International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 01 Jan. 2025, pp: 243-248 www.ijaem.net ISSN: 2395-5252

The U.S TikTok Case – Will A Unified Federal Data Protection Laws and Apt Stewardship from TikTok resolve the issues?

Christian Budu Duodu & Kwame Joseph Nkrumah
Saint Peter's University, USA, Wake Forest University, USA

Date of Submission: 05-01-2025 Date of Acceptance: 15-01-2025

ABSTRACT
By means of literature research and comparative research, this paper seeks to look at governments emphasis on data protection, and the tough laws formulated to protectits citizens and how social media platforms are playing their stewardship rolein ensuring data owners (users) are protected. The paper explores how seriously governments take data protection and the strict laws they have in place to protect their citizens, as well as the guardianship role social media platforms play in ensuring data owners (users) are protected. At the same time, this article also discusses the alternative of TikTok proposed by the United States to deal with concerns about the security of citizens' data.
This paper seeks to look at alternatives to the US proposal of the ownership of TikTok due to fear of data security of its citizens. It is a fine case to study personal data protection policies and what social media platform providers are doing to ensure they meet the growing tough data protection laws of governments around the world. B In this article, our data stewards will be the social media platforms and the owners will be users of those platforms and governments of those individuals. It is particularly important to know about these two because of the growing concerns about data security and privacy; and the risk it poses to individuals and organizations; and nations. Countries are coming out with tougher laws and social media platforms have already paid billions in fines because these two items were not professionally managed. Meta, TikTok and X (formerly Twitter) have been fined over $3 billion for General Data Protection Regulation (GDPR) violations in 2023[1].
Key Words: Data Stewards, Data owners, Data Protection, Personal Data, policies, accountability, censorship, espionage.

I. INTRODUCTION

The potential ban of TikTok in the U.S subject to the change of ownership is rangingon, and analysts are discussing. Policies on data protection in the United States is fragmented, there seem not to be a comprehensive federal policy on personal data protection as compared to that of Europe and China. That might be the reason while there is the fear of data breaches and National Security concerns. In this write up we compare the data protection polices of the U.S, China and Europe and draw out a conclusion of what might have triggered the U.S position and the consequences if the proposal to ban TikTok comes into effect.

II. COMPARISONS OF THE PERSONAL DATA PROTECTION POLICIES OF THE EU, U.S, AND CHINA

We cannot look at US concerns with data of its citizens with TikTok without looking at the national data policies of the US and China[19]. For research purposes, we will also compare the data policies of Europe which are deemed to be one of the best in the world.

2.1 The European General Data Protection Regulations (GDPR)

The GDPR is an EU law with mandatory rules for how organizations and companies must use personal data in an integrity friendly way. Personal data means any information which, directly or indirectly, could identify a living person. Name, phone number, and address are good examples of personal data. Interests, information about past purchases, health, and online behavior

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 01 Jan. 2025, pp: 243-248 www.ijaem.net ISSN: 2395-5252

are also considered personal data as it could identify a person.

Processing data means collecting, structuring, organizing, using, storing, sharing, disclosing, erasing and destruction of data. Each organization that processes personal data must ensure that the personal data it uses fulfils the requirements of the GDPR[5].

The GDPR is described as the "toughest privacy and security law in the world." The Personal Information Protection Law (PIPL) of the people republic of China is said to mimic the GDPR. The United States however lacks a comprehensive data privacy law that applies uniformly to all data types and companies and various regulations govern different sectors and data types. The United states have a fragmented approach and that does not make the policies as tough as the EU and China.

The GDPR grants individuals control over their personal data and simplifies the regulatory environment for international business by unifying the regulation within the EU. GDPR requires explicit consent for data processing, provides rights to access and erase personal data, and imposes heavy fines for non-compliance. The impact of the GDPR has led to the changes in how platforms collect consent from users in Europe and how they collect data, process and share.

2.2 Personal Information Protection Law (PIPL)

China's laws protecting individual data is the Personal Information Protection Law (PIPL). It was adopted in Aug. 20, 2021, and it is the first comprehensive framework for the protection of personal information in China. Among other things, it requires businesses to conduct impact assessments, honor data subjects' requests for information, and follow measures for cross-border data transfers. It entered into effect Nov. 1, 2021.The PIPL, also effective from November 1, 2021, governs the collection, use, and sharing of personal data.

Before transferring personal information to third parties (within China or overseas), data handlers must obtain informed consent from data subjects and ensure compliance with consent terms. All Chinese social media companies, whether private or public, are subject to the control of the Chinese Communist Party (CCP).[6]

The CCP's influence creates opportunities for state censorship, surveillance, and propaganda, affecting users both within China and globally[7].

Although the Chinese policies is modeled after the GDPR, it has a stronger emphasis on national security. It includes provisions for data localization, restrictions on cross-border data transfers, and stringent requirements for government access to data. The impact of the PIPL on social media is almost the same as the EU. It requires platforms to store Chinese user data within the country and restricts international data transfers.

2.3 What are the Consequences for Noncompliance with the GDPR and PIPL?

Europe hasadministrative fines up to €20 million or 4% of total worldwide annual turnover of the preceding fiscal year, whichever is higher, Order of correction, confiscation of unlawful income, or provisional suspension or termination. Where correction is refused, a fine of up to one million yuan (with solely responsible persons fined between 10,000 and 100,000 yuan). For grave offenses, a fine of not more than fifty million yuan, or 5% of annual revenue (with solely responsible persons fined between 100,000 and 1 million yuan) – Art. 66 (Bloomberg, 2024)

2.4 Data Protection Laws of the United States

The united states has fragmented laws. They have the federal level and the state level laws.

In the United States, the Communications Decency Act of 1996 helped to lay the groundwork for federal regulation of obscene, indecent, and illegal content online. Though some parts of the act were struck down by courts in the years following its passage, Section 230, which generally protects website platforms from liability for illegal content posted to their sites, continues to inform the legal discussion regarding social media regulation.[16]

There have been calls for Congress to expand and/or change Section 230 with regards to social media providers in light of major public events over the past decade. For example, allegations of Russian interference in the 2016 U.S. presidential election have sparked a debate over whether companies like Facebook and Twitter should be held more liable than they are for disinformation uploaded to their sites.

Since the Federal Communications Commission lacks the authority to discipline these companies, however, Section 230 does not have much of an effect on the current social media ecosystem. Similarly, the Federal Trade Commission mostly regulates social media in terms of the truthfulness of material claims that companies make using it. Like the FCC, the FTC has no mandate to punish violators. Instead, it collects complaints and uses them to build a case

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 01 Jan. 2025, pp: 243-248 www.ijaem.net ISSN: 2395-5252

against a company, sometimes with the help of the Justice Department.

It follows that the U.S. federal government is limited in its ability to regulate social media. Though Congress has presented measures to overhaul policies like Section 230 to hold companies more accountable for problematic content—measures like the Platform Accountability and Consumer Transparency (PACT) Act, introduced by Senators Brian Schatz and John Thune in 2021—there is no mandate currently in place for federal regulators to directly handle social media activity.

The U.S. federal government has failed, in the eyes of many, to adequately establish regulations over social media giants, certain states have acted on their own to hold these service providers more accountable. The vision of "accountability," however, differs across the American political spectrum. For example, Florida Governor Ron DeSantis proposed a bill in 2021 that would fine companies for "knowingly de-platforming" political candidates, likely in response to Twitter's suspension of former president Trump over the January 6th attacks.

In Maryland, state politicians passed legislation that taxes the revenue on digital advertisements sold by big tech companies like Facebook, Google, and Amazon. The tax, inspired by European policies like the French tax on digital revenue and the Austrian tax on digital advertising, is the first of its kind in that it applies solely to the revenue a company receives from digital advertising in the United States. It is expected to generate as much as $250 million in state revenue.

Virginia's Consumer Data Protection Act, signed into law by Governor Ralph Northam in March 2021, allows state residents to opt out of having their data collected and sold by social media companies. The law will be enforced by the state's attorney general, and it does not allow individuals to sue companies on their own for violations. It also allows residents to see what data companies have collected about them, and to correct or delete this information.

The Virginia legislation follows the passage of a similar measure that took effect in California in 2020. California's Consumer Privacy Rights Act, while more industry-friendly in comparison, affords similar protections to residents regarding the collection of their personal information. It also differs from the Virginia legislation in that it creates a new state agency, the California Privacy Protection Agency, which can prosecute companies who violate the policy9.

In Summary, the US does not have a comprehensive federal data protection law. Instead, it has a patchwork of sector-specific laws like HIPAA for health information, COPPA for children's online privacy, and others. However, recent executive orders aim to enhance protections for sensitive personal data. The impact of this on social media therefore is the lack of specific approach means that platforms must navigate a complex legal landscape to comply with different regulations in effect also providing a leeway or flexibility for the social media platforms.

III. WHAT ARE U. S CONCERNS WITH THE OWNERSHIP OF TIKTOK?

The TikTok app is owned by ByteDance, which is based in Beijing and therefore falls under China's controversial cybersecurity laws. These laws, among other things, contain provisions that could potentially require TikTok to hand over U.S. user data to the Chinese Communist Party upon request[10].

TikTok has over 150 million users in the United States. The US concerns include potential threats to data privacy, national security, and children's online safety. Critics worry that TikTok, owned by Chinese company ByteDance, collects sensitive data on U.S. users. The Chinese government's influence over TikTok's content moderation and algorithms raises red flags. Reports suggest that ByteDance employees in China accessed non-public U.S. user data. And the Chinese government's broad authority to compel data access from companies operating in China.

3.1 Analysis of the Concerns

In 1962, Congress passed a law restricting the ability of Americans to subscribe to foreign communist periodicals. But three years later, in Lamont v. Postmaster General, the Supreme Court issued a unanimous rebuke to Congress, ruling that Americans had the right to unrestricted access to that material[15].

This was around the cold war and today Americans find themselves facing a similar case.

There are mixed views about the U.S concerns and experts are discussing alternative views. There has been a dramatic change of fortune for TikTok. People in the United states are much less sure about banning the app than they were in March 2023. Support for banning the app dropped from 50 percent in March to 38 percent at the beginning of October 2023, according to Pew. Opinion is split three ways[12].

Shortly after the executive order dropped, French security researcher Elliot Alderson conducted a deep dive into TikTok's data logs and

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 01 Jan. 2025, pp: 243-248 www.ijaem.net ISSN: 2395-5252

found nothing unusual, saying, "In its current state, TikTok doesn't have a suspicious behavior and is not exfiltrating unusual data."[31] He continued, "We would obtain similar results with Facebook, Snapchat, Instagram and others."If CCP officials have access, it makes sense, then the access is through a back door.

Much of the data TikTok is allegedly collecting on users can be purchased on the open market, for as little as 12 cents a person—if the CCP really wanted this information, it could access it via means that would not kill TikTok.

In a thorough look at all of the criticism, Dr. Milton L. Mueller and Dr. Karim Farhat of Georgia Tech's Internet Governance Project found:

- The app "is not exporting censorship, either directly by blocking material, or indirectly via its recommendation algorithm. Its content policies are governed by market forces."
- "The data collected by TikTok can only be of espionage value if it comes from users who are intimately connected to national security functions and use the app in ways that expose sensitive information."
- And importantly, "Because social media apps publish and share so much data, China does not need to have special legal powers over ByteDance to use TikTok (or any other social media app) to monitor users."

Similarly, the Citizen Lab at the University of Toronto concluded in 2021 that "TikTok's program features and code do not pose a threat to national security." The Australian government also set up an official government task force to look into TikTok and found that there was "no reason for us to restrict those applications at this point."[12].

3.2 Alternatives to the Ownership of TikTok Proposed in the United States

"The federal government does have a legitimate interest in protecting the American people from surveillance by foreign governments. But the powers being sought by Congress represent the most radical options on the table, when other alternatives could better balance security and the protection of users' free speech rights. Congress has a range of regulatory options that fall in between doing nothing and either forcing divestment or threatening a ban"[15]. The following are suggested alternates:

i. Continuous monitoring of TikTok which may include mandated routine unannounced audit.
ii. Data Localization just like the EU and China. TikTok has already started project Texas to localize America data.
iii. Another alternative is for an American giant tech company like Oracle to host the user data. President Trump initiated something like this but did not materialize.

3.3 What U.S. May Lose When TikTok is Banned

According to a new report from Oxford Economics, TikTok contributed $24.2 billion to the U.S. economy in 2023. As per TikTok:

"According to research conducted in the summer of 2023, U.S. small- and mid-sized businesses (SMBs) that marketed or advertised on TikTok generated $15 billion in revenue in 2023. SMBs on TikTok also placed a significant value on the free services provided by TikTok, which help them grow organically. These two value streams together supported a $24.2 billion contribution to U.S. the gross domestic product (GDP) in 2023."

This ban could have devastating effects for the 7 million TikTok users who derive either part or all of their income from businesses based on the platform. Commerce on the site could grind to a halt, damaging the livelihoods of business owners who have spent years building a customer base in order to sell products on TikTok. It could also devastate users who have grown an audience on the app and turned creating content into a full- time profession[15].

The report also found that almost 40% of SMBs say that TikTok is "critical to their existence", while 224,000 jobs were supported by SMBs using TikTok as a platform to grow and expand their business [13].

CNBC's Squawk Box on Wednesday, adding that a ban could trigger retaliatory actions from China, potentially impacting American companies deeply embedded in Chinese supply chains and consumer markets. Apple, the second-largest company by market capitalization in the U.S., and Tesla, ranked 12th, find themselves in the crosshairs of the geopolitical tensions. In 2023, Apple reported revenues of $20.82 billion from China, a substantial drop of 12.9 percent from the previous year yet still almost 20 percent of its total sales. Tesla's reliance on the Chinese market is similarly notable, with the electric vehicle giant generating $21.75 billion in revenue from China in the same year, amounting to about 22.5 percent of its total revenue. Their economic entanglement points to the substantial impact any retaliatory measures by China could have on the tech giants[14].

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 01 Jan. 2025, pp: 243-248 www.ijaem.net ISSN: 2395-5252

IV. MEASURES AND STRATEGIES THAT COULD BE ADOPTED BY SOCIAL MEDIA PLATFORMS IN TERMS OF DATA PROTECTION

- They should stop collecting data of users that could easily be used to identify them, Examples are phone numbers, address, and date of birth.
- Data of user should not be stored on the server of social media platforms; it should be on the devices of each user and when one wants to access it is called. The advantages of this includes users having control over their data, it may be difficult for hackers to have access to large data at the same time.
- If platforms will collect large data, then they should have robust security in place to protect these data. They should encrypt user data during transmission and storage, and they must conduct audits to identify vulnerabilities and address security gaps. They must abide by the data collections policies of countries they operate in. They must seek consent of users before data is sold. In addition to these are offering granular privacy settings, allowing users to control who sees their posts, profile information, and contact details and encouraging two-facto authentication,
- I am of the view that users should have control over what data they want to make available and what has been made available. Users should be able to wipe out their data completely from those platforms.
- Continuous education of users and issue transparency reports when needed.

4.1 Prospects and Predictions of Future Data Protection Trends and Developments

- Data localization is a sure way to go in the future. As stated in 6.0 as to how data could be protected. Both localizing on individual device and in the country of citizenship of individuals. There is likely to be a shit in cloud services in the near future[16].
- Adoption of Privacy Enhance Computation(PEC). PEC techniques protect data in use, allowing organizations to perform data processing and analytics that were previously hindered by privacy or security concerns. Gartner predicts that by 2025, 60% of large organizations will use at least one PEC technique in analytics, business intelligence and cloud computing[16].
- Countries will resort to data sovereignty. This has started and it is expected to deepen. Countries will want their data stored in their country[17].
- Expected strong and tougher data protection law by countries.

V. CONCLUSION

It could be seen that a complete ban of TikTok may not be the best solution to the concerns raised by the US although they are legitimate. The reasons are American Tech companies (Facebook for example) was hacked and data of users were stolen. Meta, TikTok and X (formerly Twitter) have been fined over $3 billion for GDPR violations. Probably, because the US does not have a more comprehensive personal data protection laws, that may be raising the fears. A more unified personal protection data policy like the GDPR may be a solution. For example, due to the GDPR, TikTok has to invest in servers located in Europe to store the data of European citizens. As stated in the CNBC news, the world is a global village, and governments must promote fair competition which is good in building businesses. Finally, the United States as an owner of the data of its citizens, wants to make sure that the stewards which is TikTok arebeing diligent with citizen's data. The US has to know that it is a win-win situation, the stewards and the owners all benefit on a social media platform but both make sure they carry out their responsibilities for a mutual benefit.

REFERENCES:

[1]. (Written by: Vytautas Kaziukonis, Five Data Privacy Trends To Watch In 2023 (forbes.com)
[2]. Top Trends in Big Data for 2024 and Beyond | TechTarget
[3]. Social media regulation in the United States: Past, present, and future - Ascend Magazine Website
[4]. (Contributed by Ken (Jianmin) Dai and Jet (Zhisong) Deng, Dentons) China's Personal Information Protection Law (PIPL) - Bloomberg Law
[5]. https://www.gdprsummary.com/gdpr-summary/https://www.skadden.com/Insights/Publications/2021/11/Chinas-New-Data-Security-and-Personal-Information-Protection-Laws
[6]. https://www.hrw.org/news/2023/08/14/chinas-social-media-interference-shows-urgent-need-rules
[7]. https://www.dataguidance.com/sites/default/files/gdpr_v_pipl_.pdf

[8]. S.314 - 104th Congress (1995-1996): Communications Decency Act of 1995 | Congress.gov | Library of Congress
[9]. (credit: Nicola Agius on March 13, 2024, https://searchengineland.com/us-house-passes-bill-tiktok-bytedance-sell-ban-438392).
[10]. https://crsreports.congress.gov/product/pdf/IN/IN12131
[11]. The Complex Case of TikTok in the United States - The CGO
[12]. TikTok Shares Data on Its US Economic Impact Amid Renewed Scrutiny | Social Media Today
[13]. Would a TikTok Ban Be Good for the US Economy? (newsweek.com)
[14]. To Protect Free Speech, Congress Should Consider Alternatives to Banning TikTok | Cato Institute
[15]. Awofadeju, M. O., Tawo, O., Fonkem, B., Amekudzi, C., Fadeke, A. A., & Faisal, R. (2024). Integrating cyber forensic analysis into real estate investment: Enhancing security and boosting investor confidence. IRE Journals, 7(6), 390-396. https://doi.org/10.5281/zenodo.14503290
[16]. https://www.gartner.com/en/newsroom/press-releases/2022-05-31-gartner-identifies-top-five-trends-in-privacy-through-2024
[17]. https://www.accessnow.org/the-future-of-data-protection-what-we-expect-in-2021/
[18]. Awofadeju, Martins O., et al. "Strategies for Mitigating Cybersecurity Challenges to Fund Management in the Digitalized Real Estate Industry." Magna Scientia Advanced Research and Reviews, vol. 11, no. 1, 2024, pp. 385–398. https://doi.org/10.30574/msarr.2024.11.1.0061.