Proceedings of ICLLCD 2026 Symposium: Using Visual Arts to Enrich History Understanding
DOI: 10.54254/2753-7064/2026.HT30665

Surveillance and Privacy in Digital Media: A Case Study of TikTok and Further Discussion

Wenqin Ke

Beijing International Studies University, Beijing, China
18889645700@139.com

Abstract. The functions of social media platforms have undergone profound transformations due to rapid technological and social advancements. Traditional information exchange functions can no longer cater to the evolving needs of social communication and regulation. In the digital media age, information monitoring and dissemination are ubiquitous. For example, agreeing to various permissions when logging into a website, while improving the efficiency of information flow , also erodes the boundaries of personal privacy that were previously unbreached by traditional media . In this process of breaking down and crossing boundaries, the privacy boundaries belonging to the users themselves are also being reshaped. How to appropriately delineate the scope of governance and surveillance amid these dissolving and reshaping boundaries has emerged as a critical research agenda in contemporary academic and policy discourse. This paper will use a literature review approach to explore cases represented by the Facebook data breach and the US government's restrictions on TikTok, examining the trade-offs and dilemmas between government monitoring and personal privacy in the digital environment. This paper finds that while governments issue regulatory measures to protect citizens' information security, they frequently give rise to substantial controversies concerning privacy safeguarding, urgently requiring a more balanced governance path.

Keywords: Digital surveillance, privacy protection, TikTok, data security, social media governance

1. Introduction

In recent years, social media platforms have become an indispensable medium for public participation and interpersonal communication. At the same time, the escalating and predominantly unregulated utilization of social media has aroused widespread concerns among citizens regarding potential infringements on their rights and civil liberties. Social media platforms carry a significant risk of exposing substantial volumes of personal information, including information about political and religious views, personal IP addresses and occupations [1]. From the perspective of public safety, digital surveillance (GDPR, government policies) undoubtedly serves as an effective mechanism, but excessive surveillance and data abuse may encroach upon personal privacy and spark social controversies. How to strike a balance between user data protection and the boundaries of platform accountability in social media landscape has emerged as a pressing issue requiring urgent attention. This paper adopts the method of literature review and focuses on analyzing TikTok and other privacy protection-related cases. This study contributes to a deeper understanding of the challenges confronting digital privacy and offers actionable insights for policymakers and platform administrators.

2. Theoretical framework

With the rapid development of information technology and the internet, social media has become an indispensable part of people's lives. As of the end of 2024, the global number of social media users had exceeded 4 billion, representing over half of the world's population. Given this massive number of internet users, striking a balance between user data protection and platform accountability within the intricate digital ecosystem remains a pivotal concern. From a theoretical perspective, the protection of citizens' rights and the proper use and regulation of platforms spans multiple academic disciplines, posing significant challenges to traditional theoretical frameworks and demanding innovative theoretical perspectives and actionable solutions. From a practical perspective, the proper balance between privacy and surveillance in the digital society has already exerted a profound societal impact, as evidenced by platforms abusing user privacy and governments issuing bans.

In recent years, scholars worldwide have conducted extensive research on privacy and surveillance issues in the digital society, accumulating a substantial body of literature. At the same time, in specific practice, relevant platforms and governments of various countries have formulated pertinent laws and policies to mitigate privacy breaches. However, given that the Internet has only experienced rapid development in recent years to become an integral part of people's lives, with the role of social media continuously expanding, various management measures are still in their nascent or exploratory phases. Today, the development of the digital society faces many challenges. In order to maintain the stability of the Internet environment, it seems that users' active disclosure of personal privacy has become an implicitly required practice. Extant research indicates that the majority of social media users are aware of potential privacy risks and exhibit a high degree of concern regarding privacy issues. Notably, despite their awareness of such risks, users continue to disclose personal information—including location data and photographic content—on social media platforms. This has produced a rather paradoxical "privacy paradox" phenomenon, that is, users are worried about the infringement of personal information and privacy while voluntarily disclosing their private data [2]. The boundaries of users' privacy are constantly being dissolved and reshaped in daily social media activities. In the context of temporal progression, personal privacy manifests a state of being archived in the past, compromised in the present, and anticipated in the future—marking the advent of the "liquefied privacy" era [3].

Social media is an indispensable part of the vast and complex Internet. As a platform for information exchange and communication, its core function lies in facilitating the establishment and maintenance of users' social connections [4]. Consequently, it inherently entails the risk of privacy breaches, posing significant threats to users' daily Internet life and personal privacy security. With the development of technology, social media and various applications no longer just assume the responsibility of users sharing information as platforms. The proliferation of sectors such as mobile payments, ride-hailing services, and food delivery has incentivized social media platforms to proactively gather more granular personal information and user data. However, this data may be misappropriated, leading to privacy leakage and information abuse. Against the backdrop of frequent malicious and illegal information breach incidents, the regulatory role of the government has become increasingly pivotal.

DOI: 10.54254/2753-7064/2026.HT30665

Historically, amid the rapid and booming development of social media, governments predominantly adopted a laissez-faire approach, seldom implementing stringent regulatory measures. While this approach facilitated the rapid development of the Internet, the resulting regulatory issues remained prominent. Although governments around the world have now enacted legislation in an attempt to reduce this phenomenon, such regulatory efforts are still in the exploratory phase.

To address challenges, such as user information leaks and platform misconduct, a multi-stakeholder approach involving users, platforms, and governments is required. Users can enhance their privacy protection competencies through specialized online training programs; platforms need to build firewalls to prevent the unauthorized exploitation of user data by malicious actors; and the government, as regulatory authorities, should formulate more refined legal frameworks to reasonably restrict platforms' access to user data without interfering with the development of social media.

3. Case Studies

3.1. Facebook data breach case

When it comes to facial data, billions of images (and (videos) are being uploaded to various social media platforms such as Facebook Instagram, Twitter (X) or YouTube, on a monthly basis, creating mass image collections that can be processed and analyzed using sophisticated computer vision and biometric recognition technologies [5] .

In 2018, the data breach involving Facebook and Cambridge Analytica was exposed, becoming a turning point in global data privacy governance. The incident originated from Cambridge University psychologist Alexander Kogan’s collection of data from approximately 87 million Facebook users through a personality test application in 2014, which he unlawfully disclosed to the political consulting firm Cambridge Analytica. Cambridge Analytica used this data to build psychological profiles and allegedly interfered in the 2016 US presidential election and the UK's Brexit referendum [6]. The core flaw lied in Facebook’s inadequate oversight of third-party developers' data acquisition as a platform. Its open API framework enabled third-party applications to access not only user data but also their friends’ network information, while users were deprived of the right to informed consent. This incident exposed the conflict between business models and privacy protection . a $35B face data lawsuit against Facebook will proceed , Josh Constine at TechCrunch discusses Facebook's most recent legal blow as its appeal against a case of 7 million Illinois residents was rejected. The class-action case is founded on Facebook’s unauthorized use of facial recognition technology on users’ photographs [7]. Facebook's reliance on a data-driven advertising model for profit has resulted in its implicit acquiescence to data misappropriation, which also laid bare the issue of regulatory lag. Following the incident, the U.S. Federal Trade Commission (FTC) fined Facebook $5 billion and instituted a 20-year privacy compliance supervision mechanism, though the absence of proactive preventive measures was glaring. However, the incident catalyzed stricter enforcement of the EU's General Data Protection Regulation (GDPR) and prompted several countries to strengthen data localization requirements and cross-border data transfer regulations through legislation.

3.2. TikTok US restriction case

TikTok's experience in the United States paints a distinctly different scenario. Since 2019, the US government has investigated it under the guise of "national security concerns", alleging that it may transfer U.S. user data to the Chinese government and submit to content censorship mandates. In 2020, the Trump administration issued an executive order mandating TikTok’s divestiture of its U.S. business operations, a ruling subsequently stayed pending legal challenges. In 2023, the Biden administration pushed for a "data segregation" plan, requiring the local storage of US user data through Oracle cloud servers. The core contention in this case hinges on the tension between data sovereignty and national security. The US is concerned that China's National Intelligence Law, which requires companies to cooperate with government data requests, could lead to data misuse. Against the backdrop of geopolitical and technological rivalry , TikTok 's global success is seen as a symbol of China's digital technology rise, and the US is seeking to preserve its technological hegemony via restrictive measures. Ultimately, TikTok transferred data storage and content moderation authority to a US entity through "Project Texas," exchanging compliance for market access. This exemplifies the company’s adaptive innovation amid geopolitical pressures.

4. Challenges and future directions

4.1. Challenges

In the evolution of digital media, the tension between surveillance and privacy has increasingly emerged as a global focal point. This conflict encompasses not only technological-level data governance but also intricate intersections with geopolitics, commercial interests, and civil liberties. Taking the development and restrictions imposed on TikTok in the United States, as an example mentioned above, as a clear illustration, the complexity and multi-dimensionality of surveillance and privacy issues in the digital age can be observed.

TikTok, a short video platform owned by Byte Dance, swiftly penetrated the global market leveraging its highly personalized recommendation algorithm. However, its success has also triggered widespread apprehensions regarding data security and privacy safeguards. A core concern for US regulators is that TikTok's data collection could expose users to surveillance vulnerabilities. By acquiring users' geolocation data, device identifiers, browsing trajectories, and even facial recognition data, the platform can build detailed user profiles. This large-scale data collection, while ostensibly aimed at improving user experience, essentially embodies the inherent nature of commercial surveillance in the digital era. Secondly, geopolitical dynamics further amplify privacy anxieties. The US government believes that, under China's National Intelligence Law and Cybersecurity Law, Chinese companies are statutorily obligated to assist with government data inquiries, potentially allowing TikTok's stored US user data to be exploited for state-sponsored surveillance.

Despite TikTok's repeated denials of these allegations and its efforts to enhance data transparency (such as the "Texas Plan" to store US user data locally), the opaqueness of its algorithmic systems persists as a point of contention. The "black box" characteristic of these algorithms hinders external regulatory authorities from verifying the compliance of data processing activities, and the platform's content moderation framework has been questioned as potentially influenced by its home government. This phenomenon reveals a new form of digital surveillance , no longer limited to traditional government surveillance, but achieved through the technical architecture and algorithmic systems of commercial platforms, forming a more clandestine and efficient surveillance mechanism.

From a broader perspective, the TikTok case reflects the predicament of privacy safeguarding in the digital era. On the one hand, users demand personalized services, which necessitates platforms to collect and analyze vast volumes of data; on the other hand, the risks of data misuse and external surveillance are perpetually undermining public trust. Furthermore, the discourse of national security is extensively employed to legitimize data localization mandates and restrictions on cross-border data transfers, further exacerbating the fragmentation of the global digital ecosystem.

4.2. Future directions

To address these challenges, more systematic multi-level governance strategies will be imperative moving forward. Privacy protection needs to be reinforced via technological interventions, such as employing privacy-enhancing technologies like differential privacy and federated learning to reduce data identifiability at the source. Concurrently, surveillance activities should be checked and balanced, clearly differentiating between compliance reviews driven by public interest and excessive surveillance, and establishing a hierarchical and classified data access framework. Enhancing public trust hinges on transparency and accountability mechanisms, such as mandating platforms to disclose their algorithmic principles and data usage policies, and subjecting them to independent third-party audits. Furthermore, legislation ought to further delineate the rights and obligations of all stakeholders, establish unified data protection standards, preclude fragmented regulation. Ultimately, harmonizing regulatory frameworks globally and promoting interoperable international rules will constitute the pivotal pathway to balancing surveillance and privacy while safeguarding citizens' digital rights in the digital era.

The TikTok case illustrates that balancing surveillance and privacy in the development of digital media is not merely a technical or legal matter, but a complex interplay of interests and values among multiple stakeholders. Only through a multi-faceted strategy integrating technological innovation, legal refinement, and international collaboration can we truly achieve the coordinated development of privacy protection and public interest in the digital age.

5. Conclusion

This study examines the surveillance mechanisms of digital platforms, exemplified by TikTok, and the privacy case of Facebook, revealing a significant tension between government regulation and personal privacy protection in the digital media ecosystem. Key findings include: excessive surveillance may induce a chilling effect and erode public trust, whereas existing governance frameworks exhibit inherent inadequacies across technical, legal, and ethical dimensions. The study incorporates the concept of "liquid privacy," emphasizing the dynamic and reconstructive attributes of privacy boundaries in the digital society, and puts forward multi-stakeholder collaborative governance pathways (encompassing users, platforms, and governments). In practical terms, it provides references for policy-making and platform compliance, and advocates for the establishment of more transparent and unified international data governance standards.

However, this paper still has limitations, such as failing to establish a visual model to intuitively depict users' attitudes towards their data being published on websites, and failing to specifically identify the data flow mechanisms of cross-border platforms such as TikTok. Future research may further explore domains including platform regulatory ethics, cross-border data transfer mechanisms, and public privacy literacy education.

In summary, this paper provides a new perspective on the conflict and compromise between social media platform surveillance and user privacy, and also emphasizes the importance of adopting a rational perspective on governmental oversight of user information and clarifying how users, platforms, and governments should navigate the boundaries between user privacy and necessary management boundaries.

References

[1] Brennan Center for Justice. (2022). Social media surveillance by the US government. https: //www.brennancenter.org/our-work/research-reports/social-media-surveillance-us-government

[2] Fan, H. C. (2023). Dilemma and way out: Research on citizen privacy cognition in digital existence. Nanjing Normal University Press.

[3] Frith, J. (2017). Invisibility through the interface: The social consequences of spatial search. Media, Culture & Society, 39(4), 536–551. https: //doi.org/10.1177/0163443717692741

[4] Peng, L. (2012). Social media, mobile terminals, and big data: New technological factors influencing news production. Journalism Review, (16), 3–8.

[5] Meden, B., Rot, P., Terhörst, P., et al. (2021). Privacy-enhancing face biometrics: A comprehensive survey. IEEE Transactions on Information Forensics and Security, 16, 4146–4168. https: //doi.org/10.1109/TIFS.2021.3096024

[6] Isaak, J., & Hanna, M. J. (2018). User data privacy: Facebook, Cambridge Analytica, and privacy protection. Computer, 51(8), 56–59. https: //doi.org/10.1109/MC.2018.3191268

[7] Security Insight Team. (2021). Facebook’s facial recognition case: A security analysis. In Proceedings of the 15th International Conference on Cybersecurity (pp. 45–58). Chicago.