The TikTok Ban: A Technological Politics Analysis

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Devasish Pant

Spring 2025

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisor

Kathryn Webb-Destefano, Department of Engineering and Society

Introduction

In recent years, TikTok has faced increasing scrutiny from governments worldwide due to concerns over data privacy, misinformation, and national security. In the United States, discussions surrounding a potential ban on TikTok have intensified, particularly due to its ownership by the Chinese company ByteDance. Policymakers argue that TikTok poses a threat by potentially sharing user data with the Chinese government, while critics of the ban view it as a politically motivated restriction on free speech. This paper analyzes the ethical and political dimensions of the TikTok ban using the framework of technological politics. Technological politics, a framework developed by Langdon Winner, suggests that technologies are inherently political and can shape power dynamics in society (Winner, 1986). By applying this framework, this paper argues that the TikTok ban reflects broader tensions between national security, digital sovereignty, and ethical considerations of censorship and user rights.

TikTok, a social media platform known for its short-form videos, has grown into one of the most popular apps globally, boasting over a billion active users. However, its rapid rise has been accompanied by concerns regarding data privacy, algorithmic bias, and misinformation. In the U.S., the Trump administration initially attempted to ban TikTok through executive orders in 2020, citing national security risks. While these efforts were legally challenged, similar concerns have persisted under the Biden administration, with lawmakers proposing bipartisan bills to regulate or ban the app (Zeng & Kaye, 2023). The controversy surrounding TikTok reflects deeper issues related to digital governance, international relations, and the role of technology in modern geopolitics.

TikTok's algorithm plays a crucial role in its success, curating personalized content for users based on engagement patterns. However, critics argue that this algorithm may also

facilitate the spread of misinformation and manipulate public opinion. Furthermore, TikTok's data collection practices, including gathering location data, device information, and user interactions, have raised concerns over surveillance and foreign influence. Despite reassurances from TikTok executives that U.S. user data is stored securely, skepticism remains due to ByteDance's ties to China. This has led to calls for either an outright ban or forced divestiture of TikTok's U.S. operations to an American company.

Background

TikTok, launched by the Chinese company ByteDance in 2016, quickly became one of the most popular social media platforms worldwide. Known for its short-form videos ranging from dance challenges to political commentary, TikTok's success lies in its powerful algorithm, which curates personalized content based on user engagement (Bhandari & Bimo, 2022). By 2020, TikTok had amassed over a billion active users globally, including around 150 million in the United States (Fung, 2023). The platform's rapid growth, especially among young users, has made it a significant cultural force, but it has also attracted scrutiny from governments concerned about data privacy and foreign influence (Minges, 2025).

TikTok's algorithm is at the core of its user engagement strategy, utilizing machine learning to analyze user behavior and preferences. This results in a highly personalized feed known as the "For You" page, where content is curated based on factors such as likes, shares, and time spent on videos. The app also allows users to create and share videos with a wide range of editing tools, filters, and soundtracks, fostering creativity and viral trends. Due to its format and ease of use, TikTok has become a hub for grassroots activism, political expression, and social movements, further embedding itself in digital culture (Zeng & Kaye, 2022). However, the very features that make TikTok appealing also pose risks related to data privacy. ByteDance's

data collection practices include gathering location data, device information, and user interactions, which has raised concerns about potential data sharing with the Chinese government (Fung, 2023; Liu, 2024). Despite assurances that U.S. data is stored domestically, skepticism remains, prompting debates on digital sovereignty and platform regulation (Pohle & Thiel, 2020).

. U.S. lawmakers and intelligence officials have argued that because ByteDance is based in China, it could be compelled to share user data with the Chinese government under the country's National Intelligence Law. This possibility has led to fears that TikTok could be used as a tool for espionage or propaganda, especially given the platform's ability to influence public opinion through algorithmic content curation (Fung, 2023). The U.S. government's concerns intensified during the Trump administration, which issued executive orders to ban TikTok, citing national security threats. Although these efforts were blocked by court rulings, the Biden administration has continued to scrutinize the platform. Lawmakers have introduced bipartisan bills aimed at regulating or banning TikTok, highlighting fears that data collected from American users could be accessed by foreign entities (Minges, 2025). Additionally, the ban is seen as part of a broader strategy to reduce dependence on Chinese technology and assert greater control over digital ecosystems (Pohle & Thiel, 2020).

Literature Review

Scholarly discussions around digital platforms increasingly emphasize their political and structural influence, aligning with Langdon Winner's framework of technological politics, which argues that technologies can embody specific forms of power and authority (Winner, 1986). This is particularly evident in studies of TikTok, where platform design and moderation policies function as tools of geopolitical influence and social control. The following three peer-reviewed

sources, Zeng and Kaye (2022), Kuznetsova and Tolbert (2023), and Liu (2024) offer complementary and contrasting perspectives on how TikTok, as a technological artifact, has become a geopolitical battleground.

Zeng and Kaye (2022) introduce the concept of visibility moderation, which is the algorithmic manipulation of content reach on platforms like TikTok, as a form of covert governance. Their case study reveals how TikTok's recommendation system, particularly the "For You Page" algorithm, does more than personalize content; it actively shapes which political or social messages are amplified or suppressed. This form of technological control, while subtle, has profound implications for digital sovereignty and freedom of expression. According to Zeng and Kaye, TikTok's algorithmic governance has led to censorship-like outcomes, such as shadow banning or the underpromotion of content involving marginalized communities or politically sensitive topics. These practices illustrate how a platform's technical infrastructure can act politically by enforcing certain norms and values through its design, supporting Winner's claim that "artefacts have politics" (Winner, 1986).

In contrast, Kuznetsova and Tolbert (2023) provide a global comparative perspective on how digital platforms like TikTok facilitate political participation. Through a large-scale analysis of 45 countries, they argue that access to globalizing information networks, particularly through social media, correlates with increased civic engagement, even in non-democratic regimes. While their work is primarily quantitative, it highlights the potential democratizing power of technology, suggesting that platforms like TikTok could serve as tools for global information dissemination and civic mobilization. However, they also acknowledge that authoritarian states may attempt to co-opt or restrict such technologies for their own political ends, a point that underscores the tension inherent in the politics of digital platforms.

While Zeng and Kaye focus on internal platform governance as a site of political power, Kuznetsova and Tolbert emphasize external political consequences: how the same technologies that are manipulated internally by algorithms also serve as channels for activism and global discourse. This contrast illustrates a key tension in the technological politics of TikTok: on one hand, it is a controlled space that enforces selective visibility; on the other, it is a participatory medium that transcends borders and empowers users. Together, these studies support the central claim of this paper, that the TikTok ban is not just a reaction to national security concerns, but a political act embedded in broader power struggles over digital sovereignty and control of global information flows. Both sources also reinforce the idea that the design and governance of platforms like TikTok are not neutral. As Winner (1986) emphasizes, technologies can function as political actors, encoding the values, priorities, and power dynamics of their creators and regulators. The U.S. attempt to ban TikTok, therefore, should be seen not merely as policy enforcement but as a response to the perceived geopolitical threat encoded in the platform's technological architecture.

Liu (2024) brings the concept of digital sovereignty into the conversation, arguing that the TikTok ban must be understood as an act of geopolitical boundary-setting. As Liu writes, "the ban on TikTok in the United States is closely related to the concept of digital sovereignty" and "illustrates how data, infrastructure, and code have become objects of international power struggles" (p. 137). Liu sees the TikTok ban not just as a security policy but as a symbolic and practical effort by the U.S. government to reassert control over its digital borders. He notes, TikTok's popularity and control over user data grants it a quasi-sovereign status, which the U.S. aims to neutralize through legal and economic pressure. Here, TikTok is framed as a sovereign actor whose technological and algorithmic capabilities threaten U.S. information territory,

echoing Winner's assertion that "technologies can have inherently political qualities" (Winner, 1986).

What distinguishes Liu's perspective is his emphasis on algorithmic control as a form of soft power. He writes that preferences of users and interactions that are algorithmically amplified result in a disproportionate representation of negative emotions and politically extreme content. This concern aligns with Zeng and Kaye's findings on visibility moderation, but Liu ties it directly to national security, suggesting that the platform's algorithm may subtly influence democratic processes. In contrast, Kuznetsova and Tolbert remain more optimistic about the civic potential of such platforms, even as they acknowledge attempts at control.

Taken together, these three sources reinforce the central claim of this paper: the TikTok ban should be seen not just as a response to technical threats, but as an instance of technological politics in action. TikTok's technical infrastructure, its recommendation algorithm, data collection practices, and international ownership becomes a site where political control, sovereignty, and user autonomy are negotiated. Zeng and Kaye show how these negotiations happen at the code level; Kuznetsova and Tolbert demonstrate how users subvert or resist those structures; and Liu situates the platform within broader efforts to define and defend national digital sovereignty.

In Winner's terms, the U.S. government's attempt to ban TikTok is an example of using political tools to address a technology that itself performs political functions. As each of these scholars show in different ways, TikTok is not merely a social media app, it is a geopolitical actor shaped by and shaping systems of control, governance, and resistance.

Conceptual Framework

Langdon Winner's concept of technological politics serves as the guiding framework for this analysis. Winner argues that technologies are not neutral tools but are often inherently political, they can be deliberately designed or unintentionally shaped in ways that establish, reinforce, or transform power relationships (Winner, 1986). Technologies, according to Winner, can be political in two primary ways: they may either settle issues in a particular way by embodying a specific form of authority, or they may require or strongly promote particular forms of political relationships.

Applying this to the TikTok ban, the framework allows us to ask: how is TikTok itself a political actor through its design and algorithmic behavior? And how is the act of banning or regulating TikTok a political expression by the U.S. government? By examining TikTok's infrastructure and recommendation systems, we see how the platform exerts soft power through content visibility, shaping what users see and how they engage with information. Winner's framework encourages us to interrogate these systems as mechanisms of control, both by platform designers and by national governments that seek to contain or co-opt them. This approach helps us understand TikTok's technological design not just as a business strategy, but as a mechanism that actively shapes digital discourse and political behavior. The algorithmic architecture, particularly the way content is prioritized, promoted, or hidden reflects intentional or systemic values embedded within the platform. This is inherently political, as it influences what topics gain traction, whose voices are amplified, and how public opinion may be swayed.

At the same time, the U.S. government's response to TikTok is a political act that seeks to reinforce control over digital infrastructure. The threat posed by TikTok is not merely that of potential surveillance but of influence over culture, communication, and political engagement.

By attempting to ban or force the divestment of TikTok, the U.S. government is engaging in a broader contest over digital sovereignty. In Winner's terms, the regulation of technology becomes a way of asserting national power, redrawing the boundaries of control in the digital age. Thus, by using the technological politics framework, this paper interprets both TikTok's algorithmic features and the U.S. response to it as expressions of political power. The framework provides a way to analyze how decisions about technology are never neutral but are embedded in and reflective of broader societal structures and geopolitical struggles.

Analysis

Langdon Winner's theory of technological politics argues that technologies are not merely tools but political artifacts that can shape or enforce specific social orders (Winner, 1986). The U.S. effort to ban TikTok through H.R. 7521 reflects this logic: it is not only a policy decision but a declaration of which actors are permitted to participate in the governance of digital space. The legislation demands that ByteDance divest ownership of TikTok operationalizes political values, such as national sovereignty, surveillance control, and cultural influence through a technological mandate.

This framing is inseparable from broader ideological patterns. As McInerney (2024). explains, U.S. discourse around Chinese technology is often shaped by "digital orientalism," a racialized mode of othering that casts Chinese platforms as uniquely threatening. This logic legitimizes policies like the TikTok ban while eliding similar data-harvesting practices by American tech firms. It echoes Winner's view that technologies are always embedded within existing structures of power and often serve to reinforce them. The 2023 Congressional hearing with TikTok CEO Shou Zi Chew further illustrates how technological controversies become political performances. Despite efforts to distance the platform from Chinese state influence,

such as through Project Texas, which localizes U.S. user data, lawmakers from both parties remained unconvinced (Fung, 2023). Their skepticism illustrates how political mistrust can override technical assurances, reinforcing Winner's claim that some technologies become politically controversial not because of what they do but because of what they represent.

The policy complexity around TikTok is also heightened by evolving definitions of national security. According to a policy brief from American University (Minges, 2023), digital platforms now fall under this expanding umbrella due to their capacity to shape information flows, public opinion, and geopolitical narratives. This move toward "informational sovereignty" signals a shift from conventional military or economic security toward more abstract concerns about influence and control, again supporting Winner's idea that some technologies are "inherently political." While authoritarian governments can exploit digital tools for surveillance or censorship, platforms like TikTok also introduce unpredictability and potential loss of control. This dual-use dynamic underscores the complexity of digital governance and reinforces Winner's assertion that technologies do not simply follow political will, they often shape and constrain it in return.

One of the primary justifications for banning TikTok is national security. U.S. officials argue that ByteDance, the parent company of TikTok, could be compelled by Chinese law to share user data with the Chinese government. This concern is exacerbated by past cases of Chinese tech companies allegedly cooperating with state surveillance efforts. However, critics argue that banning TikTok violates fundamental principles of free speech, as it restricts a platform used by millions for expression and communication (Zeng & Kaye, 2022). Applying the technological politics framework, the TikTok ban can also be viewed as a politically motivated decision rather than a purely security-driven measure. While concerns over data

privacy are valid, similar issues exist with American-based companies like Meta (Facebook) and Google, which have faced scandals related to user data misuse (Zeng & Kaye, 2022). The selective targeting of TikTok suggests that the ban may be influenced by broader geopolitical tensions between the U.S. and China, rather than solely by ethical concerns over data privacy.

Another ethical concern surrounding the ban is the lack of consistency in regulating social media platforms. If the U.S. government aims to protect user data, it should enforce stricter data privacy regulations across all tech companies rather than singling out TikTok. Banning TikTok without providing users with a transparent legal process raises concerns about government overreach and censorship. TikTok doesn't merely entertain people, it conditions users to think and act in particular ways, implicitly endorsing a political economy of attention. This resonates with Winner's idea that certain technologies demand or favor specific forms of social organization.

The International Studies Review article (Mueller, 2019) provides further context, noting that digital platforms may serve authoritarian resilience while also introducing vulnerabilities. TikTok's ties to China complicate this dynamic: while it could theoretically align with Chinese state interests, its global reach and algorithmic opacity make it difficult to fully control. In this sense, the platform is both a tool and a wildcard, politically charged by design and by implication. Gorwa's (2024) critique of platform regulation again becomes relevant here. The architecture of TikTok, its recommendation engine, data practices, and moderation policies is governed not by public institutions but by private corporations. Even in the absence of state intervention, the platform exercises a form of unaccountable power that Winner would describe as inherently political.

Rather than an outright ban, alternative solutions could address both security concerns and ethical considerations. One potential solution is stronger data protection laws that apply to all social media companies, ensuring that user data is safeguarded regardless of the platform's country of origin. Another option is requiring TikTok to store U.S. user data in the United States under strict regulatory oversight. Additionally, increasing transparency in algorithmic decision-making could help address concerns about misinformation and bias on the platform.

Conclusion

The debate over banning TikTok is emblematic of the broader entanglement between technology, politics, and ethics in the digital age. While national security concerns, particularly regarding potential data access by the Chinese government are frequently cited, this paper has shown that the rationale for a ban cannot be separated from the geopolitical and ideological contest between the U.S. and China. Using Langdon Winner's framework of technological politics, TikTok is revealed not merely as a neutral platform but as a political artifact, one that encodes power through its algorithmic design and exerts influence over public discourse and digital behavior.

At the same time, the U.S. government's response, whether through attempted bans or divestiture efforts, reflects an assertion of digital sovereignty and an effort to redraw the boundaries of acceptable technological influence within its jurisdiction. However, this response raises serious ethical concerns. Targeting TikTok without applying consistent standards to all social media companies undermines principles of fairness, transparency, and free speech. This inconsistency suggests that the issue is less about protecting users and more about controlling narratives and power in the global information economy.

Rather than relying on punitive or exclusionary measures, a more ethically sound approach would involve the establishment of comprehensive data protection regulations and greater algorithmic transparency, measures that apply to all platforms regardless of their national origin. In doing so, the U.S. can uphold user rights and national security without compromising democratic values. Ultimately, the TikTok case illustrates how technologies are never politically neutral and how their regulation must be understood as a form of governance in its own right.

Word Count: 3,178

References

Bhandari, A., & Bimo, S. (2022). Why's everyone on TikTok now? The algorithmized self and the future of self-making on social media. Social media + society, 8(1), 20563051221086241.

Congressional Research Service. (2023, August 25). *TikTok: Recent data privacy and national security concerns* (IN12131). https://crsreports.congress.gov/product/pdf/IN/IN12131

Fung, B. (2023, March 24). *TikTok collects a lot of data. but that's not the main reason officials say it's a security risk | CNN business*. CNN. https://www.cnn.com/2023/03/24/tech/tiktok-ban-national-security-hearing

Gorwa, R. (2024). The Politics of Platform Regulation. https://library.oapen.org/bitstream/handle/20.500.12657/90834/Gorwa_The%20Politics%20of%20Platform%20Regulation.pdf?sequence=1&isAllowed=y

Kuznetsova, D., & Tolbert, C. J. (2023). Globalizing Information Networks, social media, and participation. *Social Science Quarterly*, *104*(4), 505–520. https://doi.org/10.1111/ssqu.13287

Kwet, M. (2019). Digital colonialism: US empire and the new imperialism in the Global South. *Sage Journals*, *60*(4), 3–26. https://doi.org/10.1177/0306396818823172

Liu, Y. (2024). The Risks of TikTok in the Context of Digital Sovereignty: A case study of the U.S. ban on TikTok. *International Journal of Education and Humanities*, *17*(3), 137–141. https://doi.org/10.54097/z4a9b081

McInerney, K. (2024). Yellow Techno-Peril: The 'Clash of Civilizations' and anti-Chinese racial rhetoric in the US–China AI arms race. *Sage Journals*, *11*(2). https://doi.org/10.1177/20539517241227873

Minges, M. (2025, January 23). *National Security and the Tiktok Ban*. American University. https://www.american.edu/sis/news/20250123-national-security-and-the-tik-tok-ban.cfm

Mueller, M. L. (2019). Against sovereignty in cyberspace. *International Studies Review*, *22*(4), 779–801. https://doi.org/10.1093/isr/viz044

Pohle, J., & Thiel, T. (2021). Digital Sovereignty. *Practicing Sovereignty*, 47–68. https://doi.org/10.1515/9783839457603-003

Winner, L. (1986). *The whale and the reactor: A search for limits in an age of high technology*. University of Chicago Press.

Zeng, J., & Kaye, D. B. V. (2022). From content moderation to visibility moderation: A case study of platform governance on TikTok. *Policy Internet*, *14*(1), 79–95. https://doi.org/10.1002/poi3.287