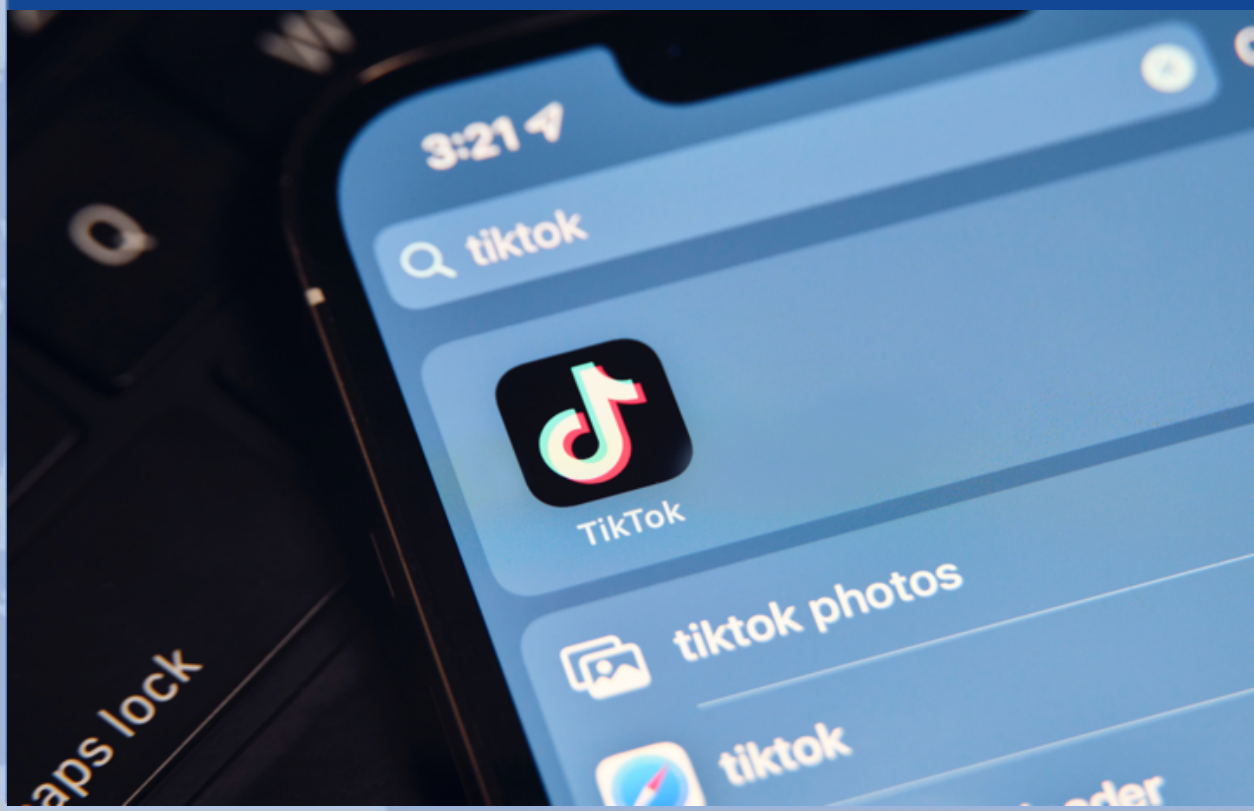
An EU solution to a Chinese app: Regulatory approaches towards TikTok's risks

LEIDEN ASIA CENTRE
Partners in Research and Knowledge

Daan Kingma



September, 2023

The LeidenAsiaCentre is an independent research centre affiliated with Leiden University and made possible by a grant from the Vaes Elias Fund. The centre focuses on academic research with direct application to society. All research projects are conducted in close cooperation with a wide variety of partners from Dutch society.

More information can be found on our website:

www.leidenasiacentre.nl

For contact or orders: info@leidenasiacentre.nl

M. de Vrieshof 3, 2311 BZ Leiden, The Netherlands

LEIDEN ASIA CENTRE

Partners in Research and Knowledge

Abstract

TikTok has become an archetypical example of Chinese digital companies going global. Its connection to China, however, has led to unprecedented scrutiny over the company's policies regarding data collection and privacy, content moderation, and recommendation algorithms. This policy brief takes a closer look at the concrete risks posed by the app, specifically its alleged CCP connection, its perceived cyber security risks, and the subjection of its parent company to Chinese security legislation. Drawing from several earlier reports into TikTok's alleged China connection, it finds that none of the risks ascribed to TikTok have been sufficiently substantiated to warrant an all-out ban that some EU policy makers and security analysts argue for. Rather, this policy brief recommends that the EU should apply its existing stringent regulatory framework for data services, which provides solutions for all of the concerns raised with regard to TikTok.

Contents

Key policy takeaways

1. **A balanced approach towards TikTok**

European regulators should take an approach towards TikTok that is proportional, evidence-based, and takes the principles of a free market and level playing field into account. Valid concerns about political influence and data security should be recognized, while knee-jerk reactions that single out TikTok solely based on its Chinese origin should be avoided. By uniformly applying regulatory measures across digital services, the EU can address risks while upholding fundamental rights.

2. **Shift in perception: TikTok is not unique**

While TikTok continues to take centre stage in the public debate surrounding political interference and data security, policymakers should recognize that the challenges posed by the platform are not unique to TikTok alone. Many of the issues raised, such as content moderation and algorithmic content recommendation, as well as privacy and security concerns, are prevalent across a wide spectrum of online platforms. Focusing solely on one platform risks overlooking systemic vulnerabilities that require across-the-board regulatory solutions.

3. **Addressing the foreign influence threat of online platforms**

Dissemination of disinformation and foreign propaganda are often cited as national security risks related to big online platforms like TikTok. Instead of imposing generalized bans, the EU should enforce its regulations, specifically the Digital Services Act (DSA), to hold platforms accountable for their content moderation practices and to ensure transparency. In the context of DSA enforcement, EU regulators should work together with large online platforms to gain insight into the platforms' content moderation mechanisms, recommendation algorithms, and efforts to combat disinformation.

4. **Addressing the cyber security threat of online platforms**

Cyber security risks, including the transfer of EU citizen data to foreign jurisdictions, should be handled within the framework of the General Data Protection Regulation (GDPR) to ensure that data transfers comply with the regulation's strict safeguards. National data protection authorities, in collaboration with the European Data Protection Board (EDPB) and

the EU Commission, should continue to evaluate and improve enforcement of the GDPR framework for cross-border data sharing with regard to TikTok and other social media.

5. **Secure app usage within government organisations**

All online applications that rely on data harvesting as a business model encompass privacy and security concerns. Both EU and national government bodies should conduct reviews of the applications used by their employees, with a specific focus on those that involve data sharing, communication, and potential security risks. Government entities should establish guidelines for app usage focussing on data protection, encryption, and other security measures necessary to safeguard sensitive government information.

Introduction

Over the past few years, TikTok has become one of the world's biggest social media platforms. Since the app's acquisition by parent company ByteDance (字节跳动), it has grown to over one billion users worldwide.[1] Many have lauded TikTok as the most successful example of an app developed by a Chinese company. However, TikTok's meteoric rise has been overshadowed by allegations of Chinese government influence over the app. For the past three years TikTok has come under attack from the US government, including a ban under the Trump administration by Executive Order, which was later ruled illegal on grounds of freedom of expression.[2] More recently, bipartisan concerns in the US culminated in the widely publicized congressional hearing on TikTok, in which CEO Shou Zi Chew was scrutinized by US lawmakers about potential Chinese influence over the platform.[3] In the EU, concerns about possible data transfer to China have led the main EU institutions, as well as several national parliaments, to ban TikTok on corporate devices.[4] Yet, some experts and politicians in the EU and the US call for more rigorous action, and propose that TikTok should be banned even for individual users.[5]

---

[1] Shou Chew, "Testimony Before the U.S. House Committee on Energy and Commerce," 23 March 2023, https://d1dth6e84htgma.cloudfront.net/Written_Testimony_of_Shou_Chew_c07504eccf_084e8683f3.pdf?updated_at=2023-03-22T03:10:22.760Z.

[2] TikTok v. Trump, 507 F. Supp. 3d 92, 98 (D.D.C. 2020). See Bernard Horowitz & Terence Check, "TikTok v. Trump and the Uncertain Future of National Security-Based Restrictions on Data Trade," *Journal of National Security Law & Policy* 13 (2022): p. 61-111.

[3] House Committee on Energy and Commerce, "Full Committee Hearing: "TikTok: How Congress Can Safeguard American Data Privacy and Protect Children from Online Harms," 23 March 2023, https://energycommerce.house.gov/events/full-committee-hearing-tik-tok-how-congress-can-safeguard-american-data-privacy-and-protect-children-from-online-harms.

[4] "Which countries have banned TikTok and why?," Euronews, 4 April 2023, https://www.euronews.com/next/2023/04/04/which-countries-have-banned-tiktok-cybersecurity-data-privacy-espionage-fears.

[5] Pernille Tranberg, "Should TikTok Be Banned in the EU?," Data Ethics, 12 March 2023, https://dataethics.eu/should-TikTok-be-banned-in-the-eu/. See also Laura Silver & Laura Clancy, "By more than two-to-one, Americans support U.S. government banning TikTok," Pew Research Center, 31 March 2023, https://www.pewresearch.org/short-reads/2023/03/31/by-a-more-than-two-to-one-margin-americans-support-us-government-banning-TikTok/.

While moves to ban TikTok are thus gaining traction worldwide,[6] critics argue that they are based on unsubstantiated concerns rather than specific evidenced incidents regarding the nature of TikTok's threat.[7] Furthermore, legal experts have warned that a complete ban on TikTok would be excessive and run against the principles of a free market and level playing field, as well as fundamental rights such as free speech and freedom of enterprise.[8] Moreover, as critics argue, TikTok's practices are no different than Western apps such as Facebook, Twitter, and Google. Furthermore, the effectiveness of banning TikTok has been called into question, as the Chinese government would be able to obtain the same data gathered by TikTok by making use of Open Source Intelligence (OSINT) tools to track user activities and identities on multiple social media.[9]

Against this background, this policy brief – focusing on the EU context – will consider the merits of a general ban on TikTok as well as possible regulatory alternatives. For this, it first sets out to investigate the risks associated with TikTok. A comprehensive risk assessment will be conducted that analyses the risks posed by TikTok's alleged connection with the CCP in combination with its extensive data collection practices and pervasive algorithms. It finds that, while some concerns are valid, they are not sufficient to warrant a ban on the app in the EU. Therefore, this policy brief also looks at some of the regulatory alternatives which EU regulators can resort to. It is proposed that, rather than banning TikTok, the EU should employ its innovative regulatory framework for the provision of digital services to address the risks identified in the risk assessment.[10] All in all, this policy brief aims to give a systematic overview of the evidence for TikTok's risks regarding political influence and cyber security and show which specific EU legislation might be applied to mitigate those risks.

[6] See Euronews, "Which countries have banned TikTok and why?".

[7] Milton Mueller & Karim Farhat, "TikTok and US national security," Internet Governance Project, n.d., https://www.internetgovernance.org/wp-content/uploads/TikTok-and-US-national-security-3.pdf.

[8] Antonia Hmaidi and Kai von Carnap, "Europe should regulate TikTok, not ban it," Euractiv, 26 April 2023, https://www.euractiv.com/section/platforms/opinion/europe-should-regulate-tiktok-not-ban-it/.

[9] Mueller & Farhat, "TikTok and US national security," p 22.

[10] See also Hmaidi and von Carnap, "Europe should regulate TikTok".

1. TikTok's problem: A risk assessment

Why is TikTok seen as particularly problematic by policymakers and the public? It is not *just* because it is a Chinese app. Other Chinese online platforms like shopping apps Shein and Temu do not receive nearly as much scrutiny. It is also not *just* because of the data harvesting practices that feed TikTok's algorithms. As mentioned above, there are other social media that do the same (Instagram, YouTube, Twitter, Facebook, Google, etc.). It is a combination of these factors, in addition to Chinese legislation[11] that some believe allows the Chinese government unfettered access to the user data of Chinese companies, which gives rise to fears of TikTok being the long arm of the CCP. The concrete risk landscape pertaining to TikTok is therefore seen to relate to:

- (1) TikTok's CCP connection;
- (2) TikTok's perceived cyber security risks;
- (3) Chinese national security legislation.

By conducting a risk assessment based on these factors, a clearer understanding of the potential risks and their implications can be gained. The evidence underlying the risk assessment is obtained primarily from thinktank and government reports that have focused on different aspects of TikTok's security risks.

1.1 TikTok's CCP connection

1.1.1 Company structure

The main argument concerning TikTok's susceptibility to Chinese government influence stems from its ownership by Beijing-headquartered parent company ByteDance.[12] Yet, considering the globalized origins and ownership structure of the latter company, it would be too simple to label it as a mere extension of the Chinese state. ByteDance, founded in a Beijing apartment in 2012 and incorporated in the Cayman Islands to attract foreign

[11] This includes, e.g., the National Intelligence Law of 2017. See section2.3. of this policy brief.

[12] See, e.g., Rachel Lee et al., "TikTok, ByteDance, and their ties to the Chinese Communist Party," Submission to the [Australian] Senate Select Committee on Foreign Interference through Social Media, 14 March 2023, https://www.scribd.com/document/633015202/TikTok-ByteDance-And-Their-Ties-to-the-Chinese-Communist-Party.

investment, has been described as "the product of Chinese computer entrepreneurs, Western capital and a globalized internet".[13] Its investors today are "global institutional funds and venture capital firms like KKR, Sequoia Capital, and Softbank, as well as other corporate entities like Morgan Stanley, Goldman Sachs Group, Weibo, and others", and aside from ByteDance founder and CEO Rubo Liang, its governing board consists of three Western investors and one Hong Kong investor:[14] ByteDance was conceived and developed to be a global company.[15] Researchers in a submission to the Australian Senate Select Committee on Foreign Interference through Social Media have visualised TikTok's company structure:

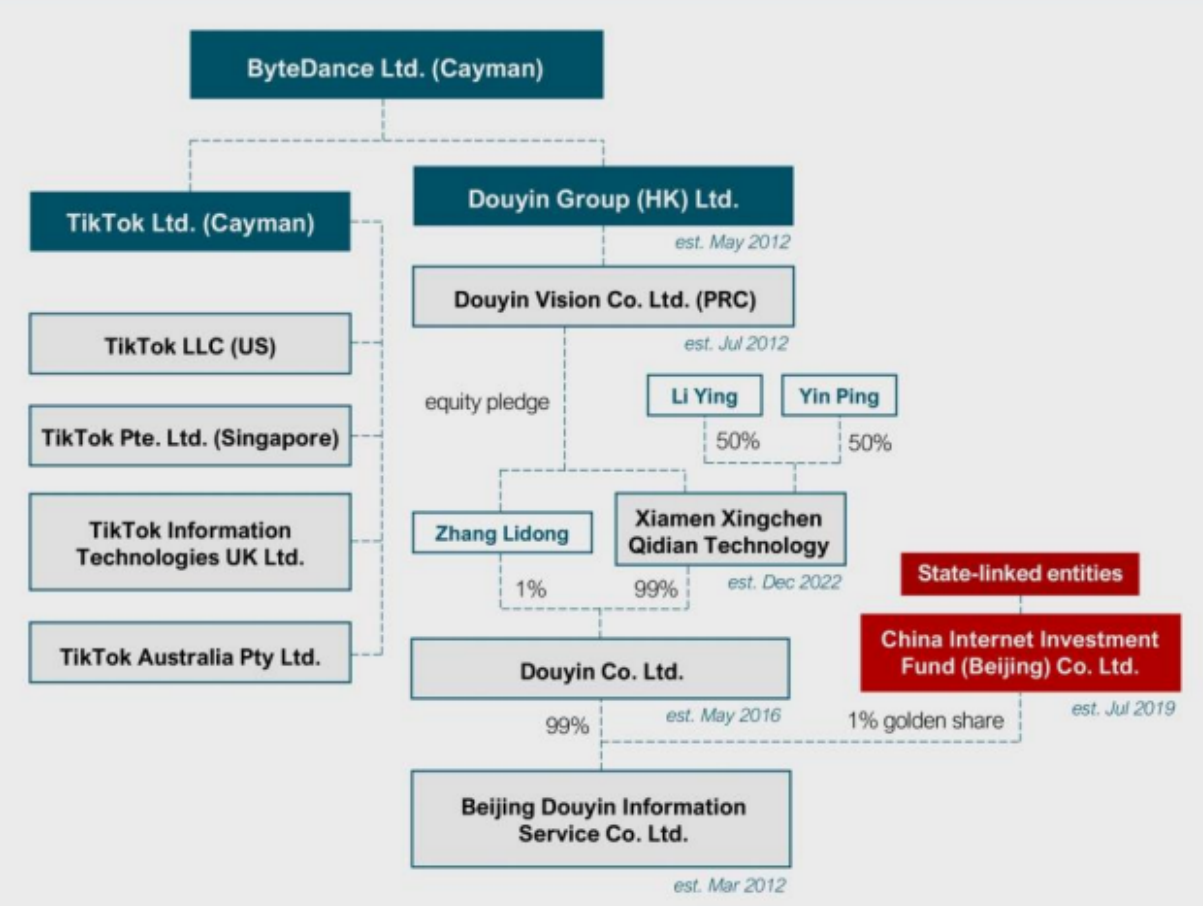


Figure 1 Source: Lee et al., "TikTok, ByteDance," p. 39.

[13] Mueller & Farhat, "TikTok and US national security," p. 7.

[14] Mueller & Farhat, "TikTok and US national security," p. 8.

[15] Mueller & Farhat, "TikTok and US national security," p. 9.

Nevertheless, although TikTok CEO Shou Zi Chew has stressed that "ByteDance is not owned or controlled by the Chinese government",[16] there are several ways in which China's ruling party can exert control over the company. Like many companies, regardless of their ownership, located in China, ByteDance has Party-cells installed.[17] The first Party-cell within ByteDance was established in October 2014. In April 2017 a ByteDance Party committee was established, with cells within ByteDance's Public Affairs Department, Technical Support Unit and Compliance Operations Unit.[18] Several high-ranking ByteDance officials are incorporated within the company's CCP structures. An example is ByteDance Party Secretary and Chief Editor Zhang Fuping, who has declared that ByteDance should "transmit the correct political direction, public opinion guidance and value orientation into every business and product line [and] use values to guide algorithms."[19] While it is very difficult to assess how influential those Party-cells are to the company's operations and decision-making,[20] existing studies show that Party work within companies mainly involves management of the staff, rather than influencing how business should be run.[21]

Furthermore, TikTok has come under scrutiny for Chinese government involvement in its Chinese sister app Douyin (抖音), of which an investment fund backed by the Cyberspace Administration of China (CAC) owns a 1% "golden share".[22] It should be emphasized, however, that TikTok and Douyin are separate companies and apps and operate in different

[16] Shou Chew, "Testimony," unpaginated.

[17] See also Article 30 of the Constitution of the Chinese Communist Party [*zhōng guó gòng chǎn dǎng zhāng chéng* 中国共产党章程], which lays down as a rule that all enterprises that employ three or more Party members need to install a Party cell within the enterprise.

[18] Fergus Ryan, Audrey Fritz and Daria Impiombato, "TikTok and WeChat. Curating global information flows," ASPI Policy Brief Report No. 37/2020, September 2020, https://ad-aspi.s3.ap-southeast-2.amazonaws.com/2020-09/TikTok%20and%20WeChat.pdf?VersionId=7BNJWaoHImPVE.6KKcBP1JRD5fRnAVTZ, p. 49.

[19] Lee et al., "TikTok, ByteDance," p. 58.

[20] See Nis Grünberg and Katja Drinhausen, "The Party leads on everything. China's changing governance in Xi Jinping's new era," MERICS, 24 September 2019, https://merics.org/en/report/party-leads-everything.

[21] Frank Pieke, "The Chinese Communist Party as a Global Force," *Journal of Current Chinese Affairs* 51, no. 3 (2022): p. 456–475.

[22] Lee et al., "TikTok, ByteDance," p. 13. Under the golden share structure, the Chinese government is granted decisive voting rights or veto power over certain business decisions. See Laura He, "China still wants to control Big Tech. It's just pulling different strings," CNN, 27 January 2023, https://edition.cnn.com/2023/01/27/tech/china-golden-shares-tech-regulatory-control-intl-hnk/index.html.

markets: "TikTok is not under the management control of the Douyin subsidiary, and the Douyin subsidiary has no ownership, visibility or input into TikTok."[23] Indeed, TikTok itself is banned within China. Although the apps share similar algorithms developed by ByteDance in Beijing, their content is segregated and cannot be accessed across platforms.[24]

1.1.2 TikTok's content moderation and recommendation

In terms of TikTok's approach to content moderation, multiple reports have found no strong evidence for censorship favouring the Chinese government on TikTok. Indeed, while Chinese sister app Douyin restricts certain politically sensitive terms in its search results, TikTok did not label any of 5,420 search results as sensitive that have been previously found censored on WeChat.[25] In fact, videos on sensitive topics in China such as Taiwan independence, Falun Gong, exploitation or oppression of Uyghurs in Xinjiang Region, ridicule of China's President Xi Jinping, etc. can all easily be accessed and are widely shared.[26] It is true that in the past TikTok has barred content about politically sensitive events, figures, and speech to keep the platform less divisive – a policy that TikTok abandoned because of its unpopularity with users months before it received media attention.[27] TikTok still restricts politically sensitive terms in certain languages in compliance with local laws, such as "Putin Is A Thief" in Russian or "gay" in Arabic.[28] However, the same charge could be laid against platforms like Twitter, which complies with censorship from the ruling parties in countries such as Turkey and India.[29] In any case, it is hard to

[23] Mueller & Farhat, "TikTok and US national security," p. 10.

[24] Mueller & Farhat, "TikTok and US national security," p. 12. See also "TikTok's secret sauce," Protocol, 15 December 2022, https://www.protocol.com/newsletters/sourcecode/two-sides-same-code?rebelltitem=1#toggle-gdpr.

[25] Pellaeon Lin, "TikTok vs Douyin. A Security and Privacy Analysis," CitizenLab, 22 March 2021, https://citizenlab.ca/2021/03/TikTok-vs-douyin-security-privacy-analysis/.

[26] Mueller & Farhat, "TikTok and US national security," p. 12.

[27] Mueller & Farhat, "TikTok and US national security," p. 16. See also Ryan, Fritz & Impiombato, "TikTok and Wechat," p. 4.

[28] Ryan, Fritz & Impiombato, "TikTok and Wechat," p. 5. Some terms were restricted because they were primarily used to look up pornographic content.

[29] "Under Elon Musk, Twitter has approved 83% of censorship requests by authoritarian governments", El Pais, 24 May 2023, https://english.elpais.com/international/2023-05-24/under-elon-musk-twitter-has-approved-83-of-censorship-requests-by-authoritarian-governments.html.

conceive how this form of localised censorship could be mandated by the Chinese government.

There are also fears that China could use TikTok, especially its recommendation algorithm, to push disinformation and CCP propaganda in order to shape public opinion. This threat also is not unique to TikTok. For example, the Mueller report has highlighted Russia's use of American social media to influence sentiment leading up to the 2016 US elections.[30] And, while some reports on TikTok have shown the presence of pro-CCP content and misinformation on the platform and warned about the app's capabilities to influence the political opinions of its users, none have presented decisive evidence revealing TikTok as a "Chinese government-controlled influence operation".[31] On the contrary, researchers have found that TikTok has become more transparent in its content moderation.[32] For example, it is publishing regular transparency reports. Importantly, in its report for 2022, TikTok claims to have countered five covert foreign influence operations, including a Russian influence network and a network of unspecified origin "targeting civic discourse in Taiwan."[33] Recently, TikTok removed 284 accounts linked to a Chinese disinformation network, following a report by Guardian Australia on the influence campaign. To summarize, concerning the transmission of foreign propaganda, TikTok seems to pose no unique threat compared to other social media.

1.2 TikTok's cyber security risks

Related to concerns regarding TikTok's connection to the Chinese government are concerns about its data collection practices, resulting in risks to cyber security. The cyber security argument has been articulated as follows: (1) TikTok collects excessive amounts of user data

[30] Robert Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election", Vol. I, 19 June 2020, https://www.courtlistener.com/recap/gov.uscourts.dcd.205521/gov.uscourts.dcd.205521.122.1.pdf.

[31] Mueller & Farhat, "TikTok and US national security," p. 12.

[32] Mueller & Farhat, "TikTok and US national security," p. 15.

[33] "Community Guidelines Enforcement Report," TikTok, 1 July 2022 – 30 September 2022, Published 19 December 2022, https://www.tiktok.com/transparency/en/community-guidelines-enforcement-2022-3/.

that (2) could be accessed by the Chinese government, which (3) could leverage this data to its advantage.[34] These assumptions will be discussed here.

1.2.1 TikTok collects excessive amounts of user data

There appears to be truth in the argument that TikTok engages in data harvesting practices by gathering excessive amounts of user data. Indeed, TikTok does not prioritise privacy. The app's permissions and device information collection are "overly intrusive and not necessary for the application to function."[35] TikTok has access to data like device information, contacts, the calendar, the location, and gathers all applications that are installed on the phone (device mapping).[36] However, TikTok's collection of user data is not more pervasive than other online platforms, including Meta, Google, and Twitter. First of all, an analysis of the privacy policies regarding the collection of user data points such as date of birth, password, phone number, email address, etc. by TikTok compared to Meta, Google, and Twitter found that, while TikTok collects more data points than Twitter, it collects less than Meta and Google.[37] Second, when it comes to the use of online tracking through so-called "pixels" installed on third-party websites, the number of TikTok trackers "[is] just a fraction of those … observed from Google and Meta."[38] Third, while TikTok does ask for a substantial number of user permissions related to various device capabilities, including camera access, the extent of these requests is comparable to what is commonly seen among similar social media platforms (figure 2). Lastly, compared to its sister app Douyin, "Douyin contains features that raise privacy and security concerns" while TikTok "does not contain these features".[39]

---

[34] Cf. Mueller & Farhat, "TikTok and US national security," p. 18.

[35] Internet 2.0, "TikTok's excessive data harvesting program," Center for Foreign Interference Research, 17 July 2021, https://www.foreigninterference.org/TikTok-excessive-data-harvesting-program.

[36] Internet 2.0, "Tiktok's data harvesting," unpaginated.

[37] Nigel Phair, "Entertainment in the Digital Age – An investigation into data leakage and privacy concerns of digital platforms," April 2023, https://drive.google.com/file/d/1tEkMVmYkOWOdCgYpX3wpPohZAA3mItrY/view.

[38] Tranberg, "Should TikTok Be Banned?"; Thomas Germain, "How TikTok Tracks You Across the Web, Even If You Don't Use the App," Consumer Reports, 29 September 2022, https://www.consumerreports.org/electronics-computers/privacy/TikTok-tracks-you-across-the-web-even-if-you-dont-use-app-a4383537813/.

[39] Idem.

All in all, most experts conclude that the app still falls within general industry norms for user data collection.[40]

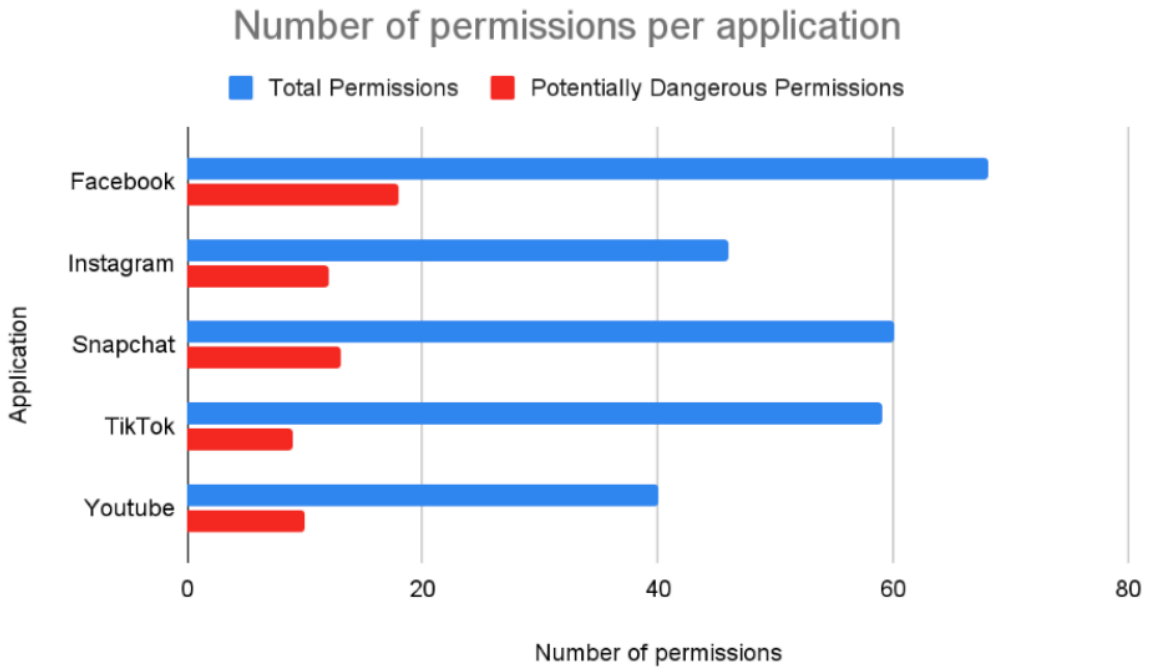


Figure 2 Source: Nigel Phair, "Entertainment in the Digital Age", p. 4.

1.2.2 TikTok's data can be accessed by the Chinese government

Concerns that user data collected by TikTok might be accessed from China by virtue of its status as Chinese-owned subsidiary are also not entirely unfounded. TikTok has confirmed that user data of two American journalists was inappropriately obtained by employees of parent company ByteDance who were investigating potential employee leaks to the press. An examination by an outside law firm followed, which led to the firing of the employees involved in obtaining the journalists' information.[41] While TikTok has stated that a US-based security team decides who can access data from China, the incident has increased fears that user data could fall in the hands of the Chinese government. Evidence of the Chinese

[40] Lin, "TikTok vs Douyin," unpaginated.

[41] Lee et al., "TikTok, ByteDance,"; "EXCLUSIVE: TikTok Spied on Forbes Journalists," Forbes, 22-Dec-2022, https://www.forbes.com/sites/emilybaker-white/2022/12/22/tiktok-tracks-forbes-journalistsbytedance/?sh=5aebf8af7da5.

government accessing TikTok data vicariously through ByteDance has however not been presented in any of the reports consulted for this research.[42] In addition, in order to further dispel such concerns, TikTok is working to store data of American users in the US on servers run by the tech firm Oracle and "creating a secure enclave for European TikTok user data" (see also section 3.2 below).[43]

1.2.3 The Chinese government could use TikTok's data to its advantage

A more fundamental question that by comparison receives less attention is what value the data collected by TikTok holds for the Chinese government. There are two aspects to this debate. First, user data of TikTok could be used for intelligence gathering or surveillance operations that target individuals. The fact that data from specific US journalists has previously been accessed by ByteDance employees from China adds to such concerns. The primary argument against this risk is that China does not need TikTok to conduct online surveillance of individuals. Anyone with a presence on *any* social media is potentially at risk of having social media data analysed by foreign intelligence agencies, for example through the use of powerful Open Source Intelligence (OSINT) tools.[44] Even without cooperation of the operator, a host of information on a social media app's user can be gathered in this way.[45] Additionally, tools like Sherlock can be employed to analyse the presence of a social media user across different applications. Individuals who might be of interest to foreign intelligence agencies should always be careful about which information they share with – and on – social media, and should not install apps on their work phones that collect excessive amounts of data like TikTok or Facebook, Twitter, Instagram etc.

Second, some argue that having access to TikTok's aggregate user data could enable Chinese intelligence services to conduct mass surveillance in order to "understand how people are

[42] Tranberg, "Should TikTok Be Banned?," unpaginated.

[43] Theo Bertram, "Setting a new standard in European data security with Project Clover," TikTok, 8 March 2023, https://newsroom.tiktok.com/en-eu/setting-a-new-standard-in-european-data-security-with-project-clover.

[44] Mueller & Farhat, "TikTok and US national security," p. 2.

[45] For example, one report describes how detailed analytics can be accessed through proxy setups that allow third parties to observe the traffic between the app and the service provider. See BTF_117, "TikTok OSINT: targeted user investigation (Part 1/3: User)," Medium, 19 April 2020, https://medium.com/@BTF117/tiktok-osint-targeted-user-investigation-9e206f8bb794.

influenced and how they think".[46] It is true that social media data can be analysed to provide insights into user behaviour, which is why many social scientists have, for example, made use of Twitter's application programming interface (API) to study political polarisation and the spread of misinformation. However, even if the Chinese government would be able to access TikTok's aggregate user data or that of other social media, whether through their APIs or other means such as buying user data from third-party data brokers, the exact nature of the resulting national security threat remains unclear. In this regard, TikTok is an unlikely target for cyber-espionage operations compared to other notable operations (Marriott Hotel breach, OPM, Equifax) that provided Chinese intelligence with large collections of valuable, sensitive information such as records of US Federal employees and contractors, credit card and social security numbers, and fingerprints.[47] In contrast, experts consider the personal user data of social media users to be more valuable to China "as a target of advertising than as a target of espionage".[48]

1.3 Chinese legislation

Finally, there are concerns that China could make use of the broad prescriptions in its extensive national security laws to demand user data from ByteDance, as it falls under Chinese jurisdiction, having its headquarters in Beijing. In this regard, Article 7 of China's National Intelligence Law (NIL) is often cited, which reads: "All organizations and citizens shall support, assist, and cooperate with national intelligence efforts in accordance with law, and shall protect national intelligence work secrets they are aware of."[49] Article 14 gives China's national intelligence services the authority to "request that relevant organs, organizations, and citizens provide necessary support, assistance, and cooperation."[50]

[46] See Paul Charon & Jean-Baptiste Jeangène Vilmer, "Chinese Influence Operations. A Machiavellian Moment," Institute for Strategic Research, October 2021, https://www.irsem.fr/report.html.

[47] Mueller & Farhat, "TikTok and US national security," p. 19.

[48] Chi Yin & Tonghui Zhu, "Why China's strong data privacy laws should reassure TikTok, ByteDance sceptics," SCMP, 18 April 2023, https://www.scmp.com/comment/opinion/article/3217079/why-chinas-strong-data-privacy-laws-should-reassure-tiktok-bytedance-sceptics.

[49] "PRC National Intelligence Law (as amended in 2018)," China Law Translate, 27 June 2017 [original post], https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/. See also Murray Scot Tanner, "Beijing's New National Intelligence Law: From Defense to Offense," Lawfare Blog, 20 July 2017, https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense.

[50] See "PRC National Intelligence Law".

Analysts have warned that the NIL may be used to force ByteDance to circumvent or undermine ongoing efforts of TikTok to move its user data outside of China. Nonetheless, no evidence has been shown that the Chinese government has in fact used the NIL *vis-à-vis* ByteDance to obtain data from TikTok. In this regard, TikTok's CEO has stated with regard to the data of US citizens that "TikTok has never shared, or received a request to share, U.S. user data with the Chinese government. Nor would TikTok honour such a request if one were ever made."[51]

Analysts who point out the dangers of the NIL and the powers that it gives the Chinese government also fail to point out the significant progress that is being made in China in the field of data protection legislation. This includes the adoption of a comprehensive Personal Information Protection Law which entered into force on 1 November 2021.[52] The law is modelled after the EU General Data Protection Regulation (GDPR) and includes similar rights and enforcement mechanisms. While critics argue that black letter law does little to control the behaviour of the Chinese state, there have been cases of local prosecutors in China who brought public interest litigation "against local government agencies for direct infringement of personal data or to request them to enforce laws in the private sector."[53] In addition, China's top court and prosecuting body have cracked down on businesses "for illegally harvesting and transferring personal data in social media accounts".[54] ByteDance is subject to China's stringent data protection framework, and it should not *a priori* be dismissed that the company might face enforcement action from the Chinese authorities if it were to inappropriately handle data obtained from TikTok.

1.4 Conclusion: TikTok's risks

[51] Shou Chew, "Testimony". See also "Information Requests Report," Tiktok, 1 July 2022 – 31 December 2022 Published 15 May 2023, https://www.TikTok.com/transparency/en/information-requests-2022-2/.

[52] Julia Zhu, "The Personal Information Protection Law: China's Version of the GDPR?," Columbia Journal of Transnational Law, 14 February 2022, https://www.jtl.columbia.edu/bulletin-blog/the-personal-information-protection-law-chinas-version-of-the-gdpr.

[53] Yin & Zhu, "China's strong data privacy laws".

[54] Idem. See Dorwart, Hunter. "Chinese Data Protection in Transition: A Look at Enforceability of Rights and the Role of Courts." In *Data Protection and Privacy, Volume 15: In Transitional Times*, edited by Hideyuki Matsumi, Dara Hallinan, Diana Dimitrova, Eleni Kosta and Paul De Hert, 43–74. Computers, Privacy and Data Protection. Oxford: Hart Publishing, 2023. Accessed June 16, 2023. http://dx.doi.org/10.5040/9781509965939.ch-003.

The risk assessment above has found that, while there are some valid concerns regarding the CCP's influence over TikTok's parent company ByteDance, claims that TikTok should be seen as the long arm of the Chinese state are unfounded – at least, no evidence to this effect has been presented in the reports on TikTok studied for this policy brief. Nevertheless, there are some challenges that TikTok provides for EU regulators. These concern the presence of Chinese (and other) disinformation and propaganda on the platform (political influence/interference risks) as well as the transfer of EU citizen data to a foreign country, namely China (cyber security risks). Considering the foregoing, the following matrix may be presented to summarize TikTok's perceived risks, in so far as they spring from its "Chineseness":

	Political influence/interference threat	**Cyber security threat**
Risks:	Foreign propaganda/censorship to exercise narrative control and influence public opinion	Extraction of user data for purposes of foreign intelligence gathering and surveillance
Means:	Content moderation and recommendation algorithms to censor or push certain content; inauthentic accounts	Transfer of data to foreign countries; access to data via foreign-headquartered (parent) companies

As none of these challenges are unique to TikTok, however, an actor-agnostic approach is needed. Singling out one company as a target for an all-out ban because it is seen to have a connection to a specific country would undermine the values and freedoms that underlie the EU economic constitution. Furthermore, the next paragraph will show that two EU legislative measures are currently in place to deal with the concerns related to TikTok without necessitating a ban on the app: The Digital Services Act (DSA) and the GDPR. They should be enforced to deal with the two key risk categories described above, thus supplementing the matrix as follows:

	Political influence/interference threat	**Cyber security threat**
Solution:	DSA enforcement	GDPR enforcement

2. The EU solution

2.1 Enforcing the DSA

As explained above, the fear of TikTok being a "Chinese influence operation" primarily relates to its content moderation and recommendation algorithms. In this regard, the new EU Digital Services Act[55] introduces new EU-wide standards for providers of digital service providers, including legally binding rules on requirements and procedures for content moderation and transparency duties concerning content moderation and recommendation.[56] These rules are specifically designed to ensure more "diligent and trustworthy content moderation, less illegal content and less disinformation online."[57] A key element of the DSA is that it poses obligations on the largest platforms to rein in potential risks to society, including "negative effects on fundamental rights, civic discourse and elections, gender-based violence, and public health." [58] Platforms are also obliged to "adapt their recommender system to prevent algorithmic amplification of disinformation", as well as conducting annual risk assessments of their services.[59]

While DSA in principle will apply from 17 February 2024, several provisions containing obligations for the largest platforms and search engines have applied since its entry into force on 16 November 2022. A Very Large Online Platform (VLOP) or Very Large Online Search Engine (VLOSE) has to comply with DSA obligations four months after being designated as such by the EU Commission. On 25 April 2023, the EU Commission designated 19 companies as VLOP or VLOSE, which means that they should make sure to

[55] European Parliament legislative resolution of 5 July 2022 on the proposal for a regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC (COM(2020)0825 – C9-0418/2020 – 2020/0361(COD)). https://www.europarl.europa.eu/doceo/document/TA-9-2022-0269_EN.html.

[56] Philipp Koehler, Gregor Schmid, "Overview on the Digital Services Act (DSA)," Taylor Wessing, 29 November 2022, https://www.taylorwessing.com/en/insights-and-events/insights/2022/11/overview-on-the-digital-services-act-dsa.

[57] "More responsibility, less opacity: what it means to be a "Very Large Online Platform", EU Commission, 25 April 2023, https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_23_2452.

[58] John Albert, "A guide to the Digital Services Act, the EU's new law to rein in Big Tech," Algorithm Watch, 21 September 2021, https://algorithmwatch.org/en/dsa-explained/.

[59] "More responsibility, less opacity".

comply with the DSA's special obligations from 25 August 2023. These are all companies that have more than 45 million monthly active users in the EU, including e.g. TikTok, Twitter, Facebook, Wikipedia, and Google Search.[60]

TikTok itself has said it welcomes the EU DSA, and is taking steps to work towards DSA compliance. As mentioned earlier, the company is regularly publishing transparency reports about its enforcement of community guidelines (including the removal of covert influence operations), compliance with government removal requests, IP removal requests, and law enforcement requests for user information.[61] It has also established a European Transparency and Accountability Centre "to provide experts with an opportunity to see first-hand how we secure our community's safety, data, and privacy", as well as a European Safety Advisory Council.[62] In August, TikTok rolled out a number of major changes to its ad products in order to comply with DSA requirements. Nonetheless, a stress test conducted in August by the EU Commission to examine TikTok's readiness to comply with DSA requirements found that there are still steps the company needs to take towards full compliance.[63]

It thus remains to be seen whether TikTok will be able to ensure timely and full compliance with the strict rules of the DSA. In order to test their compliance, VLOPs and VLOSEs are subject to yearly independent audits that produce a report with a "positive opinion" or "negative opinion" concerning the company's DSA compliance.[64] They can also be expected to face "rigorous supervision" from the EU Commission, which is exclusively competent for enforcing the DSA *vis-à-vis* VLOPs and VLOSEs.[65] To this end, the EU Commission has especially set up a European Centre for Algorithmic Transparency (ECAT), which will provide the Commission "with in-house technical and scientific expertise to ensure that algorithmic systems used by the Very Large Online Platforms and Very Large Online Search

[60] "More responsibility, less opacity".

[61] "Reports," TikTok, n.d., https://www.tiktok.com/transparency/en/reports/.

[62] Caroline Greer, "TikTok calls for the EU's Digital Services Act to support innovative transparency and accountability initiatives", TikTok, 21 June 2021, https://newsroom.TikTok.com/en-eu/TikTok-calls-for-digital-services-act-to-support-innovative-transparency-initiatives.

[63] Brian Fung, "TikTok 'stress test' shows it's not 'fully ready' for looming EU social media rules, commissioner says," CNN, 19 July 2023, https://edition.cnn.com/2023/07/19/tech/tiktok-eu-stress-test/index.html.

[64] Recital 93 DSA.

[65] "More responsibility, less opacity".

Engines comply with the risk management, mitigation and transparency requirements in the DSA."[66] If compliance of a company is found to be insufficient, the Commission may impose fines "of up to 6% of [its] group's global turnover and, as last resort, a temporary ban from the EU in case of repeated serious breaches threatening to the life or safety of persons."[67]

2.2 Enforcing the GDPR

European critics of TikTok's data transfer to China point to TikTok's privacy policy update from 2 November 2022 in which it named China as one of the countries where EU user data can be remotely accessed. The policy states that "we allow certain employees within our corporate group located in Brazil, Canada, China, Israel, Japan, Malaysia, Philippines, Singapore, South Korea, and the United States remote access to TikTok European user data."[68] Some see this as a confirmation of the ability to access EU user data by ByteDance employees subject to China's security laws. However, such fears should be placed within the context of the stringent legal constraints that TikTok is already obligated to observe under the GDPR when it comes to international data transfer.

The GDPR puts strict limitations on the conditions under which the online data of EU users can be transferred to countries outside of the European Economic Area.[69] While data may freely be transferred to certain countries that the EU Commission deems to ensure an adequate level of personal data protection ("adequate countries"), most countries – such as China but also e.g. the US – are not designated as adequate countries. If a company wants to transfer EU user data to a non-adequate country, pursuant to Article 46 GDPR, personal data may only be transferred "if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available."

---

[66] "DSA enforcement: Commission launches European Centre for Algorithmic Transparency," EU Commission, 17 April 2023, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2186.

[67] "More responsibility, less opacity".

[68] Elaine Fox, "Sharing an update to our privacy policy," TikTok, 2 November 2022, https://newsroom.TikTok.com/en-gb/an-update-to-our-privacy-policy.

[69] Maria Avramidou, "Transferring personal data outside the EU … Some key lessons from the EDPB's draft guidelines," KU Leuven Centre for IT & IP Law, 25 January 2022, https://www.law.kuleuven.be/citip/blog/transferring-personal-data-outside-the-eu/.

One of the ways to provide adequate safeguards is to implement "standard data protection clauses adopted by the Commission" (Article 46(2)(c) GDPR). According to TikTok's privacy policy, it relies on such standard contractual clauses (SCCs) to transfer data to China.[70] The latest SCCs adopted by the EU Commission in 2021, in response to the European Court of Justice's *Schrems II*[71] judgment, have been updated to deal specifically with a situation where the legal system of the recipient country of the EU user data (in this case the US) has shortcomings that impede the protection of personal data and violate the GDPR.[72] The new SCCs came with a toolbox, including "an overview of the different steps companies have to take to comply with the *Schrems II* judgment as well as examples of possible 'supplementary measures', such as encryption, that companies may take if necessary."[73]

Relying on the GDPR's SCCs for international data transfer, however, might not be enough. This becomes apparent from a recent 22 May 2023 decision of Ireland's Data Protection Commission (DPC) that handed a record fine to Facebook for transferring EU user data to the US, even though Facebook employed SCCs. Accordingly, TikTok has also announced that it is working on a plan, nicknamed "Project Clover", to store its data locally in the EU – an effort mirroring its "Project Texas" in the US.[74] The plan is based on data localisation of EU users by storing user data on servers in Europe, as well as extensive auditing by a European security company with regard to "cybersecurity and data protection controls."[75] To store data locally, TikTok is investing €1,2 billion yearly in two data centres in Dublin and one in Hamar region in Norway, operated by third party service providers.

---

[70] "Privacy Policy," TikTok, last updated 4 May 2023, https://www.tiktok.com/legal/page/eea/privacy-policy/en.

[71] CJEU, judgment of 16 July 2020, case C-311/18, *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems*. See Róisín Áine Costello, "Schrems II: Everything Is Illuminated?," European Papers, 15 October 2020, https://www.europeanpapers.eu/en/europeanforum/schrems-II-everything-is-illuminated.

[72] See also "Schrems II," GDPR Summary, 23 November 2020, https://www.gdprsummary.com/schrems-ii/.

[73] "European Commission adopts new tools for safe exchanges of personal data," EU Commission, 4 June 2021, https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847.

[74] "Setting a new standard in European data security with Project Clover," TikTok, 8 March 2023, https://newsroom.tiktok.com/en-ie/project-clover-ireland.

[75] Clothilde Goujard & Laura Kayali, "TikTok launches 'Project Clover' charm offensive to fend off European bans," POLITICO, 8 March 2023, https://www.politico.eu/article/TikTok-pitches-data-security-plan-to-fend-off-european-bans/.

If there are still concerns that data transfers to China are not taking place in compliance with the GDPR and the safeguards provided by SCCs, it is up to EU regulators to enforce compliance. In fact, the Irish DPC, which has jurisdiction over TikTok's operations in the EU, has already launched a probe into TikTok data transfers to China "looking to see if the company meets requirements set out in the regulation covering personal data transfers to third countries".[76] In a recent hearing of the EU Parliament's LIBE Committee, Irish data protection commissioner Helen Dixon stated that a final decision regarding the decision on TikTok's data transfer to China will be made this year.[77] Related to this is a probe of the DPC into the potential mishandling of the user data of children, which is set to result in a potentially hefty fine to be imposed by the DPC, following a recent decision by the European Data Protection Board under the mechanism of Article 65 GDPR.[78]

[76] Natasha Lomas, "Ireland probes TikTok's handling of kids' data and transfers to China," TechCrunch, 15 September 2021, https://techcrunch.com/2021/09/15/ireland-probes-TikToks-handling-of-kids-data-and-transfers-to-china/.

[77] Akshaya Asokan, "EU Committee Probes TikTok, UK's Updated GDPR," Bank Info Security, 23 May 2023, https://www.bankinfosecurity.com/eu-committee-probes-tiktok-uks-updated-gdpr-a-22150.

[78] "Ireland's DPC refers TikTok investigation to EDPB," International Association of Privacy Professionals, 19 May 2023, https://iapp.org/news/a/irelands-dpc-refers-TikTok-investigation-to-edpb-in-dispute-resolution-mechanism/. Clothilde Goujard, "TikTok to face European privacy fine by September," POLITICO, 4 August 2023, https://www.politico.eu/article/tiktok-to-face-european-privacy-fine-by-september/.

3. Conclusion

TikTok has become an archetypical example of Chinese digital companies going global. Its connection to China, however, has led to unprecedented scrutiny over the company's policies regarding data collection and privacy, content moderation, and recommendation algorithms – especially in the US, but also increasingly in Europe. This policy brief has taken a closer look at the concrete risks posed by the app, specifically its alleged CCP connection, its perceived cyber security risks, and the subjection of its parent company to Chinese security legislation. Drawing from several earlier reports into TikTok's alleged China connection, this policy brief has found that none of these risks have been sufficiently substantiated to warrant an all-out ban that some EU policy makers and security analysts argue for. In addition, none of the risks that critics ascribe to TikTok are unique to the company. Singling out one company because of its national origins would be discriminatory and go against the principle of fair competition. Instead, this policy brief recommends that the EU should apply its existing stringent regulatory framework for data services, which provides solutions for all of the concerns raised with regard to TikTok. In this regard, it is encouraging to see that the Irish Data Protection Commission is probing TikTok's GDPR compliance concerning data transfers to China, and the EU Commission is taking the necessary steps to enforce the new DSA rules on content moderation and recommendation against TikTok and other major digital service providers. In conclusion, rather than resorting to a blanket ban, the European Union can navigate the TikTok dilemma by leveraging targeted regulations that uphold fundamental rights while effectively mitigating potential risks.