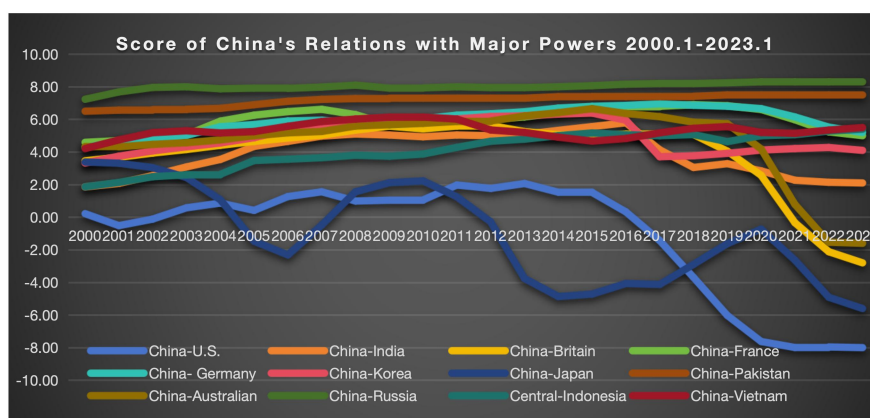


Figure 1 Score of China's Relations with Major Powers 2000.1-2023.1³

Based on the above TikTok restriction research review, existing studies predominantly place TikTok within the context of geopolitics, with a particular focus on the regulatory actions of the United States and India. The existing researches overlook the diversity of social media threats and regulatory approaches imposed by other countries, especially for the developing countries to the threats associated with TikTok. In fact, since the initiation of the CFIUS security review of TikTok in 2019, EU member states and U.S. allies have joined the bandwagon in restricting TikTok, and many developing countries have implemented restrictions on TikTok due to domestic unrest and religious reasons, among others. As of December 15, 2023, a total of 32 nation states have officially taken regulatory measures on TikTok for different reasons, and three countries are currently discussing TikTok restrictions but have not yet enacted policies. As seen in the Table 1. Therefore, this empirical study will use TikTok global regulations as a case to theoretically construct a comprehensive framework for the national threats posed by social media and the national responses. Our research contributes not only to enrich the media regulation studies in the digital age but also introduce a novel perspective to comparative media research.

Social Media National Threat Perceptions and Response

Dual Attributes of Social Media: Content and Data

Content Attribute: The definitions usually converge around the concept of social media, emphasizing digital technologies that emphasize user-generated content and network interaction (Kaplan & Haenlein, 2010; Terry, 2009; Carr & Hayes, 2015). Typically, social media is referenced through channel characteristics, either

³ Data Sources: The Database of China's Relations with Great Powers established by the School of International Relations of Tsinghua University using quantitative measurement Method.

identifying the directional nature of messages (Kent, 2010) or using specific tools like Facebook or Twitter to exemplify interaction patterns (Howard & Parks, 2012). The essence of social media is a tool for user to communicate, so whether it's traditional media with professional-generated content or social media with user-generated content, content is always the primary attribute. Social media's content attracts users, encourages interaction, and drives revenue. This content includes news, messages, knowledge, and other information types. Scholar Lusk introduces relational sociology into media studies, highlighting the impact of media content on security (Lusk, 2018).

Data Attribute: Van Dijk and Poell point out that social media's datafication is a key feature, meaning it can quantify many aspects of the world that were previously unmeasured (Van Dijk & Poell, 2013). This includes not just demographic data but also metadata from smartphones, like timestamps and GPS location. Initially, (meta)data was seen as a byproduct of online networks, but as platforms evolved, they became more focused on collecting and using data for their business models (Mayer & Cukier, 2013). The vast number of users and user-generated content on social media provide a wealth of data resources, including relationships (friends, likes, trends) on platforms like Facebook or Twitter. This data is crucial for social media, helping with targeted advertising (Alhabash & Hussain, 2017, pp. 285-299), a key source of income, and improving user engagement through algorithms. TikTok's success is partly due to its innovative use of data mining and algorithm-based content recommendation technology.

Two Dimensions of Threat Perception: National and Individual

National Security: The term "national threat" is often used in the context of national security, which refers to a country being safe from dangers, both external and internal (Liu, 2001). This definition commonly denotes the primary subject of the first dimension of national security as the nation state. The traditional concept of national security emerged from modernist political and sociological thought, starting from Thomas Hobbes to Max Weber (Hobbes & Smith, 1909; Honigsheim, 1946). They assert that a nation needs to maintain the legitimate use of force to maintain security as the core responsibilities of a nation-state. At that time, national security primarily focuses on maintaining security within geographically demarcated territories to shield the nation's survival from external and internal threats (Ripsman & Paul, 2010). In the modern world, besides military security, non-traditional security is also a core element of national security, including environmental security, energy security,

natural resources, economic interests, human security, homeland security and cyber security, etc., (Gale et al., 2015, p.19). China even has proposed a holistic perspective on national security with 11 elements (XinhuaNews, 2014). However, this issue-oriented understanding of national security only leads to an infinite division of security categories. This study aims to categorize national threats based on their impact on the state and individuals.

Individual Well Being: People are essential to a nation state; without them, a nation wouldn't exist. Therefore, the second dimension of national threat focuses on individual well-being. Countries often mention in their national security strategies the importance of protecting their citizens and ensuring their well-being.

For example, the United States aims to protect its citizens, promote economic prosperity, and uphold democratic values (White House, 2022, p.7). China's 2014 "Overall National Security Concept" emphasizes the security of its people, with political security as fundamental (Renming Paper, 2014). When individual rights and welfare are not protected, it can lead to public discontent and unrest, possibly resulting in violence or government overthrow. And in special and restrictive condition, when individual welfare is threatened, and this threat is one faced by all individuals in a broad sense, this individual threat can also escalate to the level of a national threat.

Therefore, this research does not offer a new definition of the concept of national threats. Instead, it is based on the existing general definition of national security but separates and narrows down national security from the level of threats to national security and threats to individual welfare. This is also based on the premise that the threat to a country from social media arises from individual usage. By understanding how individuals' use of social media can lead to threats, we can analyze their impact on national security.

Social Media National Threat Perceptions Typology

Content and data are the two main aspects of social media that pose different threats at national and individual levels. To better understand these threats, we have constructed a typology of national threats to social media theoretically. Typology approach involves identifying and categorizing these threats through classification, matching, and association with different concepts and variables, establishing logical

connections among them (Bailey, 1994, p.3; Gerring, 2012, p727). Using this approach, we outline four types of social media national threat perceptions, as shown in Table 2.

Table 2 Social Media National Threats Typology

	NATIONAL SECURITY	INDIVIDUAL WELL BEING
CONTENT	National Security-Content Foreign entities can create and spread content to sway public opinion and influence decision-makers. This can threaten national security by undermining legitimacy, inciting unrest, and causing polarization. Decision-makers may also be misled, especially in military and diplomatic matters. Propaganda and persuasion are the primary methods used.	Individual Well Being-Content Social media content, like harmful material, pornography, hate speech, violence, and cyberbullying, can harm people's well-being. Some content can even lead to extreme behaviors, harming both the individual and others.
DATA	National Security-Data Foreign entities can use daily social media data to gather strategic intelligence, potentially disrupting domestic democratic processes and social order by manipulating information using data-driven algorithms.	Individual Well Being-Data Misusing personal data on social media can violate privacy and allow criminals to exploit it for activities like online fraud.

(1) Social Media National Security - Content Threat Perception

Social media may poses national security threats through its content in two main ways. One is by influencing public perception, leading to citizen unsafe behavior. The other is by influencing decision-makers, leading to the formulation of unsafe policies. In the former case, there are three main threats that countries primarily face: regime stability, social security, and democratic politics. Firstly, it can be used by foreign actors to spread information that influences public opinion, incites unrest, and even undermines governments. For example, social media is accused of playing a significant role in movements like the "Twitter Revolution" in Iran in 2009 and the "Arab Spring" in 2010, where protesters used platforms like Twitter and Facebook to organize and spread their message (Hussain & Howard, 2013). These movements led to political changes and conflicts in several countries. Secondly, for more dangerous extremists, social media lowers barriers to access radical and extremist content (Sageman, 2011) and expands the spread of extremist ideologies and content (Mendelsohn, 2011; Weggemans et al., 2014) lead to social disorder. An extensive literature review on terrorism and Internet use found that "the Internet itself is not a cause of radicalization,

but rather an enabler and catalyst of individuals on a trajectory toward violent political behavior (Meleagrou & Kaderbhai, 2017). Thirdly, foreign countries could manipulate information through social media to interfere democratic procedure, domestic election especially (Jamieson, 2020).

Secondly, social media could also potentially affect decision-makers' perceptions, potentially influencing military command and other critical national decisions. In international security studies, media and security have two mainstream research paradigms, one is the CNN effect (Gilboa 2005a, 2005b), which regards the media as independent actors influencing the decision-making process. In the new media age, U.S. Department of Defense has classified social media as a new technology posing threats to national security at the same level as artificial intelligence, machine learning, quantum computing, and robotics, believing that social media content could affect the cognition of military personnel, potentially impacting military command (U.S. Government Accountability Office, 2022). This shows that social media content can possibly influence regime stability, social order, electoral processes, and national decision-making.

(2) Social Media Individual Well Being - Content Threat Perception

Social media has become a necessity in people's daily lives, offering us richer information and more convenient ways of communication. But it also carries risks to individual well being. Numerous studies indicate a correlation between high levels of social media usage among children and adolescents and adverse effects. One study showed that how adolescents themselves perceive the threat of social media to their mental health, they believe that social media could cause mood and anxiety disorders for some adolescents, it was viewed as a platform for cyberbullying and the use of social media itself was often framed as a kind of 'addiction' (O'reilly, etc., 2018). The abundance of harmful content on social media, particularly hate speech and cyberbullying, could causes psychological harm to different age individuals (Leist, 2013). The prevalence of misinformation and rumors diminishes people's ability to assess information accurately, leading to incidents where individuals have died due to incorrect treatment information during pandemics. Therefore, social media may pose potential threats to individuals due to content.

(3) Social Media National Security - Data Threat Perception

Data and content are treated separately in this study. Content focuses on influencing behavior, while data emphasizes the power generated through data analysis. Strategic information, once considered a source of state power (Keohane & Nye, 1998), has become blurred with the rise of digital platforms (Rosenbach & Mansted, 2019). The digital platforms(including social media platform) collect vast amounts of daily data, which, when processed, can become strategically significant (Napoli, 2019), which increasingly becoming primary targets for state surveillance and geopolitical pressure (Hong, 2022) .

Social media platforms are a type of platform-based enterprise, with one of its core logics being data-centric (Van Dijck & Poell 2013). By 2022, there were over 4.59 billion global social media users, projected to reach nearly 6 billion by 2027 (Statista, 2023). Scholars refer to this raw data within social media platforms as incidental data, revealing that manually collecting just two hours of incidental data is sufficient to disclose private information individuals didn't intend to publish (Kutschera, 2022). Thus, mining data from social media is a source of national intelligence analysis. It is the reason that many countries concern about TikTok. In addition, the powerful role of social media in political campaigns makes it a potential tool to influence a country's electoral process, as seen in the Cambridge Analytica scandal. Furthermore, social media-based cybersecurity threats also represent a form of national security threats. Studies indicate that threats via social networking sites spread faster than other forms of attacks due to the inherent trust among network users (Srivastava & Singh, 2021, pp. 245-253).

(4) Social Media Individual Well Being - Data Threat Perception

Mining data from social media means mining individual user data, which threatens personal privacy. Social media contains vast amounts of user-generated content, including private information, making users vulnerable to privacy risks (Ghazaleh, 2018; Ghazaleh & Liu, 2019; Ji et al., 2016) . For instance, sharing vacation plans on Twitter could lead to break-ins or thefts (Mao et al., 2011; Zhang et al., 2018). Researchers using open-source intelligence methods have shown how extracting user data from social media can affect personal privacy (Kutschera, 2022). Additionally, users often incur losses due to cyber attacks on social media platforms, impacting the interpersonal relationship networks and trust established through these platforms. Platforms like Facebook allow users to share content with their connections, but

hackers can exploit this trust to spread malware through friends' content (Huber et al., 2009). Deliri and Albanese have reviewed the most common attacks to online social networks (Deliri & Albanese, 2015, pp.195 – 209), including phishing, spamming, malicious software, trojan, data theft, network sniffing, data virus, fraud, cyber attack, hacking... Based on the user data resources, social media can be easily exploited to harm individual interests using user data.

So far, we've developed a theoretical typology of national threats from social media. Next, we'll analyze how countries regulate a specific social media platform, TikTok, in response to these threats. TikTok is an ideal case study because it embodies typical social media features, particularly strong data-related characteristics due to its algorithmic recommendation system. Additionally, TikTok is widely used globally, with 32 countries already implementing official regulations, offering diverse perspectives on national threats and responses. The upcoming sections will detail our data sources and methodology for examining these threats and responses.

Method and Data

Methods

This study used Braun and Clarke's six-step thematic analysis method to examine national perceptions of threats posed by TikTok and the corresponding responses. The steps included familiarization with the data, generating initial codes, identifying themes, reviewing themes, defining and naming themes, and producing the report (Braun & Clarke, 2006, p77). Based on our social media national threat perception typology, we categorized four themes of social media national threats: National Security-Content, Individual Well Being-Content, National Security-Data, and Individual Well Being-Data.

The criteria for each threat were coded based on private sector and national documents. Content threat themes were derived from Facebook's Community Standards Enforcement Report (Meta, 2023), which categorizes social media content threats to individuals. Additionally, national documents representing different media systems from the UK's Online Harms White Paper (UK Online Harms White Paper, 2020) and China's Provisions on the Governance of the Online Information Content Ecosystem (CAC, 2020) were selected to offer liberal and authoritative national perspectives on content threats. Criteria for data-based threat themes were primarily

based on the European Union General Data Protection Regulation (GDPR) and China's "Data Security Law" and "Personal Information Protection Law," reflecting national perceptions of data threats.

Regulatory measures taken by countries against TikTok were categorized into four types: (1) Complete Ban, (2) No TikTok on Government Devices, (3) Content Regulation, and (4) Privacy Regulation. An encoding book was generated for coding using DiVoMiner content analysis software. Two coders established research categories and coding indicators, achieving consensus on the coding process and content judgments. Reliability testing was conducted on a sample of 10 countries (accounting for 26% of the total sample size), with a final Cohen's Kappa coefficient for inter-coder agreement of 0.91, indicating good reliability. Dichotomous variables (0 and 1) were used to indicate whether a country adopted a certain type of national threat perception toward TikTok and regulatory measure. By coding TikTok threats and national regulations of 38 countries, the study analyzed the relationship between single and combined TikTok national threats and corresponding regulatory measures.

Data Sources

This study searched for countries that have implemented regulatory measures against TikTok and those that have discussed but not yet implemented such measures. Google searches were conducted using keywords like "TikTok Ban," "Fine TikTok," "TikTok Regulation," and "Block TikTok" to compile a list of countries regulating TikTok from 2020 to 2023. TikTok was chosen as the focus from 2020 due to the U.S. declaring it a national security threat. Data collection concluded on December 15, 2023, with 38 countries identified for study. Information was gathered from official statements, bills, hearing documents, investigation reports related to TikTok, primarily from government sources, and analyzed to represent national threats posed by TikTok. A total of 90 text documents were collected.

Research Findings

Data Threat is the Major National Concern to TikTok

According to the typology of social media national threat perceptions, it is found that many countries recognize multiple types of threats from TikTok. Figure 2 displays the distribution and combination of four types of social media national threat perceptions concerning TikTok. It can be observed that the perception of threats to national-level

data is the highest. In 38 countries, not only do 35% of them perceive TikTok threats solely from national data security, but there are 53% of countries where the threat combinations involve national data threat. An interesting finding emerges when observing threats categorized as data and content separately: the proportion of threats related to TikTok's content matches the proportion of data, as depicted in Figure 3. Those indicates that data has become one of the important attributes of TikTok, and both content and data threats posed by TikTok receive quite equal concerns from these countries.

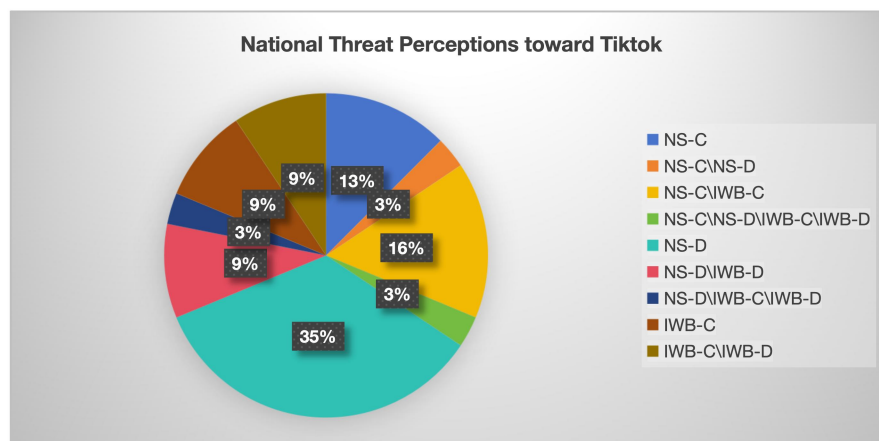


Figure 2 TikTok Threat Perceptions

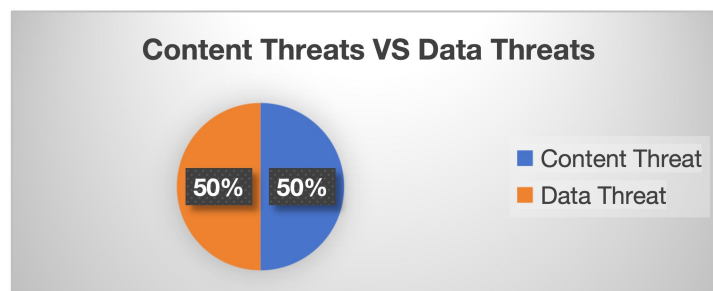


Figure 3 Content Threats VS Data Threats

The Politicization of TikTok Regulation

The extensive research about TikTok regulations is closely related to geopolitical factors amid the intensifying competition among major powers, especially related to the relations between China and the United States. To further understand the geopolitical impact on TikTok, this study expanded the sample size to 38 countries. Further division based on the political identity of these countries revealed that among the 32 countries that have officially regulated TikTok, 11 of them are G20 members, and 9 of them are APEC members. However, among the top 20 countries in terms of user volume, only 9 countries have implemented regulatory measures on TikTok. This indicates that countries with significant political and economic power show more

attention to TikTok.

Exploring whether the United States affects other countries' regulation of TikTok, the data reveals that among the 38 countries, 18 are U.S. allies, with 14 of them adopting similar regulatory measures as the United States—prohibiting the installation of TikTok on government devices. Eight countries implemented these measures after the United States banned TikTok installation on government devices in 2023. And seven countries, mainly U.S. allies or European Union members, mentioned other countries in their statements regarding TikTok regulation. France (Reuters, 2023) and Canada (Government of Canada, 2023), for example, made it clear when they banned TikTok from government devices that they were aligned with their international partners. New Zealand also said the action was taken following a discussion with their colleagues across government and internationally (New Zealand Parliament, 2023). Hence, it can be inferred that to some extent, the U.S. approach to restrict TikTok has been emulated among its allies. Moreover, Italy, Norway, Belgium, and the Netherlands are seven countries that directly referenced China or the Chinese Communist Party in their official statements regarding TikTok, which has been one of the core reasons the United States perceives TikTok as a threat (Schumer & Cotton, 2019).

National Threat Perceptions and Responses toward TikTok

(1) National Security-Data Threats Trigger Isolative Regulation Response

We correlated each threat with four types of regulation, the results are presented in Table 4. The correlation coefficient of NS-Data and No TikTok on Official Device is 0.939, indicating a strong positive correlation. That means the more a country perceives TikTok as a threat to national security through data, the more likely it is to prohibit the installation of TikTok on government devices.

Table 4: Correlation between TikTok national Threats and Regulatory Measures

	Completely Ban	No TikTok on Official Device	Content Regulation	Privacy Regulation
NS-Cont	0.254	-0.461	0.279	-0.266
NS-Data	-0.412	0.939	-0.666	0.108
IWB-Cont	0.332	-0.700	0.473	0.110
IWB-Data	-0.131	0.000	0.120	0.833

To further validate the extent to which the national security-data threat leads a country to isolate TikTok on government devices, we present all the countries that perceive TikTok as having a national security-data threat, as shown in Table 5. Among the 17

countries that consider TikTok to pose a national security-data threat, except for India, which completely banned TikTok, the remaining 16 countries have implemented measures to isolate TikTok on government devices. Therefore, it can be argued that the national security-data threat plays a predominant role in prompting these countries to adopt measures isolating TikTok in confidential devices.

Table 5 Nations Consider TikTok Threats from National Security-Data

TikTok Threats	Country	No TikTok on Official Device (Yes or No)
NS-D	Korea,Estonia,Latvian,Malta,Canada, Denmark,Norway,Australia,Japan, France,New Zealand	Yes
NS-C\NS-D	Belgium	Yes
NS-C\NS-D\ IWB-C\IWB-D	America	Yes
NS-D\IWB-D	Ireland,Britain, Netherland	Yes
NS-D\IWB-C\ IWB-D	India	No

From a national security and data threat perspective, countries are worried about the use of social media by foreign nations or agents to acquire confidential information, manipulate data, and carry out cyber attacks. Government information is highly sensitive, so when addressing the threat that social media poses to national security, especially data-related risks, countries typically focus on preventing social media platforms from connecting to government devices. This helps minimize the risk of social media gaining access to sensitive state information.

(2) Individual Well Being-Data Threat Trigger Privacy Regulation Response

Among the sample of 38 countries, seven (America, Britain, Netherland, Turkey, Ireland,Vietnam, France) have adopted privacy regulation measures concerning TikTok, all citing inadequate protection of user personal data by TikTok, especially concerning adolescent user data. The most prevalent means of privacy regulation involves fines, 5 out of 7 adopted privacy regulation countries have levied substantial fines against TikTok for its inadequate data protection. Additionally, Vietnam has formally demanded that TikTok comply with its national personal data protection requirements (Vietnamnews, 2023). France has mandated its national entities to participate in TikTok's "Clover" project for EU data localization (Kayali, 2023). These countries have raised significant doubts regarding TikTok's protection of user personal data, hence primarily opting for regulatory actions through privacy

compliance.

As can be seen from the correlation of single variables in Table 4, when TikTok is considered a threat to individual well being-data(IWB-D), the country is more inclined to adopt countermeasures of privacy regulation. The correlation coefficient of IWB-D and Privacy Regulation is 0.833, indicating a positive strong correlation. In addition, 7 of the 8 countries that perceive TikTok exists a threat to individual well-being data have taken steps to regulate privacy, specifically 5 of them fine TikTok because of user privacy violation, illustrated in Table 6. This also indicates that individual well-being-data threats play a predominant role in leading countries to adopt privacy regulations.

Table 6 TikTok Threat Perceptions of Country Adopted Privacy Regulation

TikTok Threats	Country	Privacy Regulation	Fine TikTok
NS-D/IWB-D	Ireland, Britain, Netherland	Yes	Yes
NS-C/NS-D/IWB-C/IWB-D	America	Yes	Yes
IWB-C/IWB-D	Turkey	Yes	Yes
IWB-C/IWB-D	Vietnam,Italy	Yes	No
NS-D/IWB-C/IWB-D	India	No	No

(3) Content-oriented Threats Trigger Complete Bans or Content Regulation Response

When investigating a country's perception of threats from TikTok stemming from national security content (NS-C)and individual well-being content(IWB-C), their response measures become more complex. Among the 12 countries perceiving TikTok threats to include national security content, 7 fully encompass those perceiving threats from individual well-being content. Furthermore, some of these countries have implemented complete bans, while others have adopted content regulation measures, as shown in Table 7.

Table 7 TikTok Threat Perceptions of Country Adopted Completely Ban and Content Regulation

TikTok Threats	Country	Completely Ban	Content Regulation
NS-C/NS-D	Belgium	No	No
NS-C/NS-D/IWB-C/IWB-D	America	No	No
NS-C/IWB-C	Jordan, Kenya, Pakistan	No	Yes
NS-C/IWB-C	Egypt, Nepal, Somalia	Yes	No
NS-C	Malaysia, Thailand,	No	Yes

NS-C	Azerbaijan, Senegal	Yes	No
------	---------------------	-----	----

A more in-depth analysis of countries implementing a complete ban reveals that, the country's domestic situation and religions will strongly affect national social media regulation. If the country is in a situation of internal turmoil or conflict, it is more inclined to ban the use of social media nationwide. The complete ban on TikTok in India is widely believed to be directly related to the border conflict between India and China at that time (Ellis, 2020). Similarly, during the escalation of tensions in the Nagorno-Karabakh region, Azerbaijan officially suspended TikTok, citing national security reasons and stating that the platform was spreading military secrets and misinformation (State Security Service of the Republic of Azerbaijan, 2022). In Senegal, during nationwide protests following the sentencing of opposition leader Ousmane Sonko, the government blocked several popular social media applications including TikTok to prevent expanding its crackdown on dissenting voices (Dione & Kouam, 2023). In 2022, Jordan also announced a temporary ban against TikTok, following the death of a police officer during clashes with protesters (NBC News, 2022).

Countries like Nepal, Somalia, Afghanistan, and Kyrgyzstan, which have banned TikTok, are more concerned about TikTok content threats to religious beliefs. For instance, the Nepalese government believes that TikTok's harmful content affects "social harmony". (Sharma, 2023). In Somalia, a Muslim-majority country, the government justified the ban on TikTok, along with the closure of over 40 platforms, including Facebook and Twitter accounts and websites labeled as "terrorist accounts," citing security and moral reasons (Caato, 2023). In Afghanistan, still in turmoil and under Taliban rule, the strict control over societal entertainment activities led to the banning of TikTok and the popular online game PUBG (Azadi, 2022). Kyrgyzstan closed TikTok, citing concerns about its impact on children's mental health, but this move is viewed as part of the government's efforts to restrict freedom of speech and information flow (RFE/RL's Kyrgyz Service, 2023). Bangladesh (Ahamed, 2020) and Pakistan also banned TikTok due to the widespread dissemination of immoral content. However, after TikTok complied with content regulation requirements, Bangladesh and Pakistan reinstated the use of TikTok. .

In addition, countries like Italy, Vietnam, Kenya, and Malaysia have also recognized

the risks associated with TikTok's content. However, instead of implementing more extreme banning measures, they have requested TikTok to enhance its content regulation capabilities. In 2021, Italy authorities ordered TikTok to block the accounts of all Italian users whose age couldn't be verified, after a 10-year-old girl died while using TikTok (Balmer, 2021). Following a thorough investigation, Vietnamese authorities request TikTok delete all content violating Vietnamese laws, prevent their reposting, enhance compliance with local laws in their community guidelines, and provide information to address platform violations (Vietnamnews, 2023). In Kenya, the parliament reached an agreement not to ban TikTok but sought content regulation. Then, TikTok established an office in Kenya for content moderation (Eng, 2023). Malaysia issued a warning to TikTok over alleged blocking of pro-Palestinian content. The Communications Minister stated that if TikTok continued to block such content, decisive action might be taken (Reuters, 2023). 2023 Thailand's Election Commission ECT has partnered with TikTok to help set up information hubs and debunk misinformation during the general election (English, 2023). From these specific cases, it can be seen that when TikTok's content poses a threat to some countries with domestic stability and democracy, these countries are more inclined to deal with the risk by improving TikTok's content moderation capabilities.

Conclusion

Through our research on global TikTok regulations, we have observed a growing recognition among countries of the risks presented by social media at the data level. Both content and data have emerged as the main sources of threats from digital social media to nations. In the regulation of TikTok, geopolitical considerations play a crucial role. Amidst the escalating competition between the United States and China, Chinese enterprises have garnered significant attention from the U.S., resulting in concerted pressure on TikTok through allied nations. The analysis of the interplay between national threat perceptions from social media and regulatory actions reveals that when a country perceives TikTok as a data-level national threat, there is a tendency to enforce measures that isolate TikTok from critical devices to safeguard national security. In cases where TikTok is viewed as a threat to individual well-being at the data level, countries tend to introduce privacy regulations that often entail imposing fines on TikTok and requiring the platform to enhance its data protection capabilities. When TikTok's content is deemed a national threat, countries may resort to implementing strict measures such as complete bans and content regulations. In

nations grappling with domestic instability or strong religious convictions, there is a proclivity towards outright bans on social media. Conversely, in countries characterized by domestic stability and democratic values, there is a preference for content regulation, with an emphasis on urging TikTok to enhance its content moderation mechanisms to curb the dissemination of harmful content.

This study enriches the classic research topic of the interaction between media and the state by constructing a typology of social media threats to national security. By categorizing social media threats into content and data dimensions, as well as distinguishing between national and individual security, the study narrows down the complexity of media impact on national security. This effort represents an academic endeavor to prevent the deteriorative securitization in the policy realm. While data-driven digitization indeed brings more security risks, formulating reasonable regulatory policies requires an accurate understanding and assessment of the security implications of this digitization. Through an analysis of the regulatory practices adopted by 38 countries towards TikTok, this study reveals diverse national threats and response strategies among different nations. Future research could delve into the reasons behind countries' varying threat perceptions and responses to the same social media platform. I believe this study will make a significant contribution to traditional media system research.

Reference

- 47NEWS. (2023, February 27). 公用スマホ TikTok など禁止 松野氏、機密情報扱う機器で. 47NEWS. <https://www.47news.jp/8993985.html>
- Aday, S., Farrell, H., Lynch, M., Sides, J., & Freelon, D. (2012). New media and conflict after the Arab Spring. United States Institute of Peace (Peaceworks No. 80). <https://www.files.ethz.ch/isn/150696/PW80.pdf>
- Ahamed, S. (2020, August 6). TikTok will remove 'offensive' videos, Bangladesh minister says. Bdnews24.Com. <https://bdnews24.com/technology/tiktok-will-remove-offensive-videos-bangladesh-minister-says>
- Azadi, R. R. (2022, April 21). Taliban bans TikTok, popular video game in Afghanistan. RadioFreeEurope/RadioLiberty. <https://www.rferl.org/a/taliban-bans-tiktok-video-game-pubg/31814523.html>
- Bailey, K. D. (1994). Typologies and taxonomies. SAGE.
- Bajpai, M. K., Singh, K. K., & Giakos, G. (2021). Machine vision and augmented intelligence-theory and applications.
- Balmer. (2021, January 23). Italy tells TikTok to block users after death of young girl.

- Reuters. <https://www.reuters.com/article/idUSKBN29R2H5/>
- Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77–101.
- Caato, B. M. (2023, August 26). Outcry in Somalia over government decision to ban TikTok, Telegram. Al Jazeera. <https://www.aljazeera.com/news/2023/8/26/outcry-in-somalia-over-government-decision-to-ban-tiktok-telegram>
- Cyberspace Administration of China (CAC). (2020, March 1). Provisions on the governance of the online information content ecosystem.
- Carr, C. T., & Hayes, R. A. (2015). Social media: Defining, developing, and divining. *Atlantic Journal of Communication*, 23(1), 46–65.
- Cartwright, M. (2020). Internationalising state power through the internet: Google, Huawei and geopolitical struggle. *Internet Policy Review*, 9(3).
- Chen. (2022). Digital wild west: Foreign social media bans, data privacy, and free speech. *UC Law SF Communications and Entertainment Journal*, 44(2).
- Deliri, S., & Albanese, M. (2015). Security and privacy issues in social networks. In F. Colace, M. De Santo, V. Moscato, A. Picariello, F. A. Schreiber, & L. Tanca (Eds.), *Data management in pervasive systems*. Springer.
- Dione, & Kouam. (2023, August 3). Senegal blocks TikTok in widening clampdown on dissent. Reuters. <https://www.reuters.com/world/africa/senegal-suspends-tiktok-saying-it-was-threatening-stability-2023-08-02/>
- Dong. (2021). A preliminary exploration of the development of digital media in international communication: A case study of the global expansion of TikTok and the U.S. ban. *PR Magazine*, 9, 134–136. (in Chinese). <https://doi.org/10.16645/j.cnki.cn11-5281/c.2021.09.045>
- Ellis-Petersen, H. (2020, June 30). India bans TikTok after Himalayan border clash with Chinese troops. *The Guardian*. <https://www.theguardian.com/world/2020/jun/29/india-bans-tiktok-after-himalayan-border-clash-with-chinese-troops>
- Eng, T. A. (2023, August 15). Kenyan parliament receives TikTok ban petition. *TRT Afrika*. <https://www.trtafrika.com/africa/kenyan-parliament-receives-tiktok-ban-petition-14489683>
- English, K. (2023). Despite western countries' bans, TikTok plays a role in the Thai election.
- Executive Order. (2020). Executive Order 13942 of August 6, 2020. In *Presidential Documents*.
- Gale, W. G., Holmes, S. E., & John, D. C. (2015). Social security coverage for state and local government workers: A reconsideration. *The Journal of Retirement*, 26.
- Gerring, J. (2012). Mere Description. *British Journal of Political Science*, 42(4), 721–746.
- Ghazaleh, B. (2018). Social media and user privacy. *arXiv Preprint arXiv:1806.09786*.
- Beigi, G., & Liu, H. (2019). Identifying novel privacy issues of online users on social

- media platforms. *ACM SIGWEB Newsletter*, 2019, 1-7.
<https://doi.org/10.1145/3293874.3293878>
- Gilboa, E. (2005a). Global Television News and Foreign Policy: Debating the CNN Effect. *International Studies Perspectives*, 6(3), 325–341.
- Gilboa, E. (2005b). The CNN Effect: The Search for a Communication Theory of International Relations. *Political Communication*, 22(1), 27–44.
- Goodin, B. (2020, August 9). Banning TikTok and stoking Sinophobia isn't likely to get Trump reelected. *Washington Post*.
<https://www.washingtonpost.com/outlook/2020/08/10/banning-tiktok-stoking-sinophobias-isnt-likely-reelect-trump/>
- Government of Canada. (2023, February 27). Statement by Minister Fortier announcing a ban on the use of TikTok on government mobile devices.
<https://www.canada.ca/en/treasury-board-secretariat/news/2023/02/statement-by-minister-fortier-announcing-a-ban-on-the-use-of-tiktok-on-government-mobile-devices.html>
- Hobbes, T. (1909). *Leviathan*. Reprinted from the Edition of 1651. With an Essay by the Late W.G. Pogson Smith.
- Honigsheim, P. (1946). From Max Weber: Essays in Sociology. *American Journal of Sociology*, 52(4), 376–378.
- Howard, P. N., & Parks, M. R. (2012). Social media and political change: Capacity, constraint, and consequence. *Journal of Communication*, 62, 359–362.
- Huber, D. M., Stewart, K. N., & Tjoa, S. (2009). Towards Automating Social Engineering Using Social Networking Sites. *Proceedings - 12th IEEE International Conference on Computational Science and Engineering, CSE 2009*, 117-124.
- Jamieson, K. H. (2020). *Cyberwar*. Oxford University Press, USA.
- Ji, S., Li, W., Srivatsa, M., He, J. S., & Beyah, R. (2016). General Graph Data De-Anonymization. *ACM Transactions on Information and System Security*, 18(4), 1–29.
- Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of social media. *Business Horizons*, 53, 59–68.
- Kayali, L. (2023, July 6). French senators want a wider TikTok ban. *POLITICO*. Retrieved from
<https://www.politico.eu/article/french-senators-want-a-wider-TikTok-ban/>
- Kent, M. L. (2010). Directions in social media for professionals and scholars. In R. L. Heath (Ed.), *Handbook of public relations* (2nd ed., pp. 643–656). Thousand Oaks, CA: Sage.
- Hussain, M. M., & Howard, P. N. (2013). What best explains successful protest cascades? ICTs and the fuzzy causes of the Arab Spring. *International studies review*, 15(1), 48-66.
- Keohane, R. O., & Nye, J. S. (1998). Power and Interdependence in the Information Age. *Foreign Affairs*, 77(5), 81.
- Kuang, & Zhang. (2020). The Globalization Predicament of Chinese Social Media in a Geopolitical Environment: A Case Study of TikTok. *International Communications*, 11(4), 4–6. (in Chinese)

- Kumar, A. (2023). State nationalism or popular nationalism? Analysing media coverage of TikTok ban on mainstream Indian TV news channels. *Media Asia*, 50(4), 616-632.
- Kumar, A., & Thussu, D. (2023, May 21). Media, digital sovereignty and geopolitics: The case of the TikTok ban in India. *Media, Culture & Society*, 45(8), 1583–1599.
- Kutschera, S. (2022). Incidental data: Observation of privacy compromising data on social media platforms. *International Cybersecurity Law Review*, 4(1), 91–114.
- Leist, A. K. (2013). Social Media Use of Older Adults: A Mini-Review. *Gerontology*, 59(4), 378–384. <https://doi.org/10.1159/000346818>
- Liu. (2001, April). On the Basic Meaning, Genesis, and Development of National Security. *Journal of North China Electric Power University(Social Sciences)*, 62–65. (in Chinese)
- Lusk, A. (2018, April 12). Moving Beyond the CNN Effect or Stuck in the Middle? How Relational Sociology Remaps Media and Security Studies. *International Studies Review*, 21(1), 1–11.
- Mao, H., Shuai, X., & Kapadia, A. (2011). Loose tweets: An analysis of privacy leaks on Twitter. 10.1145/2046556.2046558.
- Mayer-Schonberger, V., & Cukier, K. (2013, March 14). *Big Data*. Hachette UK.
- McCabe, D., & Kang, C. (2023, March 15). TikTok Pushed by U.S. to Resolve National Security Concerns. *The New York Times*. Retrieved from <https://www.nytimes.com/2023/03/15/technology/tiktok-biden-pushes-sale.html>
- Mendelsohn, B. (2011). Foreign Fighters—Recent Trends. *Orbis*, 55(2), 189–202.
- Meleagrou-Hitchens, A., & Kaderbhai, N. (2017). Research perspectives on online radicalisation: A literature review, 2006–2016. *International Centre for the Study of Radicalisation*, 19, 1-98.
- Meng, & Li. (2020). The Social Motivations and Formation Mechanisms Behind the Trump Administration’s “TikTok Ban.” *International Communications*, 10(11), 57–59. (in Chinese)
- Meta. (2023). Facebook Community Standards.
- Mishra, M., Yan, P., & Schroeder, R. (2022). TikTok politics: Tit for tat on the India–China cyberspace frontier. *International Journal of Communication*, 16, 814–839.
- Napoli, P. M. (2019). User data as public resource: Implications for social media regulation. *SSRN Electronic Journal*.
- NBC News. (2022, December 17). Jordan bans TikTok after police officer killed in protests. Retrieved from <https://www.nbcnews.com/news/world/jordan-bans-tiktok-police-officer-killed-protests-rcna62229>
- New Zealand Parliament. (2023, March 17). Media statement: TikTok on Parliamentary Service devices.
- O’Reilly, M., Dogra, N., Whiteman, N., Hughes, J., Eruyar, S., & Reilly, P. (2018). Is social media bad for mental health and wellbeing? Exploring the perspectives of adolescents. *Clinical Child Psychology and Psychiatry*, 23(4), 601–613.
- Pan. (2020, March). Breaking through the challenges in the United States for TikTok,

WeChat, and others: A dual perspective from international relations and law. Law-Based Society, 5, 65–73. (in Chinese)

PIB Delhi. (2020, June 29). Government bans 59 mobile apps which are prejudicial to sovereignty and integrity of India, defence of India, security of state and public order. Retrieved from <https://pib.gov.in/PressReleaseDetailm.aspx?PRID=1635206>

Renming Paper. (2014, April 16). Xi Jinping presides over the first meeting of the Central National Security Commission, emphasizing the establishment of a centralized, unified, efficient, and authoritative national security system. Retrieved from http://paper.people.com.cn/rmrbhwb/html/2014-04/16/content_1415585.htm

Reuters. (2023a, March 24). France to ban TikTok on work phones of civil servants - minister. Retrieved from <https://www.reuters.com/technology/france-ban-tiktok-work-phones-civil-servants-minister-2023-03-24/>

Reuters. (2023b, October 26). Malaysia warns TikTok, Meta over alleged blocking of pro-Palestinian content. Retrieved from <https://www.reuters.com/technology/malaysia-warn-tiktok-meta-over-alleged-blocking-pro-palestinian-content-minister-2023-10-26/>

RFE/RL's Kyrgyz Service. (2023, August 30). Kyrgyz authorities ban TikTok citing effects on child development. Retrieved from <https://www.rferl.org/a/kyrgyzstan-tiktok-ban-children/32571122.html>

Riaz, D. (2020). Regulatory tactics to ban TikTok: Case studies from Pakistan, India and the US. <https://doi.org/10.13140/RG.2.2.12506.11208>

Ripsman, N. M., & Paul, T. (2010). Globalization and the National Security State. Oxford University Press.

Rosenbach, E., & Mansted, K. (2019). The geopolitics of information. Belfer Center for Science and International Affairs.

Sageman, M. (2011). Leaderless Jihad. University of Pennsylvania Press.

Schumer, & Cotton. (2019, October 23). TikTok letter. Senate.gov.

Sharma, B. (2023, November 14). Nepal is banning TikTok over hate content, officials say. The New York Times. Retrieved from <https://www.nytimes.com/2023/11/13/world/asia/tiktok-nepal-ban.html>

Shen, H., & He, Y. (2022). The geopolitics of infrastructuralized platforms: The case of Alibaba. Information, Communication & Society, 25(16), 2363–2380.

Song, L., & Ray, A. (2023). “How can a small app piss off an entire country?”: India’s TikTok ban in the light of everyday techno-nationalism. Inter-Asia Cultural Studies, 24(3), 382–396.

State Security Service of the Republic of Azerbaijan. (2022, September 14). Information of the Press service of the State Security Service. Retrieved from <https://www.dtx.gov.az/en/news/1715.html>

Statista. (2023, August 29). Number of worldwide social network users 2027. Retrieved from <https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/>

Terry, M. (2009). Twittering healthcare: Social media and medicine. Telemedicine

and e-Health, 15, 507–510.

U. S. Congress. (2021). No TikTok on Government Devices Act. In Congress.gov (S.1143 — 117th Congress (2021-2022)), May 12.

U.S. Government Accountability Office. (2022). Information Environment: Opportunities and Threats to DOD's National Security Mission (GAO-22-104714). September 21.

UK Online Harms White Paper. (2020). GOV.UK. December 15.

Van Dijck, J., & Poell, T. (2013). Understanding Social Media Logic. *Media and Communication*, 1(1), 2–14.

Vietnamnews. (2023, October 6). Inspection results on TikTok operations in Việt Nam released, multiple violations detected. Vietnamnews. Retrieved from <https://vietnamnews.vn/society/1594820/inspection-results-on-tiktok-operations-in-vi-nam-released-multiple-violations-detected.html>

Weggemans, D., Bakker, E., & Grol, P. (2014). Who are they and why do they go? The Radicalization and Preparatory Processes of Dutch Jihadist Foreign Fighters, 8, 100-110.

White House. (2022, October 22). United Nations National Security Strategy. White House.

Wolford, B. (2023, September 14). What is GDPR, the EU's new data protection law? GDPR.eu. Retrieved from <https://gdpr.eu/what-is-gdpr/>

XinhuaNews. (2014, April 15). Xi Jinping: Uphold the Overall National Security Concept and Follow the Path of National Security with Chinese Characteristics.

XinhuaNews. [In Chinese] Retrieved from http://www.xinhuanet.com/politics/2014-04/15/c_1110253910.htm

Zhang, J. X., Xue, S., Sun, J. C., Zhang, R., & Zhang, Y. C. (2018). Privacy-preserving social media data outsourcing. In Proceedings of the IEEE International Conference on Computer Communications (INFOCOM'18).