London Politica X Warwick Think Tank

April 2023

THE SOCIAL FACE OF SPYWARE

Exploring TikTok Surveillance Practices

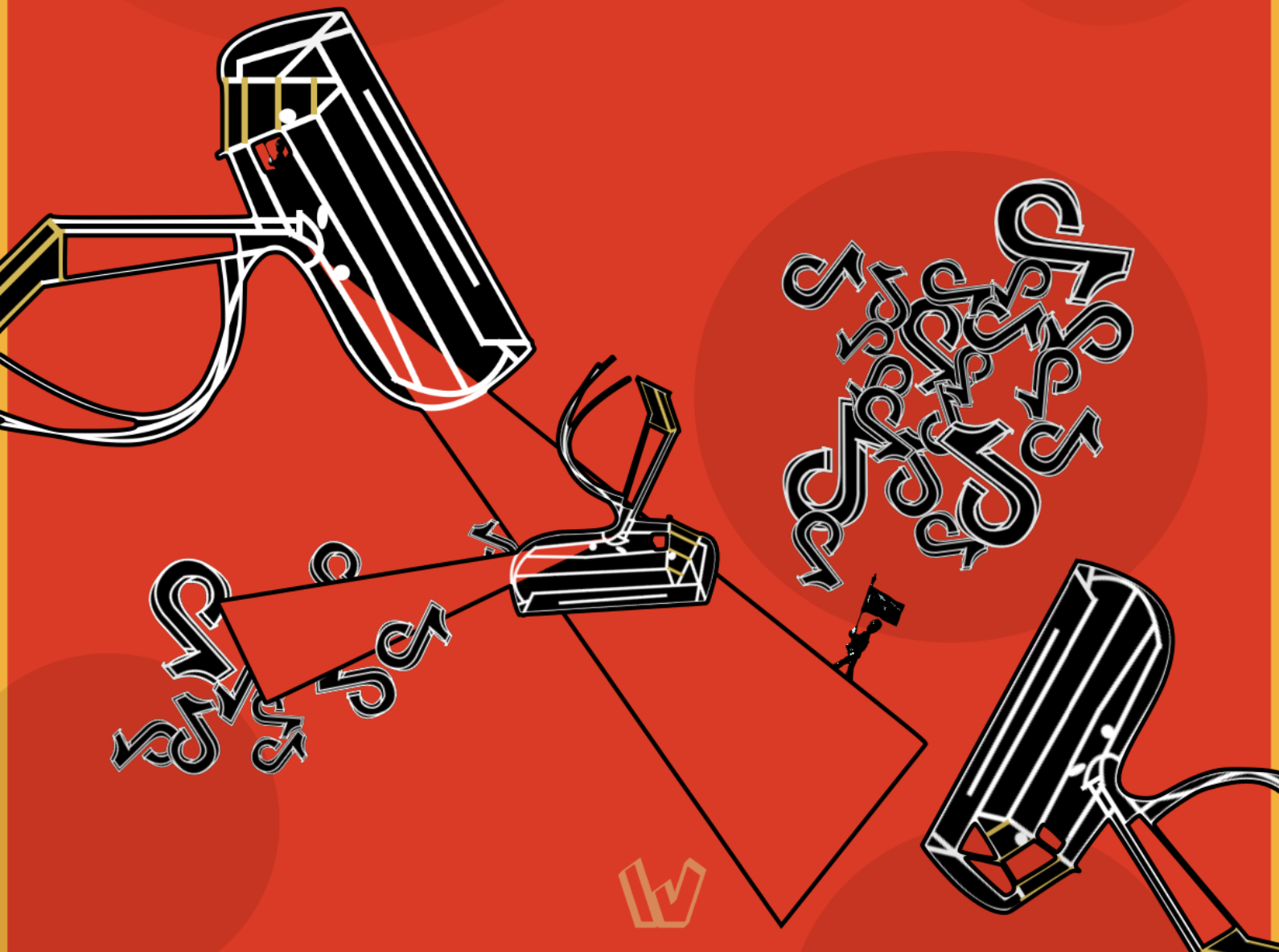


Table of Contents

Foreword

Cherifa Bourchak

Following the recent heated battle for a TikTok ban in U.S Congress earlier this month, the words ‘TikTok’, ‘China’ and ‘Spyware’ have taken the internet by storm. Privacy rights and regulation are no rarity in the world of social media politics, but TikTok’s surging popularity and its threat as a ‘non Western’ application has placed its potential risk in a category of its own. At the heart of this debate is the fight for control over TikTok’s algorithm, which has been branded as one of the most advanced uses of artificial intelligence in consumer technology. In the current climate of advertising legislation, regulatory crackdown and impending privacy laws combined with the recent U.S ban on semiconductors, makes TikTok’s spotlight on data privacy not only a global conversation with far reaching implications, but also an inevitable one.

The Social Face of Spyware report comes as part of a collaboration between **London Politica** and **Warwick Think Tank**, merging risk expertise with a policy concentration in a blend of investigative and analytical writing. As the title suggests, the report examines the ways in which the revolutionary social interface of TikTok may contain deeper interwoven systems of data collection, user tracking and surveillance tools that make it a substantial political threat. Through our series of articles, we delved into the ways in which TikTok has influenced propaganda, whether it can be used as a means of surveillance, how it compares in the face of long standing privacy regulations and its implications within the wider international landscape.

About:

London Politica is a leading pro-bono risk advisory company delivering bespoke analysis and actionable solutions for clients to navigate political risk. Together with our global team of analysts, our services are tailored to unique organisational goals, helping clients manoeuvre the international landscape day-by-day.

Website | London Politica
LinkedIn | London Politica
Email | contact@londonpolitica.com

Warwick Think Tank is one of the largest student-led think tanks in Europe. We serve as a dynamic and politically neutral space, bringing together a community of passionate and diverse students to engage in the world of policy.

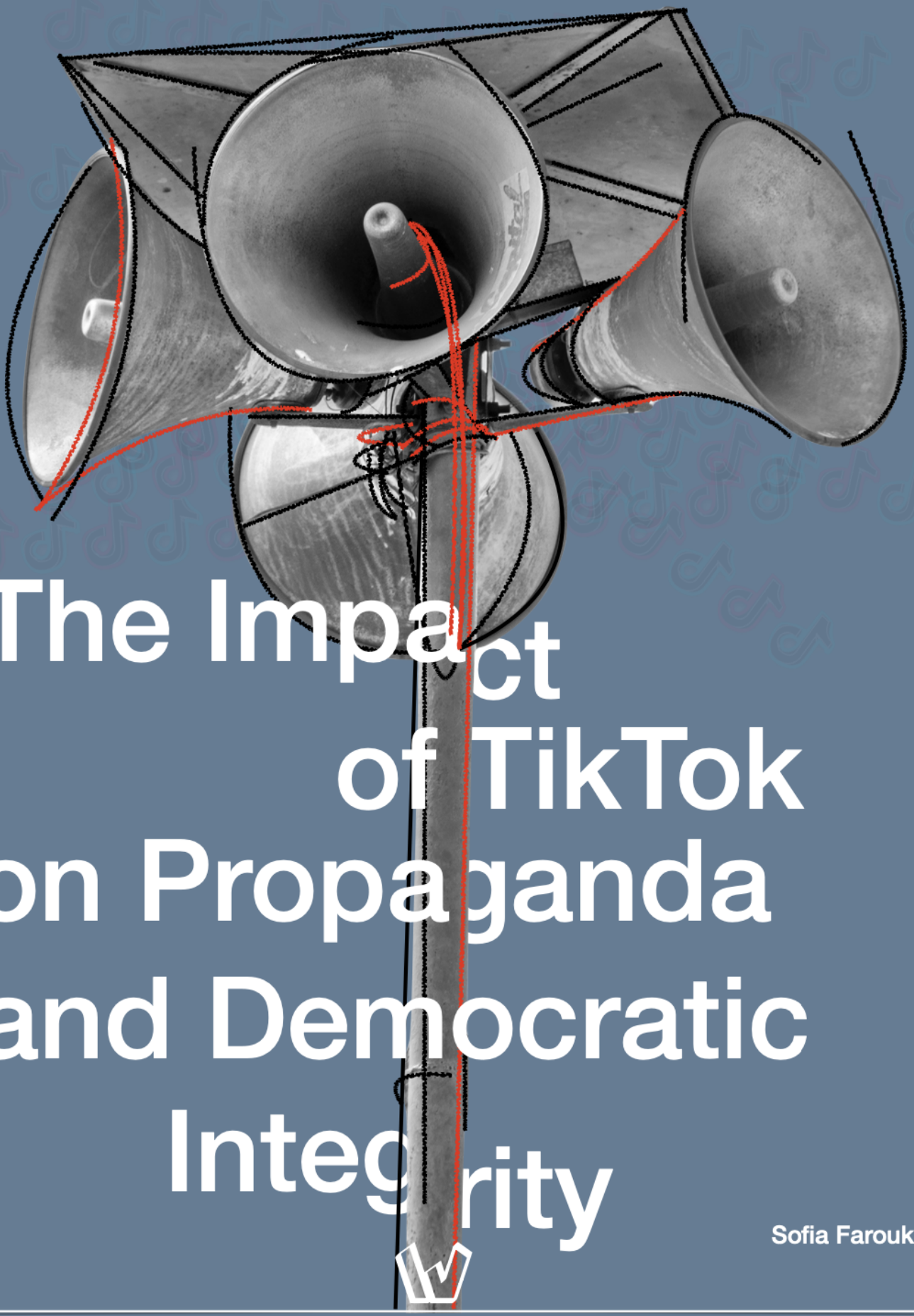
Website | Warwick Think Tank
LinkedIn | Warwick Think Tank
Email | warwickthinktanksoc@gmail.com

All graphics are created and designed by Anna Pang.

London Politica X Warwick Think Tank

Chinese Spyware & TikTok

April 2023



The Impact of TikTok on Propaganda and Democratic Integrity

Sofia Farouk

The Impact of TikTok on Propaganda and Democratic Integrity

by Sofia Farouk

In recent years, TikTok has emerged as one of the most popular social media platforms worldwide. However, its impact on democratic integrity and propaganda has been subject to scrutiny, prompting concerns about the app's potential to exacerbate political polarisation, spread disinformation, and incite racial tensions. This article aims to provide an initial examination of how TikTok has influenced propaganda and democratic integrity in the United States, India, and Malaysia. By evaluating its mechanisms, we can better understand the challenges posed by social media platforms like TikTok and develop effective solutions to safeguard against threats to democracy.

The proliferation of social media platforms has had a significant impact on the global political landscape, with TikTok being one of the most popular and widely used apps in recent years. However, TikTok's impact on democratic integrity has come under scrutiny due to various accusations of exacerbating political polarisation, spreading disinformation and propaganda, and inciting racial tensions. These accusations raise concerns about the potential impact of social media on democratic processes and highlight the need for effective content moderation policies to safeguard against such threats to democracy.

Proliferation of Racial Tensions:

TikTok has been accused of exacerbating political polarisation through the proliferation of extremist content on its platform, including content that incite racial riots and violence after the uncertain GE15 in Malaysia. In the 48 hours following polling day on Malaysia's 15th General Election, numerous posts were discovered on TikTok cautioning about the possibility of a recurrence of the deadly race riots on May 13, 1969. These posts received several hundred thousand views. With Malaysian history rooted in longstanding ethnic and racial tensions, May 13, 1969 signifies one of the most violent occasions of racial riots in Malaysia between Malaysia's Malay and Chinese communities, resurging trauma for many. As such the Malaysian Ministry of Digital and Communication demanded takedowns of such content. Similar cases in India ensued with content that demonises the Dalit group, circulating on TikTok and exacerbating tensions within the caste system.

While many would expand this trait with all social media platforms, the concept of short-form videos and algorithms promotes content that generates high levels of engagement and views, in essence making it difficult to control the dissemination of content once viral. These accusations raise concerns about the potential for social media to undermine democratic processes, and if left unchecked could lead to social unrest. These consequences

also highlight the need for effective content moderation policies and strategies that promote media literacy and critical thinking among users to safeguard against threats to democratic processes.

However, amongst democratic countries, TikTok's content governance has faced scrutiny alongside calls for better regulation of social media. Content moderation policies can be a double-edged sword; risking supressing legitimate speech and opinions while combating harmful content.In Malaysia, the government introduced new rules that require social media platforms to register and adhere to content moderation guidelines, granting them the authority to remove fake news or any content that threatens national security. But, with weaker democratic countries susceptible to corruption, there is an added layer of these paternalistic controls acting in the vested interest of politicians.

Crafting policies that effectively safeguard users from the dissemination of harmful content while preserving the principles of free speech and open debate represents a complex and multifaceted challenge. It is crucial to fully appreciate and scrutinise the potential impact of social media on democratic institutions, and to engage in the development of solutions that can guard against threats to the integrity of democratic processes.

Exacerbation of Disinformation and Censorship:

In the same vein, TikTok has faced serious accusations of promoting propaganda and disinformation, particularly in the US where the app was criticised for censoring content critical of China's government and spreading misinformation about COVID-19. These accusations raise concerns about the app's impact on democratic integrity and the potential for such platforms to be used as tools for spreading disinformation and undermining the democratic process.

TikTok's algorithms can contribute to the proliferation of propaganda and disinformation, resulting in a "filter bubble" that reinforces users' existing beliefs and opinions. This can make it easier for biassed or false information to spread unchecked, potentially leading to polarisation and division. Additionally, the app's content moderation policies can influence what content is shown to users, which can have implications on democratic values such as free speech and open debate.The algorithmic amplification of propaganda and disinformation can create an echo chamber that undermines democratic values, making it more difficult for users to engage with opposing viewpoints.

More than Propaganda: Mobilising Active Groups

TikTok's impact on democratic integrity extends beyond the social landscape, with empirical evidence revealing both positive and negative effects. In the US, the app mobilised young

people to attend political rallies and participate in activism. In India, it was used to spread false information during the Delhi riots, while in Malaysia, it disseminated misinformation about COVID-19 and the government's response. These examples demonstrate how TikTok can be used to mobilise groups and promote political engagement, but also highlights its potential for spreading propaganda and disinformation, ultimately undermining democratic values. TikTok's role in promoting civic engagement should be acknowledged, but the potential risks of its use in spreading propaganda and disinformation should not be ignored

With over 1 billion active monthly users, TikTok has extensive reach that has far-reaching implications for democratic integrity. While these platforms have been accused of exacerbating political polarisation, disseminating propaganda and disinformation, and inciting racial tensions, they have also been used to mobilise young people and promote political engagement. The development of effective content moderation policies that strike a balance between protecting users from harmful content while preserving free speech and open debate is a challenging task that requires careful consideration.

The impact of social media on democratic integrity is a multifaceted issue that requires an interdisciplinary approach for a comprehensive understanding. The susceptibility of young people to the spread of misinformation and propaganda on social media, coupled with algorithmic recommendation systems that amplify certain content, can exacerbate political polarisation and promote disinformation campaigns. Nevertheless, social media platforms like TikTok can also foster online communities and provide a platform for political engagement, leading to increased civic participation. Developing effective content moderation policies that balance the competing demands of protecting users from harmful content while preserving free speech and open debate is crucial. By promoting critical thinking, media literacy, and awareness of the potential impact of social media on democratic integrity, we can work towards solutions that safeguard against threats to democracy. Ultimately, a balanced approach to social media regulation can ensure that these platforms contribute positively to democratic integrity.

>/TikTok[Surveillance_Practices]


```
<!DOCTYPE html>
<html data-require="tiktok" + "pixels"
<head>
        <meta http-equiv="chinese spyware"
        ">

        <title>TikTok Pixels as [Potential] Chinese Spyware

        <script src="privacy policy"
</head>
<body>
         <div class="actions, behaviours">
         <var id="meta pixels"
         <var id="google analytics"
         <UIDs>

              <div class="blackmail"?
```

<Ella Startt>

TikTok Pixels as Potential Chinese Spyware

by Ella Startt

Worries about the Chinese social media company TikTok sharing sensitive user data with the Chinese Communist Party (CCP) have steadily increased in countries wary of China's global expansion efforts. Most recently, the Biden administration in the U.S. approved legislation on March 1st 2023 giving the president power to ban the application on the national level. Discussions around national security risks posed by TikTok have largely focused on in-app big data that could be transferred to the CCP upon their request, as all Chinese companies are required to comply with Chinese authorities under article 7 of the PRC's National Intelligence act. But there is another, less-known risk associated with data saved on TikTok servers that could have wider-reaching implementations: the increasing presence of TikTok pixels on websites.

TikTok pixels refer to HTML code snippets that website administrators can install to track user actions, behaviours, and conversions through their activity log, which can be activated on any website by its administrator. The main beneficiaries from these pixels are businesses that want to create more targeted marketing campaigns to boost website visibility and company revenue where applicable. However, a joint study between security firm Disconnect and Consumer Reports revealed that an increasing number of governmental, educational and medical websites dealing with sensitive information where users are likely expecting more data privacy measures, have also been turning to TikTok's analytical tool. TikTok pixels aren't dissimilar from its American counterparts Meta Pixels and Google Analytics, as these can all collect user IP addresses, search terms, pages being clicked on and more. Meta Pixels have already been implicated in several lawsuits for using sensitive information acquired through pixels installed on medical websites to target individuals with very specific ads related to their health conditions. Considering Meta's recent legal scrutiny, it makes sense to draw attention to the data being collected and shared by TikTok pixels, especially at a time when worries have been mounting over the potential use of TikTok account data in Chinese cyberespionage activities.

The two most recent data-related scandals that TikTok has been tied to remain focused on data harvesting of TikTok user accounts. In June 2022, leaked audio files from 80 internal TikTok meetings confirmed that China-based engineers had access to US user's TikTok data between September 2021 and January 2022, showing that US data could be accessed within the CCP's jurisdiction, making TikTok legally obliged to comply with the Chinese Government if it requests any specific data, implying the CCP could request sensitive data to spy on targeted individuals outside Chinese territory, or access TikTok data to diffuse efficient propaganda campaigns. In December 2022, ByteDance's general counsel Erich Andersen admitted in an email to Agence France Presse in late December that ByteDance had indeed sought to find the source of a media leak by tracking two reporters based in the

US and the UK from their IP addresses linked to their TikTok accounts. In summer 2022, ByteDance had been tracking these two journalists after assuming they had potentially been involved in a data leak, and were tracking the two journalists' location to find ByteDance employees they crossed paths with. After the scandal, ByteDance allegedly fired the four individuals responsible and removed access to US data from the department involved, however some US politicians, including Republican Senator Marco Rubio who continues to warn against the usage of the social media app.

Whilst these two scandals have focused on cyberespionage of TikTok account data, many of these takeaways are interwoven within the political risks associated with TikTok pixels. The December scandal provided crucial insights into ByteDance's use of IP addresses to track individuals tied to TikTok accounts, data that TikTok pixels can also track. In addition, both the TikTok app and TikTok pixels send information such as unique IDs (UIDs), what users are searching for, clicking on or typing to TikTok servers. ByteDance has legal access to this data, as TikTok's privacy policy allows it to share its data with other members of its "corporate group", such as ByteDance. This data includes information received from websites that have TikTok pixels installed, which as previously seen, includes user IP addresses and what pages or ads they clicked on.

ByteDance has further been linked to having close ties with the Chinese Government, suggesting it would not hesitate to comply with the CCP if it ever requested access to TikTok data. ByteDance has bent to the pressures of Beijing before when it took down its Neihan Duanzi app upon the CCP's request. In a letter of self-criticism, ByteDance's CEO Zhang Yiming promised to deepen cooperation with party media and its diffusion of official party-line content. In addition, the Chinese government used its golden share in the company to place the CCP party official Wu Shugang on ByteDance's board of directors. According to the Wall Street Journal, this provides an avenue for Beijing to influence crucial aspects of ByteDance and TikTok's operations, including the fate of its algorithm.

It is worth noting that there have been no known instances of ByteDance accessing data provided by TikTok pixels with an intention of sharing it with the Chinese Government, but legally and technologically speaking, such a scenario is possible. The leaked recordings confirmed that US staff do not have the knowledge nor the right to access the data on their own, and that a Beijing-based engineer has "access to everything". Based on these recordings and TikTok's privacy policy - which authorises entities within ByteDance to access TikTok data for general functioning, content delivery, research and development, analytics and content moderation purposes – it is likely that Beijing-based engineers frequently handle TikTok data. As engineers within China's jurisdiction are able to access TikTok data, these engineers would be legally obliged to comply with article 7 of the National Intelligence Act, making the whole of this data at risk of being used by the CCP for various foreign policy goals.

TikTok pixels add another important layer to existing account information being stored on TikTok servers; the company possesses access to both TikTok and non-TikTok user online activity across all websites with the pixel installed. As such, TikTok pixels expand the breadth of data that ByteDance, and therefore the CCP, could access for cyberespionage activities. Numerous worries have mounted over what the CCP could theoretically do with all this data. The Chinese government was already caught in late 2020 contracting Zhenhua Data to compile dossiers on more than 2.4 million people globally.

With this in mind, accessing TikTok's database would be an ideal next step for the CCP. Considering the CCP's history of co-opting elites and blackmailing others to achieve its political aims beyond mainland China, data from TikTok's app and pixels could be used to force certain strategic individuals to cooperate with the CCP by leveraging retrieved data from search and browser histories revealing sensitive, controversial or humiliating information. More recently, several politicians have pointed to the CCP's potential manipulation of its powerful "For You" algorithm to advance its foreign policy goals, a scenario which could easily turn into a Cambridge Analytica scandal 2.0. TikTok pixels may therefore provide an opportunity to extend such manipulation to non-TikTok users, reaching audiences that might be sceptical about the app's functionality with convincing propaganda.

London Politica X Warwick Think Tank

Chinese Spyware & TikTok

April 2023

The TIKTOK ALGORITHM and Soft Influence

Andres De Miguel, Joris Zilinskis

The TikTok Algorithm and Soft Influence

by Andres de Miguel & Joris Zilinskis

TikTok's algorithm in effect is the process and set of code by which videos are recommended to users of the app. It takes into account your activity including likes, views and follows to determine the content you like the most and tailors the videos it shows you to fit those tastes. Initially, this may seem harmless, as with other social media apps that offer a competitive 'personalised user experience', one would not be at fault for seeing TikTok's version of this process as nothing out of the norm. While TikTok has been criticised as a security threat for many reasons by the west, the focus of this article is tied specifically to the algorithm, and its potential for radicalisation, invasion of privacy, and soft influence on its user base.

The Immense Power of the Tik Tok Algorithm:

TikTok's algorithm is more advanced at perceiving the identity and tastes of its users than anything that has been seen before on a social media platform. An experiment carried out by the Guardian on different people using the app for a limited number of times each day saw the algorithm catch on extremely quickly to the users' tastes and more importantly their specific identity. It determined one user was a Muslim south Asian girl within a day of use, and that another user was a mother who lived in the Bay Area of California within three. It is this hyper-advanced algorithm, with the opacity of said algorithm and the fact that the app now has 1 billion active monthly users, has made Tik Tok a cause for national security concerns. This concern is especially prominent in US discourse with worries that this data processing software has made it easier for users of TikTok to be subconsciously influenced by the algorithm of an app controlled by a Chinese company.

This view of Tik Tok as a force for the subtle influence of its users is not without merit. As well as carefully doctoring the content users do see, the app also carefully discerns the content that users don't see. A pseudonymous former employee at ByteDance explained its well-developed censorship protocol; with transcripts of live videos for analysis of sensitive content as well as Natural Language Processing Models to flag up any problematic individuals, the app creates a carefully revised image of the world that users then indulge in for an average of 1.5 hours a day, and for younger users this figure can triple.TikTok further has the ability to manufacture virality of content it sees to be good for the platform, as was revealed by Forbes, through a process called 'heating', which heavily contributes to a perception of reality manufactured by the app itself for its users to be absorbed into.

Even more troubling a prospect, the Tik Tok algorithm is made more efficient by the GPS data the app collects. This information is then used to suggest content that is relevant to the

user's location and interests. For example, if a user frequently interacts with content related to food and has a history of interacting with content in a specific area, TikTok's algorithm may suggest videos related to local restaurants or food events in that area. While the use of GPS data in recommendation algorithms can provide a more personalised experience for users, it also raises concerns about privacy and data security. Some users may feel uncomfortable with the idea of their location being tracked and used by a social media platform. Recently, it has been found that some TikTok employees have accessed the location data of specific journalists in the US when trying to look for information leaks from the company confirming the worries of the users. TikTok has addressed these concerns by implementing measures to ensure user data is kept secure and by providing users with control over their data-sharing settings. Still, the aggressive data-gathering activities have prompted multiple western governments to ban the application from government-issued smartphones.

The Algorithm as a tool for Radicalisation:

Although one could claim that this process of control within social media apps by the companies that control them is common, which is not wrong, TikTok goes a step further than its competitors due to the nature of the app and its inbuilt code. The concept of the 'For You' page means users don't have to do anything for Tik Tok to gather information on them since the videos shown on the 'for you' page are often of creators the user doesn't follow or has never seen. The average length of the videos shown on Tik Tok also means someone could consume hundreds of them in the span of a few hours, giving the algorithm plenty of data to calibrate the users' exact preferences. We have already seen the harmful effects of this process. An article from INSIDER on the self-radicalisation of TikTok's frequent users revealed the potential of the app's algorithm for sending its users down dark rabbit holes towards extreme, often right-leaning, ideologies, and radical groups such as ISIS due to its incredible capacity to recalibrate its idea of the user's tastes and begin pumping similar content to them almost instantly. Further, a Wall Street Journal study revealed TikTok's algorithm was more reluctant to show its users different types of videos when they have already been categorised into a certain viewpoint. This is extremely problematic, as 40% of TikTok's users are young individuals under 25 who are still forming their opinions and thus can be more easily pushed into extremist views.

On the other hand, TikTok has another tool which can decrease these effects - the interactive add-ons. This function was initially developed to allow users to collaborate on the same dance or song and increase the interaction rate, yet recently it was also used in political discussions. This has enabled many users to effectively drive home a specific point or present counterarguments to statements made in the original video to which they are responding. To examine this ability, a recent study analysed videos related to the 2020 US election. The study revealed that Republican-leaning users tended to express support for videos that aligned with their views, whereas Democratic-leaning users responded to Republican videos

by providing counterpoints. This finding indicates the potential for breaking the echo chamber created by the app, as it presents an opportunity for discourse and the exchange of ideas. However, the indoctrinating tendencies of the app could still persist. Therefore, the study suggests that making tweaks to the algorithm could promote interaction with issues that users care about, leading to a more diverse range of content and perspectives. Such changes could ultimately contribute to a more informed and engaged society, one where social media platforms like TikTok can be leveraged for meaningful dialogue and debate.

The Facial Recognition Problem:

Social media's broader problem with the mental health of its young users is also exacerbated by what has been coined TikTok's 'beautiful algorithm'. Through the use of facial recognition data, TikTok analyses the facial landmark map of a creator and rates their attractiveness on a scale of 1 to 5, with the creators at the top of the beauty scale receiving more exposure than those at the bottom end. The regular exposure to beautiful faces has clear ramifications for the mental health and confidence of young users on the app who can't help but compare themselves to the creators they see on the app every day. Even more problematic than this, is that the technology used to recognise faces also has a racial bias, since the faces creators are compared relative to are mostly Caucasian or Asian, those with differing features, but none the less generally attractive receive less exposure than their fair-skinned counterparts for they are deemed to be 'uglier' by the algorithm responsible for their success. Not only does this facial recognition bias reduce the reach of people with disabilities as well as queer and overweight individuals, but it also poses a major threat to security due to its natural association with surveillance technology.

But why is this being mentioned in an article about Chinese spyware? What does China have to gain from the influence Tik Tok has on the people that use it? The main concern is the difference between the content that western users are being shown on TikTok in comparison to Chinese users of Douyin, the Chinese version of the app. Young Chinese users are shown 'productive' content such as educational videos, museum exhibits and patriotic content, with a time limit of 40 minutes a day as opposed to the proliferation of mostly shallow, and more importantly endless, entertainment on western feeds. Tristan Harris, a former Google employee cites a study of pre-teens being asked what they would like to be in the future, with American children saying they want to be 'influencers' while Chinese children want to be astronauts.

In response to pressure from the US government and other Western entities, TikTok has attempted to modify its operations. To comply with EU regulations prohibiting the export of data outside the Union, EU users' personal data is stored in Ireland, while US users' data is stored on Oracle servers in the US to appease regulators. Despite these changes, concerns over access to personal data persist, as demonstrated by the recent unlawful access to

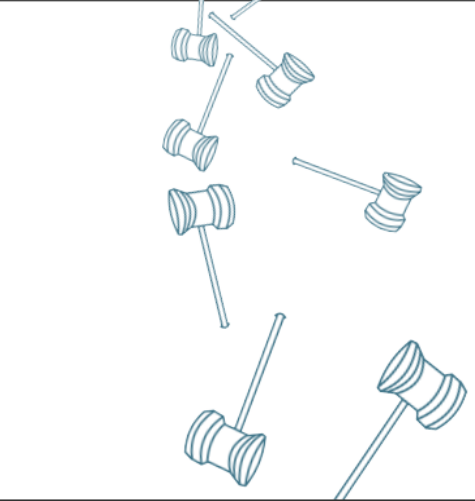
multiple journalists' GPS information, as mentioned above. To address this issue, ByteDance has implemented more stringent access restrictions for its Chinese moderators and relocated the headquarters of its non-China serving company to Singapore. Additionally, the company has established TikTok US Data Security Inc, an independent board responsible for overseeing the app's operations in the United States. While these changes represent important steps toward ensuring user safety, their effectiveness remains to be seen. It is essential to note that privacy and security concerns surrounding TikTok and similar apps are not limited to geopolitical tensions but also involve the legal and ethical responsibilities of companies towards their users. As such, ongoing scrutiny and continued efforts to enhance user data protection and privacy remain necessary.

The overall implications of the TikTok algorithm are evident, and the U.S.'s worries are put into perspective. A hyper-effective set of code for determining the identity of its users, recalibrated after every action taken, the potential for self-radicalisation and the general harmful effects of falling attention spans and mental health issues are taken to the extreme, it's no wonder Tik Tok has become a cause for concern and hot topic in political discourse. While attempting to make the algorithm more transparent might be difficult to accomplish, despite recent pushes from legislators, and outright banning the app coming with an instant wave of backlash from users, a potential solution to this issue may be to spread awareness and begin to collectively distance ourselves from technology with evidently harmful effects.

Chinese Spyware & TikTok

April 2023

The Legal Implications of TikTok Restrictions



Fabienne Bull

The Legal Implications of TikTok Restrictions

by Fabienne Bull

National concerns are emerging regarding the privacy and security of data collected by TikTok. An increasing number of states are prohibiting government officials from using the app, with several regions going so far as to establish nation-wide bans. Whilst legislative measures seem set to rise, legal actions against TikTok are likely to be accompanied by questions regarding the implications such restrictions have upon freedom of speech, censorship, and fair market practice.

Critically, states are concerned about cyber security and the protection of both nationally and personally sensitive information. Indeed, India has banned not only TikTok, but *dozens* of other Chinese-made apps, declaring them as 'prejudicial to the sovereignty and integrity of India, defence of India, security of state, and public order'. Both Bangladesh and Pakistan have instated several temporary TikTok bans over the last few years, and Indonesia has previously restricted access and deployed a short-term ban due to content concerns. More recently, the US, Canada, Taiwan, and the EU have introduced varying levels of restrictions of TikTok use by public sector employees.

In the US, Donald Trump did *attempt* to entirely bar use of the app, but was ultimately curtailed on free-speech grounds. However, recent weeks have seen the passing of Congress legislation to ban government employees from downloading or using TikTok on government owned devices. Pressure is mounting to deploy a national ban, with both Republicans and some Democrats urging the restriction under the bracket of national security concerns. Indeed, as of March 1st, further legislation has been passed to give President Joe Biden the power to instate the blanket ban, but it remains unclear whether this will come to fruition. Canada has banned TikTok on government-issued mobile devices, deeming it to '[present] an unacceptable level of risk to privacy and security', and European Commission employees will have to remove TikTok from both work and personal phones by March 15 for 'cybersecurity' reasons. It's worth noting that the escalating retreat from TikTok is not solely specific to public sector workers; a number of schools and universities have also removed it from school-owned devices whilst simultaneously discouraging students from using it for personal reasons.

Whilst the elevated discourse around TikTok restrictions is certainly indicative of rising national security concerns, actually banning the app remains controversial. Specifically, there are legal difficulties regarding free speech and private business, with concerns over the extent to which banning TikTok would be too extreme a form of censorship. Indeed, a spokesperson for China's foreign ministry has emphasised the need to 'respect the principles of market economy and fair competition, stop suppressing companies, and provide an open, fair and non-discriminatory environment for foreign companies'. India's removal of the app certainly

demonstrates the financially damaging implications of bans; prior to June 2020, the state was one of ByteDance's largest markets, accounting for 30.3% of the total TikTok app downloads. Aside from just damaging ByteDance's own revenues, any prospective bans would have a severe impact upon content creators, globally. Sponsored videos, the ability to direct audience traffic to other platforms, brand exposure, and donations from live streaming all rely on having as large an online following as possible. Nation-wide bans not only financially implicate the company itself, but the thousands of content creators who rely on the platform as a fundamental source of income.

The US faces some particularly nuanced difficulties in attempting to introduce a ban on TikTok; the legislation required is extensive, and many worry that it would force the government to sanction other companies that interact with ByteDance. Critically, this could include Korean and Taiwanese manufacturers that supply Chinese companies with semiconductor chip manufacturers, meaning the breadth of the US' legislation makes it logistically problematic. Unsurprisingly, a ban also directly implies political considerations; TikTok has over 110 million American users above the age of 18, many of which would not look kindly upon any unconsented withdrawal of access. Indeed, the American Civil Liberties Union (ACLU) observed that 'a ban on TikTok would violate the First Amendment rights' of all such users, and called for Americans to fight against this 'censorship' to reinforce their 'constitutional right to expression'. There are also concerns that banning access to TikTok through Apple Store and Google Play downloads will encourage people to 'jail break' their devices. Changing manufacturer settings on electronic devices implicitly increases security risks; software downloaded from unconventional means are far more likely to include privacy invading code. Rather than enhance security then, banning access could invertedly result in further privacy exploitation.

As a final point, it's important to recognise that any prospective ban in countries such as the US will be hindered by lobbying from TikTok and its parent company ByteDance. Last year alone, ByteDance spent nearly $5.4 million on lobbying, and this is only expected to increase. Given the huge market that TikTok has in the US, it is perhaps unsurprisingly that ByteDance is also seeking alternative means to circumvent restrictions; it's attempting to broker a deal with the US government to prevent an outright ban.

Contrary to the momentum seen recently in reducing TikTok influence, many countries remain ambivalent to TikTok's potential privacy violations. In terms of direct vocalisation, Australia has admitted it's not received any advice from its intelligence services to invoke similar measures, and the UK has announced it will not follow Brussels and the US in banning government employees from accessing it. It appears apparent that further restrictions on TikTok will be difficult to implement; the financial and political ramifications of outright bans are laborious to manipulate, and are likely to be met with as much internal resistance as external.

London Politica X Warwick Think Tank

Chinese Spyware & TikTok

April 2023

Are TikTok's Data Harvesting Practices More Concerning Than Instagram's?

Eleonora Trinchieri

Are TikTok's data harvesting practices more concerning than Instagram's?

by Eleonora Trinchieri

In recent years, social media platforms have become an integral part of our daily lives. Two of the most popular social media platforms are Instagram (1.4 B active users) and TikTok (1 B active users). As of January 2023, almost 31 percent of global Instagram audiences were aged between 18 and 24 years, and 30.3 percent of users were aged between 25 and 34 years. In the case of Tik Tok, 60% are between the ages of 16-24. 26% are between the ages 25-44. Both of these platforms have a massive user base, and they collect a vast amount of user data. However, there has been growing concern about the security risks posed by these platforms. The purpose of this article is to compare and assess which platform poses more risk to user security in terms of data harvesting - TikTok or Instagram.

TikTok:

TikTok is a social media platform that allows users to create short-form videos. It has become incredibly popular among younger audiences, and it has over a billion active users worldwide. However, TikTok has come under scrutiny for its data harvesting practices. In 2020, the Indian government banned TikTok, citing concerns over data privacy and national security.

One of the main concerns with TikTok is that it collects a vast amount of user data. This includes information such as location data, device information, and browsing history. TikTok has also been accused of collecting biometric data, such as facial recognition data, from its users. This type of data can be incredibly sensitive, and it raises concerns about how TikTok is using this data.

1. Personal information: TikTok collects users' names, email addresses, phone numbers, and other information that users provide when they create an account.
2. Location data: TikTok collects users' precise location data, including GPS coordinates, and may also infer users' location based on IP address or other signals.
3. Browsing history: TikTok collects information about users' browsing history, including the videos they watch, the comments they leave, and the accounts they follow.
4. Device information: TikTok collects information about users' devices, including their device type, operating system, hardware model, and other technical details.

5. Biometric data: TikTok collects biometric data, such as facial recognition data, from users' videos.
6. Advertisements: TikTok collects information about users' interactions with advertisements, including when they view an ad, click on an ad, or make a purchase after clicking on an ad.
7. Contacts: TikTok may access users' contact lists and collect information about the users' friends and family.

Besides the practical breaches of users' security, the threat that TikTok poses is also seen as a political one due to its ownership by the Chinese company ByteDance and the potential for the Chinese government to use the app to influence or interfere in foreign political affairs.

One concern is that TikTok could be used to spread propaganda or misinformation on behalf of the Chinese government. TikTok has been criticised for censoring content related to politically sensitive topics, such as protests in Hong Kong and human rights abuses in Xinjiang, which raises questions about its ability to promote a particular political agenda Another concern is that TikTok could be used to collect sensitive information on users, including their political beliefs and affiliations. TikTok collects a significant amount of data on its users, including their browsing history and location data, which could potentially be used to identify and target users based on their political views.

There have also been concerns that TikTok could be used to influence political campaigns, particularly in the United States. During the 2020 U.S. presidential election, TikTok was used to mobilise young voters and promote political content. While this in itself is not necessarily a threat, it does raise questions about the potential for foreign actors to use TikTok to influence political outcomes.

Overall, while there is no direct evidence that TikTok poses a significant political threat, the potential for the Chinese government to use the app to influence foreign political affairs is a cause for concern. It is important to remain vigilant and take steps to protect the privacy and security of users on the app.

Instagram:

Instagram is a photo and video sharing social media platform that has over 2.2Bn active users worldwide. It is owned by Facebook, which has also come under scrutiny for its data harvesting practices. However, Instagram has not faced the same level of scrutiny as TikTok when it comes to data privacy.

Instagram collects a large amount of user data, including location data, device information, and browsing history. It also collects data about users' interests, preferences, and behaviour

on the platform. This type of data can be used for targeted advertising, which is a common practice among social media platforms.

1. Personal information: Instagram collects a range of personal information from users, including their name, email address, phone number, and date of birth. This information could potentially be used for identity theft or targeted advertising.
2. Location data: Instagram collects users' location data, including their GPS coordinates, which could potentially be used to track users' movements and target them with location-based ads.
3. Search history: Instagram collects information about users' search history on the app, which could potentially be used to target users with personalised ads or to infer information about their interests or behaviours.
4. Content engagement: Instagram collects information about the content users engage with on the app, such as the photos and videos they like, comment on, or share. This information could be used to personalise users' feeds or to target them with ads.
5. Contacts: Instagram may access users' contact lists and collect information about the users' friends and family. This information could be used for targeted advertising or to infer information about users' relationships or social networks.
6. Facial recognition: Instagram uses facial recognition technology to identify users in photos and videos, which raises concerns about potential privacy violations and the use of this technology for surveillance purposes.

One of the main concerns with Instagram is that it is owned by Facebook. Facebook has faced numerous privacy scandals in recent years, including the Cambridge Analytica scandal, where it was revealed that the company had harvested the data of millions of Facebook users without their consent. This has led to concerns that Facebook may be using Instagram's user data in a similar manner.

Comparison:

When comparing TikTok and Instagram in terms of data harvesting, there are several factors to consider. Firstly, TikTok collects a vast amount of user data, including biometric data, which is a cause for concern. Instagram also collects a significant amount of user data, but it is not known to collect biometric data.

Secondly, TikTok is owned by a Chinese company, which has raised concerns about the Chinese government potentially having access to user data. Instagram is owned by Facebook, which has faced numerous privacy scandals in recent years, but there is no evidence to suggest that Facebook is using Instagram's user data in an inappropriate manner.

Thirdly, both TikTok and Instagram use user data for targeted advertising. However, Instagram's advertising practices are more transparent, and users can control the type of ads they see. TikTok's advertising practices are not as transparent, which raises concerns about how user data is being used.

In conclusion, both TikTok and Instagram collect a vast amount of user data, which raises concerns about user privacy and security. However, TikTok's data harvesting practices and political implications seem to be more concerning to most Western countries than Instagram's. This is because TikTok collects biometric data, which is incredibly sensitive, and there are concerns about the Chinese government potentially having access to user data as the regulations of the platform have extremely blurred lines.