International Journal of Education and Humanities
ISSN: 2770-6702 | Vol. 17, No. 3, 2024

The Risks of TikTok in the Context of Digital Sovereignty: A Case Study of the U.S. Ban on TikTok

Yuquan Liu

Shanghai Maritime University, Shanghai 201306, China

Abstract: TikTok stands out as the top choice for digital social networking among the youth in the United States, despite being viewed by the U.S. authorities as a potential risk to the nation's security. Over the past few years, the concept of digital sovereignty has gained prominence, with growing global interest and scrutiny from the international community regarding this matter. This article organizes the relevant concepts of digital sovereignty, discusses geopolitics and digital boundaries, reviews the ban on TikTok in the United States, and combines the background of digital sovereignty with the ban on TikTok to draw a conclusion: TikTok poses a threat to the U.S. government and society in terms of data collection, algorithmic control, and political influence, and these threats are part of the background of digital sovereignty. Ultimately, this article calls for a joint effort from the international community to balance the relationship between data security, freedom of information, and technological innovation, and to strengthen the emphasis on the issue of digital sovereignty.

Keywords: Digital Sovereignty; Ban on TikTok; Digital Boundaries; U.S. Authorities; Political Influence.

1. Introduction

In the contemporary era, as geopolitical competition and economic confrontation become increasingly intertwined and complex, the traditional understanding of national sovereignty has been challenged. Especially, the advancement of digital technology has led to a reevaluation of the notions of sovereignty, boundaries, and territoriality (Glasze et al., 2022). This pivotal transformation has generated a growing appetite for "digital sovereignty" across various governmental entities and populations. Within diverse political landscapes, including those of China, Russia, India, and the European Union, there is a push for nations to assert a more robust presence in the pursuit of strategic self-determination and the establishment of digital frontiers. In the early 2000s, Europe initiated the advocacy for the notion of "digital sovereignty" as a means to tackle the emerging challenges of the digital era (Budnitsky & Jia, 2018). The term "digital sovereignty" became widely known after Snowden's revelations in 2013 and quickly became part of the political agenda in several European countries (Glasze et al., 2022). This discourse is not confined to the EU sphere but is also central to policy debates within each constituent nation, highlighting Europe's quest for technological self-sufficiency to diminish reliance on dominant nations like the United States and China (Farrand & Carrapico, 2022). The ongoing dialogue on digital sovereignty mirrors the conflict between legal and political imperatives and societal norms during the digital transformation phase. Moreover, widely-used phrases like "technological sovereignty" and "data sovereignty" underscore the increasing demand for bolstering national governance in the digital realm. The conversation and implementation of digital sovereignty can be perceived as the crystallization and embodiment of these emerging geopolitical data dynamics (Glasze et al., 2022). Countries are striving to "territorialize" the digital domain by establishing data jurisdiction, ensuring the security of information infrastructure, and constructing normative frameworks for national and citizen identity, thereby shaping various aspects of digital territory (Möllers, 2021). This process has not only changed the practical operation of sovereignty but also posed new challenges to international relations and global governance. The U.S. government's security measures against TikTok also confirm that digital content is increasingly becoming a site and tool for geopolitical confrontation and geo-economic competition (Ash et al., 2018). Currently, there are few articles discussing TikTok in conjunction with digital sovereignty, so this paper, starting from the concept and theoretical framework of digital sovereignty, takes the ban on TikTok in the United States as an example, reviews the ban on TikTok in the U.S., and discusses the risks TikTok poses to the U.S. in the context of digital sovereignty.

2. Digital Sovererignty: The Notion

Digital sovereignty is not a term with a clear definition, but rather encompasses a variety of approaches, concepts, and needs (Glasze et al., 2022). Nevertheless, a fundamental aspect is that sovereignty necessitates a degree of authority to establish, sustain, or potentially extend, with diverse entities employing the concept of digital sovereignty in a multitude of manners (Couture & Toupin, 2019). At present, crafting a universal definition is challenging, as nations, global entities, advocates, and various other stakeholders articulate this notion through distinct instruments, technological frameworks, and perspectives. In conceptual terms, "digital sovereignty" exemplifies the rationale for treating "sovereignty" as a geopolitical construct that is enacted by a range of players, contingent on context, and designed to fulfill particular political objectives (Glasze et al., 2022). The primary objective of digital sovereignty is to enable various stakeholders to exercise their autonomy and self-determination within a society that is increasingly shaped by data (Couture & Toupin, 2019). These frameworks, crafted by governments and civil society organizations, are drawing the interest of numerous participants who aim to reestablish their control and self-determination over digital technologies and infrastructures (Glasze et al., 2022). Digital sovereignty expands the claim of sovereignty beyond the confines of the state. It builds upon the traditional notion of sovereignty, enabling a variety of entities and even individuals to claim

and exert their sovereign rights. Digital sovereignty has a certain impact on policy-making (Broeders et al., 2023). For the French Ministry of Armed Forces, any cyber assault aimed at French computer systems or digital activities that affect French territory "can at the very least be considered a violation of sovereignty." The crux of the matter is that both legal frameworks governing international data transfers and the evolving geopolitics of cybersecurity serve as mechanisms for nations and other entities to create digital territories and redefine the spatial aspects of sovereignty in the digital era. This is achieved through legislative, communicative, and technological practices.

3. TikTok: A Review of the Ban Incident in the United States

TikTok is a short video social platform developed by the Chinese company ByteDance. It was first launched in China in 2016 under the name "Douyin" and entered the international market in 2017 as TikTok, targeting regions outside mainland China, Hong Kong, and Macau. Its unique feature is the algorithmic recommendation system, which automatically recommends videos based on user interests, greatly enhancing user engagement and platform stickiness.

TikTok's popularity in the United States is very high and continues to grow. According to statistical data from 2024, TikTok has about 170 million monthly active users in the U.S. (Monthly TikTok User Engagement in the U.S 2019-2020, 2022). The average American user spends 53.8 minutes per day on TikTok, showing a very high level of user engagement. TikTok's user base is mainly young people, with more than half of the weekly active users in the United States aged between 18 and 34 (Backlinko Team, 2024). TikTok is not only an entertainment application but has also successfully transformed itself into a discovery platform, with more and more marketers planning to increase their investment on the platform. Since 2020, TikTok has always been at the forefront of social platform popularity in the United States, surpassing the previously most popular platform, Facebook (Figure 1). However, this social software, widely loved by young people, is considered by the U.S. government to be a threat to national security. Since 2019, the U.S. government has continuously taken measures to suppress TikTok, plunging it into a ban controversy.

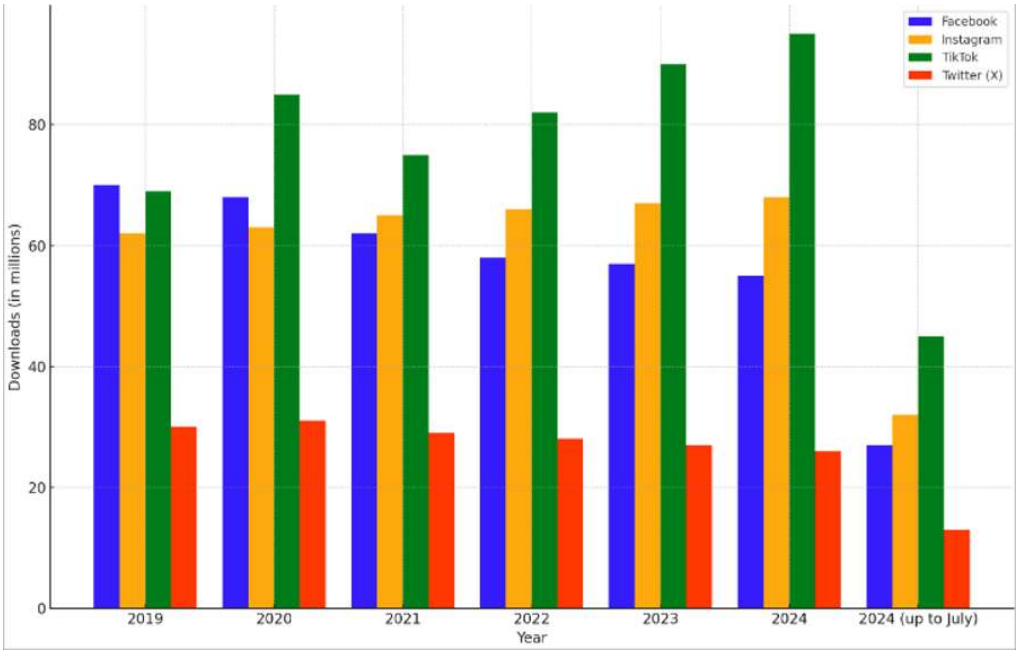

Figure 1. Social Media Platform Downloads in the US (2019-2024)
Data Source: Statistia

Table 1. TikTok Ban review table

2019.2	The US Federal Trade Commission imposed a penalty of $5.7 million on TikTok.
2019.11	The Trump administration initiated a probe into ByteDance's acquisition of Musical.ly, citing national security concerns as the rationale.
2020.9	TikTok rejected Microsoft's offer
2021.2	The US government has asked a federal appeals court to put on hold a lawsuit challenging TikTok's ban
2021.6	President Joe Biden enacted an executive order that overturned the prohibition on TikTok that had been established by his predecessor, Donald Trump, during his tenure.
2023.3	TikTok CEO is paid to attend Congressional hearings this week
2023.5	Montana's Republican governor has signed a bill banning TikTok downloads statewide
2024.3	The United States has proposed a legislative day that would limit ByteDance to divest TikTok within a certain period of time, otherwise it will be banned
2024.4	The Senate voted 79-18 to pass the TikTok spinoff bill
2024.4	US President Joe Biden signs the divestiture bill.

Source: https://www.imtiktoker.com/article/1679

On December 22, 2023, the Biden administration in the United States signed the H.R.2670 - National Defense Authorization Act for Fiscal Year 2024. This bill mandates a ban on the use of TikTok on government devices, including federal government devices and personal devices on the Department of Defense information network.

On April 24, 2024, the Biden administration signed the H.R.815 - Making emergency supplemental appropriations for the fiscal year ending September 30, 2024, and for other purposes bill. The bill prohibits all covered applications, including TikTok, within 270 days of its enactment, unless the application is divested from China.

Since the 118th Congress of the United States (2023-2024), the proportion of bills related to TikTok that call for a complete ban on TikTok across the country is as high as 81.6% (Figure 2). Among the bills that do not explicitly call for a comprehensive ban, almost all require a ban on TikTok under certain specific circumstances.

However, according to the records of the White House press conferences, as high as 68.4% of the records clearly indicate that the United States will not ban TikTok (Figure 3). Currently, the U.S. government has not explicitly stated the name of the enterprise or institution that will acquire TikTok in the future. Moreover, given TikTok's past resistance to the U.S. government's coercive measures, the future development of the situation remains uncertain, making it difficult to determine the outcome of the TikTok ban incident in the United States at present.

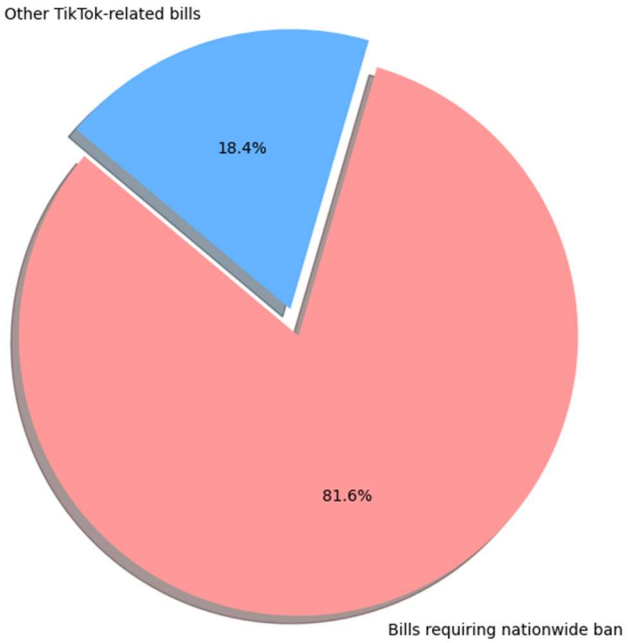

Figure 2. Proportion of US Bills Related to TikTok:Nationwide Ban vs.Other Bills
Source: http://congress.gov

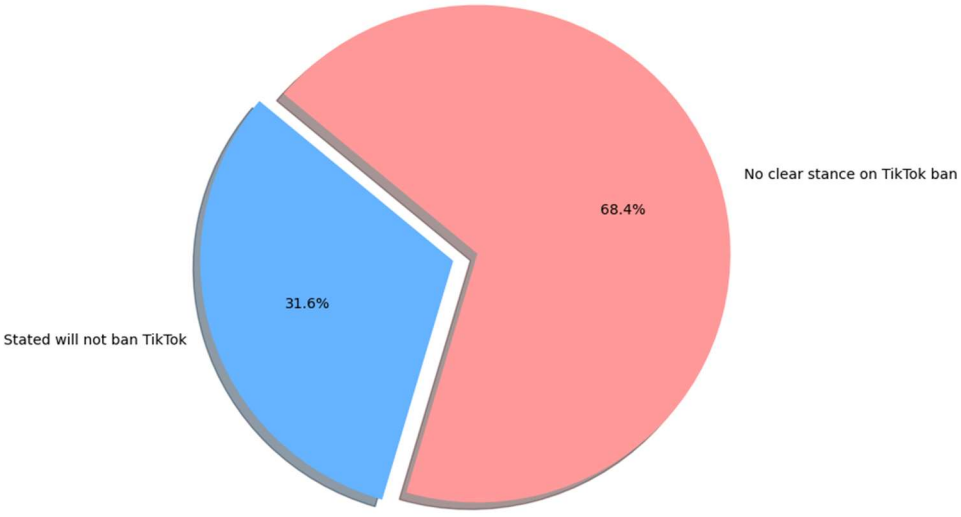

Figure 3. White House Stance on TikTok Ban in Press Conferences since 2023
Source: https://whitehouse.gov

4. Digital Sovereignty and TikTok

At a U.S. House Energy Committee hearing in 2023, TikTok CEO Shou Zi Chew repeatedly mentioned the "Texas Project" as a means to ensure that "American data is stored in the United States, safeguarded by an American company, and managed by American personnel". The initial two decades of the 21st century have seen the rise of an actual digital corporate sovereignty. This form of governance is backed by proponents who argue that corporate self-regulation is adequate, viewing legislative oversight as undesirable and superfluous. The multidimensional concept of digital sovereignty is manifested in specific digital platforms with a huge number of users, establishing strong network centrality. This leads to an imbalance of network nodes, providing the state with power and influence beyond its national territory . TikTok's commitment to "store American data in the United States" implies the variability and context-dependence of digital territorial discourse in different backgrounds, which may or may not explicitly use the concept of digital sovereignty, but can "problematize specific threats" and "depict specific enemy images" (Glasze et al., 2022).

The ban on TikTok in the United States is closely related to the concept of digital sovereignty. Digital sovereignty is not only the state's control over its digital space but also includes the community and individuals' control over the digital technologies and platforms they use. We understand digital sovereignty as the "need for control in the digital domain," which includes multiple levels (Falkner et al., 2024). The term "digital sovereignty" can be seen as a shorthand for the connection between sovereignty and digital technology, data, and infrastructure (Becerra & Waisbord, 2021; Couture & Toupin, 2019), which stipulates the need for control over the digital at the physical layer (resources, infrastructure, equipment), the code layer (standards, rules, design), and the information layer (content, data) (Chander & Sun, 2021; Floridi, 2020). Attempts to increase digital control at the physical, code, and information levels belong to the category of digital sovereignty. Control means the ability to influence and restrict the manufacturing (including the mining and processing of necessary raw materials), design, use, and output of digital technology (Falkner et al., 2024).

5. Algorithmic Control and Political Influence

TikTok's algorithm for suggesting content prioritizes videos according to the interactions of users, details about the videos themselves, and the configurations of devices or account preferences (Cheng & Li, 2024). Humans have an innate tendency to be vigilant about dangers in their surroundings and are prone to spreading negative news. This inclination is because adverse information assists individuals in anticipating and preparing for possible negative outcomes (Heath, 1996). Anxiety and anger intensify people's curiosity and focus on political occurrences (Brader et al., 2008). The majority of individuals lack comprehension of how algorithms function, and those with such understanding are typically from a younger demographic and possess higher levels of education. Users with extreme political inclinations can exacerbate the feedback loop that amplifies biased information, thereby granting extreme political perspectives increased visibility on the internet (Shepherd, 2020). Preferences of users and interactions that are algorithmically amplified result in a disproportionate representation of negative emotions, moralizing content, and information that is politically extreme on the platform. (Brady et al., 2023; Arugute et al., 2023). The discordance between the social learning functions and the content algorithm's focus on maximizing engagement can result in suboptimal human-machine interactions within online social networks. This can engender adverse outcomes like heightened social misunderstanding, escalated conflict, and the proliferation of misinformation (Brady et al., 2023). When content algorithms excessively suggest political information, it can amplify users' perceptions of emotional polarization, expressions of anger, and the extremity of ideological views within their social networks (Levendusky & Malhotra, 2016). An inclination towards negative social data aids in the prompt recognition and communication of societal risks (Rozin & Royzman, 2001). The more that users with strong partisan leanings follow algorithmic suggestions, the more their video content tends to align with their own political affiliations (Brown et al., 2022). Political actions that social media users witness in their feeds are indicative of their own tendencies to engage in political posting and offline political activities (Kim & Ellison, 2022). Crafting posts designed to elicit anger and then leveraging positive reactions to these posts raises the probability that users will express anger regarding political matters aligned with their partisan views (Brady et al., 2021). The dissemination of disinformation is viewed as a substantial menace to democratic systems worldwide. Misinformation frequently circulates via social media channels (Bridgman et al., 2020), and there have been calls for social media platforms to take action in rectifying the spread of false information on their services (Clayton et al., 2020). While fact-checking can have an impact, it has faced criticism and there are concerns about potential (partisan) biases (Uscinski & Butler, 2013). The United States is perceived as being more vulnerable to disinformation threats due to elevated levels of polarization and diminished trust in news sources (Humprecht, Esse & Van Aelst, 2020).

6. Conclusion

This article delves into the notion of digital sovereignty, with a particular focus on the TikTok ban episode in the United States, underscoring the intricate and pressing nature of digital sovereignty amidst globalization. By examining the TikTok scenario, the article illustrates that while the Internet was initially conceived to foster the unrestricted exchange of information and worldwide interconnectivity, its actual trajectory has leaned towards prioritizing national security and geopolitical concerns, mirroring the profound, underlying rivalry among nations for dominance in technology and information. The TikTok ban in the U.S. accentuates the multifaceted aspects of digital sovereignty, encompassing not just governmental control over digital infrastructure but also the exertion of authority over data streams, the dissemination of information, and the privacy of users.

By scrutinizing the political sway of TikTok's algorithms and the skew in information distribution, the article highlights the pivotal role of social media platforms in influencing public sentiment and political engagement. Research indicates that TikTok's tailored recommendation algorithms and user interactions not only encourage incidental news consumption but might also intensify the propagation of

negative emotions and radical political content. Moreover, as a principal platform for political campaigning, the engaging and interactive nature of TikTok's content offers innovative avenues for establishing close ties between politicians and the populace.

References

[1] Glasze, G., Cattaruzza, A., Douzet, F., et al. (2022). Contested spatialities of digital sovereignty. Geopolitics, 28(2), 919-958. https://doi.org/10.1080/14650045.2022.2050070

[2] Budnitsky, S., & Jia, L. (2018). Branding internet sovereignty: Digital media and the Chinese-Russian cyberalliance. European Journal of Cultural Studies, 21(5), 594–613. https://doi.org/10.1177/1367549417751151

[3] Farrand, B., & Carrapico, H. (2022). Digital sovereignty and taking back control: From regulatory capitalism to regulatory mercantilism in EU cybersecurity. European Security, 31(3), 435–453. https://doi.org/10.1080/09662839.2022.2102896

[4] Möllers, N. (2021). Making digital territory: Cybersecurity, techno-nationalism, and the moral boundaries of the state. Science, Technology, & Human Values, 46(1), 112–138. https://doi.org/10.1177/0162243920904436

[5] Ash, J., Kitchin, R., & Leszczynski, A. (2018). Digital geographies. SAGE.

[6] Couture, S., & Toupin, S. (2019). What does the notion of "sovereignty" mean when referring to the digital? New Media & Society, 21(10), 2305–2322. https://doi.org/10.1177/1461444819865984

[7] Foridi, L. (2020). The fight for digital sovereignty: What it is, and why it matters, especially for the EU. Philosophy & Technology, 33(3), 369–378. https://doi.org/10.1007/s13347-020-00423-6

[8] Falkner, G., Heidebrecht, S., Obendiek, A., & Seidl, T. (2024). Digital sovereignty - Rhetoric and reality. Journal of European Public Policy, 31(8), 2099-2120. https://doi.org/10.1080/13501763. 2024.2358984

[9] Becerra, M., & Waisbord, S. R. (2021). The curious absence of cybernationalism in Latin America: Lessons for the study of digital sovereignty and governance. Communication and the Public, 6(1–4), 67–79. https://doi.org/10.1177/ 20501582 20974687

[10] Chander, A., & Sun, H. (2021). Sovereignty 2.0. Georgetown Law Faculty Publications and Other Works, 2404. https://doi.org/10.2139/ssrn.3904949

[11] Cheng, Z., & Li, Y. (2024). Like, Comment, and Share on TikTok: Exploring the Effect of Sentiment and Second-Person View on the User Engagement with TikTok News Videos. Social Science Computer Review, 42(1), 201-223. https://doi.org/10.1177/08944393231178603

[12] Heath, C. (1996). Do people prefer to pass along good or bad news? Valence and relevance of news as predictors of transmission propensity. Organizational Behavior and Human Decision Processes, 68(2), 79–94. https://doi.org/10.1006/obhd.1996.0091

[13] Shepherd, R. P. (2020). Gaming Reddit's Algorithm: r/the_donald, Amplification, and the Rhetoric of Sorting. Computers and Composition, 56, 102572. https://doi.org/10.1016/j.compcom.2020.102572

[14] Brady, W. J., Jackson, J. C., Lindström, B., & Crockett, M. J. (2023). Algorithm-mediated social learning in online social networks. Trends in Cognitive Sciences, 27(10), 947-960. https://doi.org/10.1016/j.tics.2023.07.005

[15] Arugute, N., et al. (2023). Network activated frames: content sharing and perceived polarization in social media. Journal of Communication, 73, 14–24. https://doi.org/10.1111/ jcom.12708

[16] Levendusky, M. S., & Malhotra, N. (2016). (Mis)perceptions of Partisan Polarization in the American Public. Public Opinion Quarterly, 80, 378–391. https://doi.org/10.1093/poq/nfw018

[17] Rozin, P., & Royzman, E. B. (2001). Negativity Bias, Negativity Dominance, and Contagion. Personality and Social Psychology Review, 5, 296–320. https://doi.org/10.1177/1088868830100500302

[18] Brown, M. A., et al. (2022). Echo Chambers, Rabbit Holes, and Algorithmic Bias: How YouTube Recommends Content to Real Users. SSRN. https://doi.org/10.2139/ssrn.4114905

[19] Kim, D. H., & Ellison, N. B. (2022). From observation on social media to offline political participation: The social media affordances approach. New Media & Society, 24, 2614–2634. https://doi.org/10.1177/1461444820975465

[20] Brady, W. J., et al. (2021). How social learning amplifies moral outrage expression in online social networks. Science Advances, 7, eabe5641. https://doi.org/10.1126/ sciadv.abe5641

[21] Clayton, K., Blair, S., Busam, J. A., Forstner, S., Glance, G., Green, A., Kawata, A., et al. (2020). Real Solutions for Fake News? Measuring the Effectiveness of General Warnings and Fact-Check Tags in Reducing Belief in False Stories on Social Media. Political Behavior, 42(4), 1073–1095. https://doi.org/10.1007/s11109-019-09533-0

[22] Bridgman, A., Merkley, E., Loewen, P. J., Owen, T., Ruths, D., Teichmann, L., & Zhilin, O. (2020). The Causes and Consequences of COVID-19 Misperceptions: Understanding the Role of News and Social Media. Harvard Kennedy School Misinformation Review, 1(3), 1–18. https://doi.org/10.37240/89.misinforeview.2020.03

[23] Uscinski, J. E., & Butler, R. W. (2013). The Epistemology of Fact Checking. Critical Review, 25(2), 162–180. https://doi.org/10.1080/08913811.2013.843872

[24] Humprecht, E., Esser, F., & Van Aelst, P. (2020). Resilience to Online Disinformation: A Framework for Cross-National Comparative Research. The International Journal of Press/Politics, 25(3), 493–516. https://doi.org/10.1177/ 1940161219900126

[25] Zulli, D., & Zulli, D. J. (2022). Extending the Internet meme: Conceptualizing technological mimesis and imitation publics on the TikTok platform. New Media & Society, 24(8), 1872-1890. https://doi.org/10.1177/1461444820983603