Sam Newman

24 March 2023

TikTok: Data Vulnerabilities and Need for Government Action

TikTok is the second fastest to app to have one billion users, has the seventh most users of all social media platforms, and 62% of TikTok users are between the ages of 10 to 29 (Oberlo). While the app has been praised for its entertainment value and is incredibly popular, there are growing concerns about its security and privacy implications. For these reasons, many countries have banned TikTok from government devices and some have gone farther by restricting access for all citizens. Countries have taken such action due to questionable data collection policies, TikTok's strong ties with the Chinese government, and the apps capabilities of spreading disinformation. This essay will briefly outline why some countries have banned TikTok before arguing that governments should swiftly ban the use of TikTok on government devices to protect sensitive data and the spread of disinformation.

Countries Banning TikTok

On July 3, 2018, Indonesia became the first country to place a ban on TikTok due to "in appropriate content for children", however the ban was lifted just eight days later, as TikTok promised to improve its' content moderation (Johnson). Since 2018, other countries have followed Indonesia's lead, most opting to ban TikTok from government devices and a few countries outlawing TikTok from citizens' devices as well. In 2020, India banned TikTok, along with 58 other Chinese apps, due to national security concerns, claiming that these apps were "engaged in activities prejudicial to sovereignty and integrity of India" (Kumar). India's ban reduced TikTok's users by around 200 million users (Maiorca) as many fled to rival social media

apps, especially Instagram (Tak). Other countries, such as Pakistan and Bangladesh, have banned TikTok due to concerns about the inappropriate content and spread of disinformation. In Pakistan, TikTok was banned after the country's telecommunications regulator received complaints about "immoral and indecent" content on the platform (Zahid). In Bangladesh, the concerns were raised about the spread of fake news and disinformation, resulting in a ban (Kumar).

While counties like Indonesia, Pakistan, India, and Bangladesh have restricted civilians' access to TikTok, most countries have opted to ban TikTok from government devices. This is especially true in western countries. The United States, United Kingdom, Canada, New Zealand, Taiwan, Latvia, the European Union, Australia, Denmark, Belgium and 19 states in the U.S., have elected to ban TikTok from solely government devices (Tak). While most of these bans have occurred in just the past six months, concern of TikTok to national security is not nascent. In 2020, the TikTok faced a potential ban in the United States due to concerns about data privacy and its ties to the Chinese government. The Trump administration argued that TikTok's data collection practices posed a national security threat, and threatened to ban the app unless it was sold to a U.S. company (Satariano). Ultimately, the ban was never enforced. However, on December 30, 2022, President Biden approved the "No TikTok on Government Devices Act", prohibiting the use of the app on government owned devices (Johnson). The U.S. ban has since triggered a wave of TikTok bans on government devices throughout the Western world and more countries are expected to follow suit. While some countries have cited national security concerns as the primary reason for banning TikTok, others have focused on concerns related to content moderation and the spread of fake news. Regardless of countries' reasons, there is grand momentum to reign in the use of TikTok on government devices.

Relationship Between ByteDance and Chinese Government

TikTok collects a significant amount of data from its users, including location data, device information, and IP addresses, which is used to target users with ads and to improve the app's algorithm (Hsu). While this type of data collection is not unusual for social media apps, the fact that TikTok is owned by a Chinese company, ByteDance, has raised concerns about the potential for misuse of this data, given that the data is located on servers in China (Tak) and ByteDance's strong ties to the Chinese government (Johnson). This corporate-government relationship is typical for many Chinese companies since most Chinese businesses have an internal Chinese Communist Party (CCP) committee (Wang). For ByteDance, this position is held by the vice president of ByteDance, Zhang Fuping, which is problematic given the elevated role that Fuping holds in the company. One of the committee's roles at ByteDance is to "regularly gather to study President Xi Jinping's speeches" and "pledge" to innovate in technology (Wang). In exchange for ByteDance's cooperation and support, the Chinese government gives ByteDance research and development subsidies, tax breaks, and other forms of support (Hsu). Such financial support makes it hard for Chinese tech companies to resist a relationship with the government, despite Chinese government demands from tech companies. For instance, according to the Australia Policy Institute, ByteDance was asked to "disseminate state propaganda" downplaying the Beijing's abuses in two major Chinese cities (Wang). While it is tempting to judge ByteDance's compliance, there is a history of China strongly prosecuting companies that don't comply with governmental values and political agendas. For example, ByteDance was once forced to shut down a product for "vulgar content" and was only able to reinstate the product after the company's founder published a video that both apologized for "deviating from socialist values" and promised to ensure that government "voices are broadcast to strength" (Hsu). The ability for

China to financially strangle ByteDance into coercion underscores the vulnerability of TikTok's data security. The Chinese government has great economic and social control over ByteDance's operations which is a grave concern in the protection of user data on TikTok servers.

There is a concerning history of cooperation and manipulation between ByteDance and China, which should cause concern for data protection on TikTok. It remains unknown if the Chinese government has accessed user data from TikTok or if ByteDance would cooperate in giving the Chinese government user data. However, it is abundantly clear that ByteDance and the Chinese government have a working relationship founded on fear and cooperation. Motivation for Chinese officials to access the data could range from a desire to manipulate and influence government officials, gain insight into US government operations, or other political advantages. The feasibility and plausibility of the Chinese government wanting to access user data from TikTok should prompt countries to remove TikTok from government devices.

Lack of Transparency

Another area of concern is TikTok's lack of transparency in respect to data privacy, data collection, and content moderation practices. TikTok collects the following data on its' users: email address, phone number, date of birth, device information, location information, phone contact list, browser and search history, and anything from the device's clipboard (Baker-White). However, the organization has failed to communicate how it collects the data and what is does with the stored data. A revealing report by the Electronic Frontier Foundation concluded that TikTok's data collection practices are "vague and unclear" and do not provide sufficient transparency to users (Gronewold). This has led to lawsuits and TikTok pleading guilty to multiple cases of improper uses of data. In 2021 alone, ByteDance settled more than 20 lawsuits for $92 million dollars and was fined for illegally retaining data on minors (Baker-White). While

the cause of the lawsuits varied, most centered on TikTok failing to notify users about data collection policies or giving away user data to third-party organizations without user consent, both illegal activities. A clearer privacy policy could help TikTok right it's course and improve trust outside the organization. However, until TikTok significantly improves their communication on data protection, governments officials' access should be revoked. Another example of ByteDance's illegal use of user data was its' plan to use TikTok user location information to monitor the "physical location of specific American citizens" (Baker-White). Uncovered by an investigative report by Forbes, ByteDance later denied the claims (Gronewold). Various reports have pinned similar acts of data protection malpractice against TikTok. In a lawsuit filed by the US government against TikTok, the app was accused of collecting data on its users without their consent (Johnson). Although the company has made significant strides in user consent, it seems that TikTok has a corporate tendency to ask for forgiveness instead of permission.

A diverse coalition of watchdogs, government organizations, and lawyers have raised the alarm on TikTok's lack of transparency in respect to privacy policy and data collection. Although TikTok has improved in transparency, their changes have been too slow and have occurred only in reaction to oversight. Thus, governments would be prudent to restrict the quantity of data that TikTok collects from government officials.

Susceptibility to Cyber Attacks

Additionally, TikTok is more vulnerable to cyber-attacks than other social media applications due to several features of the app. Many of these vulnerabilities were exposed via a report by Check Point, a cybersecurity firm. The report explained the cyber-attacks could

manipulate the content on user's accounts, extract personal information, and have general access to the account (Carlos). Hackers could also send a text message to a user and, upon clicking the link, a hacker could access the user's account and content. This would be an effective attack since most of the app's users are between the ages of 10 and 29 and lack digital safety habits. Other research found that a security hole which allows cyber-attackers to "manipulate videos, delete user content, and make private videos public" (Adkoli). All three of these outcomes have potentially huge ramifications if they were conducted on a government device containing confidential information. The possibility of having a prominent government official's video manipulated could interfere with elections, public messaging, and compromise the individual in a ransom. To TikTok's credit, once these issues were brought to the companies attention they were quickly resolved. However, users must update to the most recent version of the application, otherwise they will continue to old forms of the application.

Another vulnerable feature of the app is that TikTok does not require two-factor authentication, unlike most social media platforms (Zahid). This signals that TikTok does not value user security as much as other popular social media platforms. Additionally, TikTok's platform of user-generated content makes it easier for cybercriminals to exploit vulnerabilities in the platform (Carlos). Given that 100% of the app's content is user driven, the ability to manipulate user content will disrupt a significant portion of the application. A separate report by Check Point discovered that TikTok's algorithmic video recommendation system can be manipulated to spread malware and phishing attacks (Adkoli). TikTok has been subject to great criticism for its' video algorithm, however it has not been widely publicized that the algorithm is also vulnerable to cyber-attacks. Lastly, TikTok's allows third-party integrations which exposes user data to applications outside of TikTok's surveillance.

Personal information stored in TikTok is at great risk given the platform's susceptibility to pernicious cyber-attacks, especially for government devices. A cyber-attack on a government device could have far reaching consequences to government officials' public persona, personal safety, and national security. TikTok's relaxed security policies reflect ByteDance's propensity to be reactive instead of proactive in protecting user information. All individuals, and especially government officials, should take necessary precautions in protecting their personal information.

Tool for Disinformation

Given the apps' international popularity, there is the potential for TikTok to spread propaganda or disinformation. TikTok's platform relies on enormous quantities of being constantly uploaded which complicates the ability to moderate TikTok content for deep fakes, edited information, and fake news stories. Furthermore, editing videos is an integral part of the app design, as users are encouraged to create, edit, and publish their personal videos. Thus, the line between harmful, dangerous edits and creative edits is "opaque" (Hart and Snell). TikTok's difficulty to censor disinformation is emphasized in a report by the US Senate Committee on Homeland Security and Government Affairs which identified TikTok as a "potential tool" for the Chinese government to spread propaganda and disinformation (Zahid). TikTok's global popularity entices cyber-attacks because a single video containing disinformation could have far-reaching impact given its' one billion users. For the aforementioned reasons, it is difficult to identify, let alone prevent, the dissemination of disinformation on TikTok. A malevolent use could be portraying false information as true or dramatically influencing public opinion. Additionally, TikTok's algorithm encourages users to continue watching videos containing disinformation. This was confirmed by SumOfUs, a corporate accountability advocacy group, watching 20 videos that doubted the integrity of the election system. Within one hour, the

algorithm only pushed videos containing “election disinformation, polarizing content, far right extremism, QAnon conspiracy theories and false Covid-19 narratives” (Hsu). TikTok not only hosts pernicious content, but it actively promotes factitious content to users.

The difficulty in moderating TikTok’s content coupled with the algorithms design, creates an infectious environment if a cyberattack occurred. ByteDance’s relaxed disposition in respect to protecting user data should motivate governments to block use of the app on government devices. Otherwise, irreparable harm could be inflicted upon government officials, citizens, or national security through the production and dissemination of disinformation.

Conclusion

In 2018, Indonesia became the first country to temporarily ban TikTok. Five years later, more than 15 other countries have joined Indonesia, and more than ten of those bans have occurred in the past five months. While this is encouraging news, there are still many countries that have yet to react to TikTok’s presence on government devices, especially countries with lower Gross Domestics Product’s (GDP). Countries with lower GDP’s typically have more unstable institutions which are more susceptible to damaging disinformation. All countries must act quickly in banning TikTok from government devices as a necessary precaution to protect national security. While this does not the eliminate the threat of TikTok being weaponized, it is a low-cost action that reduces some amount of risk. Opponent’s may argue that government officials could then download the app form their personal phones, however that is still distancing the government from TikTok. While TikTok is not a malicious company, it’s close relationship with the Chinese government, lack of transparency in its’ privacy policy, vulnerability to cyberattacks, and potential for disinformation, should concern countries around the globe.

Countries must swiftly ban TikTok from government devices before their inaction becomes the newest viral video.

Works Cited

Adkoli, Jayashree. "TikTok App is Filled with Vulnerabilities." Cybersecurity Insiders, Cybersecurity Insiders, 17 Aug. 2020, https://www.cybersecurity-insiders.com/tiktok-app-is-filled-with-vulnerabilities/. Accessed 21 Mar. 2023.

Baker-White, Emily. "TikTok Owner ByteDance Is Still Collecting And Sharing American User Data, Despite Settlements And Promises To The Contrary." Forbes, 20 Oct. 2022, https://www.forbes.com/sites/emilybaker-white/2022/10/20/tiktok-bytedance-surveillance-american-user-data/?sh=6f9a031a6c2d. Accessed 21 Mar. 2023.

Carlos, Juan. “Check Point Research Reveals Multiple Vulnerabilities in TikTok”. Check Point, 08 Jan. 2020, https://www.checkpoint.com/press/2020/check-point-research-reveals-multiple-vulnerabilities-in-tiktok/. Accessed 21 Mar. 2023.

Gronewold, Nathan. "TikTok Denies It Harvests User Data to Monitor Americans' Locations." New York Post, 21 Oct. 2022, https://nypost.com/2022/10/21/tiktok-denies-it-harvests-user-data-to-monitor-americans-locations/. Accessed 21 Mar. 2023.

Hsu, Tiffany. "Worries Grow That TikTok is New Home for Manipulated Video and Photos." The New York Times, The New York Times Company, 4 Nov. 2022, https://www.nytimes.com/2022/11/04/technology/tiktok-deepfakes-disinformation.html. Accessed 21 Mar. 2023.

Johnson, Hermes. “Indonesia Overturns Ban on Chinese Video App Tik Tok.” *The Straits Times*, 11 July 2018, https://www.straitstimes.com/asia/se-asia/indonesia-overturns-ban-on-chinese-video-app-tik-tok. Accessed 21 Mar. 2023.

Kaspersky, John. "Is TikTok Safe?." Kaspersky Resource Center, Kaspersky, 29 May 2020, https://usa.kaspersky.com/resource-center/preemptive-safety/is-tiktok-safe. Accessed 21 Mar. 2023.

Lee, Carol E. "TikTok Now Has 150 Million Active Users in the U.S., CEO to Tell Congress." *NBCNews.com*, NBCUniversal News Group, 19 Mar. 2023, https://www.nbcnews.com/politics/congress/tiktok-now-150-million-active-users-us-ceo-tell-congress-rcna75607. Accessed 21 Mar. 2023.

Oberlo, Jerry. "10 TikTok Statistics That You Need to Know in 2021". Available online: https://www. oberlo.com/blog/tiktok-statistics. Accessed 21 Mar. 20223

Maiorca, Danny. "In What Countries Is Tiktok Banned?" *MUO*, 4 Jan. 2023, https://www.makeuseof.com/what-countries-is-tiktok-banned/. Accessed 21 Mar. 2023.

Kumar, Hari. "India bans TikTok and 58 other Chinese apps in sweeping move." CNN, 30 Jun. 2020, https://edition.cnn.com/2020/06/29/tech/india-bans-chinese-apps-intl-hnk/index.html. Accessed 21 Mar. 2023.

Satariano, Adam. "TikTok's Chief Is on a Charm Offensive to Win Over Washington. It's Not Working." The New York Times, 24 Sep. 2020, https://www.nytimes.com/2020/09/24/technology/tiktok-trump-oracle-walmart.html. Accessed 21 Mar. 2023.

Tak, Abhi, et al. "Which Countries Have Banned TikTok in 2021 and Why?" *Amazon Seller News Today*, 25 May 2022, https://www.cruxfinder.com/banned-tiktok/. Accessed 21 Mar. 2023.

Wang, Yaqiu. “Targeting TikTok's Privacy Alone Misses a Larger Issue: Chinese State Control.” *Quartz*, Quartz, 24 Jan. 2020, https://qz.com/1788836/targeting-tiktoks-privacy-alone-misses-a-much-larger-point. Accessed 21 Mar. 2023.

Zahid, Farhan. "Pakistan bans TikTok for 'immoral and indecent' content." Al Jazeera, 10 Oct. 2020, https://www.aljazeera.com/news/2020/10/10/pakistan-bans-tiktok-for-immoral-and-obscene-content. Accessed 21 Mar. 2023.