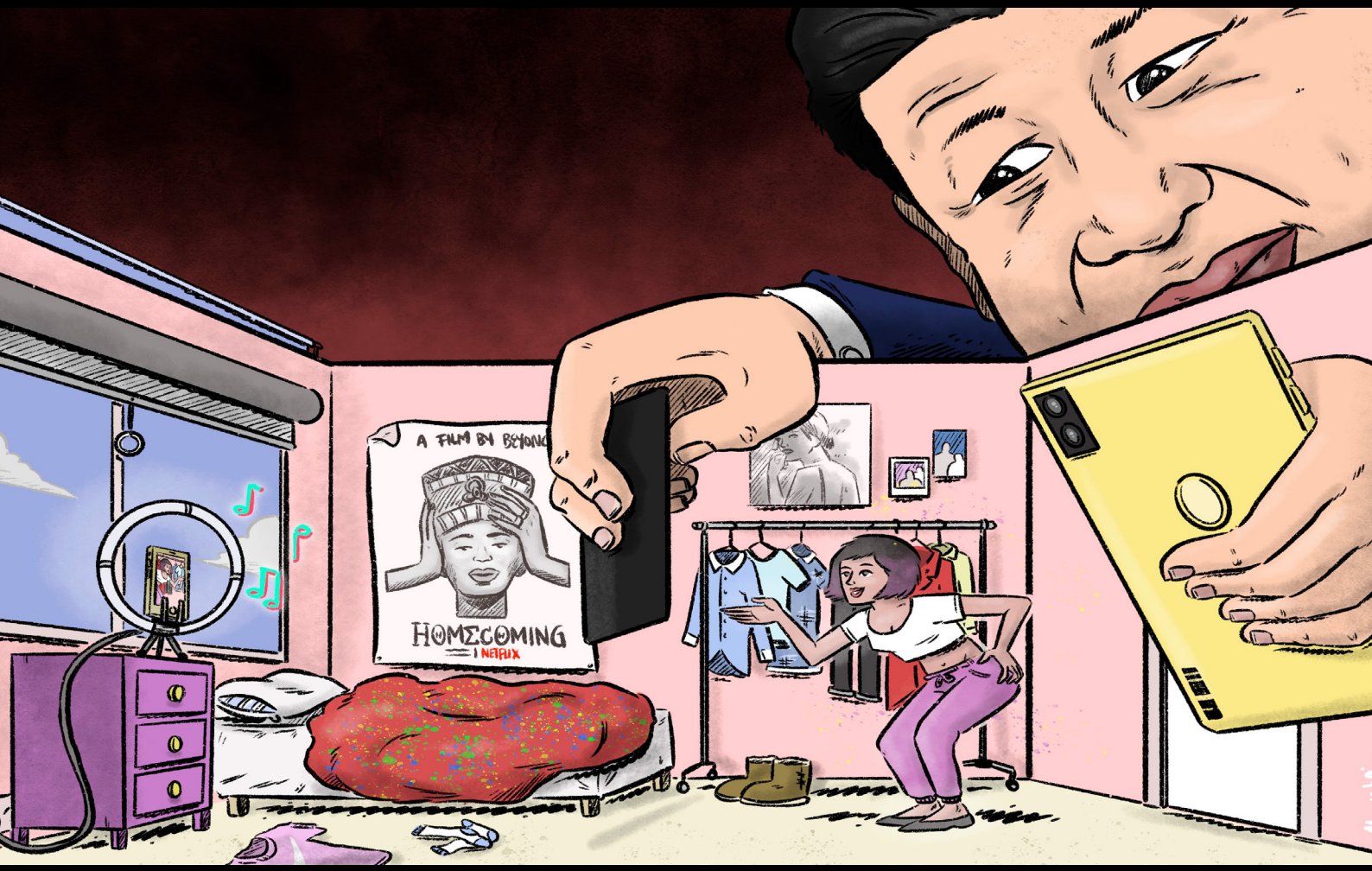
TikTok and WeChat

Curating and controlling global information flows

Fergus Ryan, Audrey Fritz and Daria Impiombato



ASPI AUSTRALIAN STRATEGIC POLICY INSTITUTE
INTERNATIONAL CYBER POLICY CENTRE

Policy Brief
Report No. 37/2020

About the authors

Fergus Ryan is an Analyst working with the International Cyber Policy Centre at ASPI.

Audrey Fritz is a Researcher working with the International Cyber Policy Centre at ASPI.

Daria Impiombato is an Intern working with the International Cyber Policy Centre at ASPI.

Acknowledgements

We would like to thank Danielle Cave and Fergus Hanson for their work on this project. We would also like to thank Michael Shoebridge, Dr Samantha Hoffman, Jordan Schneider, Elliott Zaagman and Greg Walton for their feedback on this report as well as Ed Moore for his invaluable help and advice. We would also like to thank anonymous technically-focused peer reviewers.

This project began in 2019 and in early 2020 ASPI was awarded a research grant from the US State Department for US$250k, which was used towards this report. The work of ICPC would not be possible without the financial support of our partners and sponsors across governments, industry and civil society.

What is ASPI?

The Australian Strategic Policy Institute was formed in 2001 as an independent, non-partisan think tank. Its core aim is to provide the Australian Government with fresh ideas on Australia's defence, security and strategic policy choices. ASPI is responsible for informing the public on a range of strategic issues, generating new thinking for government and harnessing strategic thinking internationally. ASPI's sources of funding are identified in our Annual Report, online at www.aspi.org.au and in the acknowledgements section of individual publications. ASPI remains independent in the content of the research and in all editorial judgements.

ASPI International Cyber Policy Centre

ASPI's International Cyber Policy Centre (ICPC) is a leading voice in global debates on cyber, emerging and critical technologies, issues related to information and foreign interference and focuses on the impact these issues have on broader strategic policy. The centre has a growing mixture of expertise and skills with teams of researchers who concentrate on policy, technical analysis, information operations and disinformation, critical and emerging technologies, cyber capacity building, satellite analysis, surveillance and China-related issues.

The ICPC informs public debate in the Indo-Pacific region and supports public policy development by producing original, empirical, data-driven research. The ICPC enriches regional debates by collaborating with research institutes from around the world and by bringing leading global experts to Australia, including through fellowships. To develop capability in Australia and across the Indo-Pacific region, the ICPC has a capacity building team that conducts workshops, training programs and large-scale exercises for the public and private sectors.

We would like to thank all of those who support and contribute to the ICPC with their time, intellect and passion for the topics we work on. If you would like to support the work of the centre please contact: icpc@aspi.org.au

Important disclaimer

ASPI

Tel +61 2 6270 5100
Email enquiries@aspi.org.au
www.aspi.org.au
www.aspistrategist.org.au
facebook.com/ASPI.org
@ASPI_ICPC

First published September 2020.

ISSN 2209-9689 (online), ISSN 2209-9670 (print)

Cover image: Illustration by Wes Mountain. ASPI ICPC and Wes Mountain allow this image to be republished under the Creative Commons License Attribution-Share Alike. Users of the image should use the following sentence for image attribution: 'Illustration by Wes Mountain, commissioned by the Australian Strategic Policy Institute's International Cyber Policy Centre.'

Funding for this report was provided by the US State Department

TikTok and WeChat

Curating and controlling global information flows

Fergus Ryan, Audrey Fritz and Daria Impiombato

Policy Brief
Report No. 37/2020

Contents

What's the problem?

While most major international social media networks remain banned from the Chinese market in the People's Republic of China (PRC), Chinese social media companies are expanding overseas and building up large global audiences. Some of those networks—including WeChat and TikTok—pose challenges, including to freedom of expression, that governments around the world are struggling to deal with.

The Chinese 'super-app' WeChat, which is indispensable in China, has approximately 1.2 billion monthly active users[1] worldwide, including 100 million installations outside of China.[2] The app has become the long arm of the Chinese regime, extending the PRC's techno-authoritarian reach into the lives of its citizens and non-citizens in the diaspora.[3] WeChat users outside of China are increasingly finding themselves trapped in a mobile extension of the Great Firewall of China through which they're subjected to surveillance, censorship and propaganda. This report also shows how Covid-19 has ushered in an expanded effort to covertly censor and control the public diplomacy communications of foreign governments on WeChat.

Newcomer TikTok, through its unparalleled growth in both Asian and Western markets, has a vastly larger and broader global audience of nearly 700 million as of July 2020.[4] This report finds that TikTok engages in censorship on a range of political and social topics, while also demoting and suppressing content. Case studies in this report show how discussions related to LGBTQ+ issues, Xinjiang and protests currently occurring in the US, for example, are being affected by censorship and the curation and control of information. Leaked content moderation documents have previously revealed that TikTok has instructed "its moderators to censor videos that mention Tiananmen Square, Tibetan independence, or the banned religious group Falun Gong," among other censorship rules.[5]

Both Tencent and ByteDance, the companies that own and operate WeChat and TikTok, respectively, are subject to China's security, intelligence, counter-espionage and cybersecurity laws. Internal Chinese Communist Party (CCP) committees at both companies are in place to ensure that the party's political goals are pursued alongside the companies' commercial goals. ByteDance CEO Zhang Yiming has stated on the record that he will ensure his products serve to promote the CCP's propaganda agenda.[6]

While most major international social media platforms have traditionally taken a cautious and public approach to content moderation, TikTok is the first globally popular social media network to take a heavy-handed approach to content moderation. Possessing and deploying the capability to covertly control information flows, across geographical regions, topics and languages, positions TikTok as a powerful political actor with a global reach.

What's the solution?

The global expansion of Chinese social media networks continues to pose unique challenges to policymakers around the world. Thus far governments have tended to hold most major international social media networks and Chinese social media networks to different standards. It's imperative that states move to a policy position where all social media and internet companies are being held to the same set of standards, regardless of their country of origin or ownership.

This report recommends (on page 48) that governments implement transparent user data privacy and user data protection frameworks that apply to all social media networks. If companies refuse to comply with such frameworks, they shouldn't be allowed to operate. Independent audits of social media algorithms should be conducted. Social media companies should be transparent about the guidelines that human moderators use and what impact their decisions have on their algorithms. Governments should require that all social media platforms investigate and disclose information operations being conducted on their platforms by state and non-state actors. Disclosures should include publicly releasing datasets linked to those information campaigns.

Finally, all of these recommended actions would benefit from multilateral collaboration that includes participation from governments, the private sector and civil society actors. For example, independent audits of algorithms could be shared by multiple governments that are seeking the same outcomes of accountability and transparency; governments, social media companies and research institutes could share data on information operations; all stakeholders could share lessons learned on data frameworks.

TikTok censorship

TikTok's rapid expansion around the world has been punctuated by a string of censorship controversies that it has struggled to explain away. Initial instances of censorship, documented in this report, were the result of a 'blunt approach' to content moderation that TikTok spokespeople admit they deployed in the app's 'early days'.[7] More recent examples of apparent censorship—including posts tagged with #BlackLivesMatter and #GeorgeFloyd—have been explained away by TikTok as the result of a 'technical glitch'.[8]

Our research suggests that many of these cases were most likely not aberrations, but the side effects of an approach that ByteDance, TikTok's owner and operator, has used in an attempt to avoid controversy and maintain what it considers to be an apolitical stance as it grows a worldwide audience.[9] But the very nature of TikTok's targeted global censorship isn't apolitical; in fact, it makes the app a politically powerful actor.

Our research shows, for example, that hashtags related to LGBTQ+ issues are suppressed on the platform in at least 8 languages. This blunt approach to censorship affects not only citizens of a particular country, but all users speaking those languages, no matter where in the world they live. TikTok users posting videos with these hashtags are given the impression their posts are just as searchable as posts by other users, but in fact they aren't. In practice, most of these hashtags are categorised in TikTok's code[10] in the same way that terrorist groups, illicit substances and swear words

are treated on the platform. On some occasions, hashtags are categorised as non-existent, when in fact they're tagged on videos across the platform.

TikTok spokespeople have repeatedly stated that the platform is not 'influenced by any foreign government, including the Chinese Government',[11] and that 'TikTok does not moderate content due to political sensitivities.'[12] But the censorship techniques outlined below disprove some of those claims and, instead, suggest a preference for protecting and entrenching the sensitivities, and even prejudices, of some governments, including through censoring content that might upset established social views.

On 6 and 7 September ASPI contacted TikTok and provided them with hashtags our research discovered were being shadowbanned and asked for comment on these research findings. These hashtags were:

- **#acab** – English, acronym for "all cops are bastards," use of which began during the George Floyd protests in the United States
- **#путинвор** – "Putin Is A Thief" in Russian
- **#Jokowi** – nickname for Joko Widodo, President of Indonesia
- **#GayArab** – English
- **#гей** – "Gay" in Russian
- **#مثلي_الجنس** – "Gay" in Arabic
- **#ялесбиянка** – "I am a lesbian" in Russian
- **#ягей** – "I am gay" in Russian
- **#gei** – "Gay" in Estonian
- **#gej** – "Gay" in Bosnian
- **#สมเด็จพระเจ้าลูกเธอเจ้าฟ้าสิริวัณณวรีนารีรัตนราชกัญญา** – #Princess Sirivannavari Nariratana Rajakanya in Thai
- **#กษัตริย์มีไว้ทำไม** – "Why Do We Need A King" in Thai
- **#ไม่รับปริญญาจากสถาบันกษัตริย์** – "I won't graduate with the monarchy" in Thai
- **#المتحول جنسي** – "Transgender" in Arabic
- **#التحول_الجنسي** – "Transgender/transitioning" in Arabic

The response by a TikTok spokesperson was:

> *"As part of our localised approach to moderation, some terms that the ASPI provided were partially restricted due to relevant local laws. Other terms were restricted because they were primarily used when looking for pornographic content, while the Thai phrases the ASPI supplied are either readily found when searched or do not appear to be hashtags that any TikTok users have added to their posts. We also identified, and fixed, an issue where some compound phrases in Arabic were being incorrectly moderated because part of the phrase may relate to pornography. Separately, a couple of English phrases were incorrectly moderated, and we have resolved the error. We are currently conducting a review of those terms that were moderated in error and will look for ways to improve our processes to avoid similar issues in the future. In addition, we want to be crystal clear that TikTok strongly supports our LGBTQ creators around the world and is proud that LGBTQ content is among the most popular category on the platform with billions of views."*

World leaders and politics

Leaked content moderation guidelines seen by *The Guardian* in March 2020 barred content related to a specific list of 20 'foreign leaders or sensitive figures' including Kim Jong-il, Kim Il-sung, Mahatma Gandhi, Vladimir Putin, Donald Trump, Barack Obama, Kim Jong-un, Shinzo Abe, Park Geun-Hee, Joko Widodo and Narendra Modi (Figure 1).[13] ByteDance said those rules were retired in May 2019, but our research has found that hashtags related to criticism of the leaders continue to be censored. The censorship ranges from #путинвор ('Putin Is A Thief') to even seemingly innocuous hashtags, such as #Jokowi—the politically neutral nickname for Indonesian President Joko Widodo. These hashtags have been shadow banned by TikTok, meaning that content tagged with them has been suppressed and often totally hidden from public view; posts are made much more difficult to find on the platform though they're not necessarily deleted. It's a more insidious form of censorship in that users are being censored, but often don't know it because they can still see their own content.

Figure 1: List of censored or shadow-banned political hashtags on TikTok

COUNTRY	LANGUAGE	HASHTAG	TRANSLATION	ON TIKTOK
RUSSIA	RUSSIAN	ПУТИНВОР	PUTIN IS A THIEF	SHADOWBANNED
INDONESIA	INDONESIAN	JOKOWI	(JOKO WIDODO)	SHADOWBANNED
THAILAND	THAI	สมเด็จพระเจ้าลูกเธอ เจ้าฟ้าสิริวัณณวรีนารีรัตนราชกัญญา	PRINCESS SIRIVANNAVARI NARIRATANA RAJAKANYA	REMOVED
THAILAND	THAI	ไม่รับปริญญาจากสถาบันกษัตริย์	I WON'T GRADUATE WITH THE KING	REMOVED
THAILAND	THAI	กษัตริย์มีไว้ทำไม	WHY DO WE NEED A KING	REMOVED

Source: ASPI's International Cyber Policy Centre (ICPC).

In the course of our research, we regularly encountered discrepancies between the number of videos visible on a hashtag and the number of videos recorded under 'videoCount' in the code. Those discrepancies could be due to videos being in review or videos that have broken TikTok's community guidelines, which include taking down content that is disinformation or is hateful, violent or sexually explicit content. But the discrepancy could also be due to videos being shadow banned. A source from

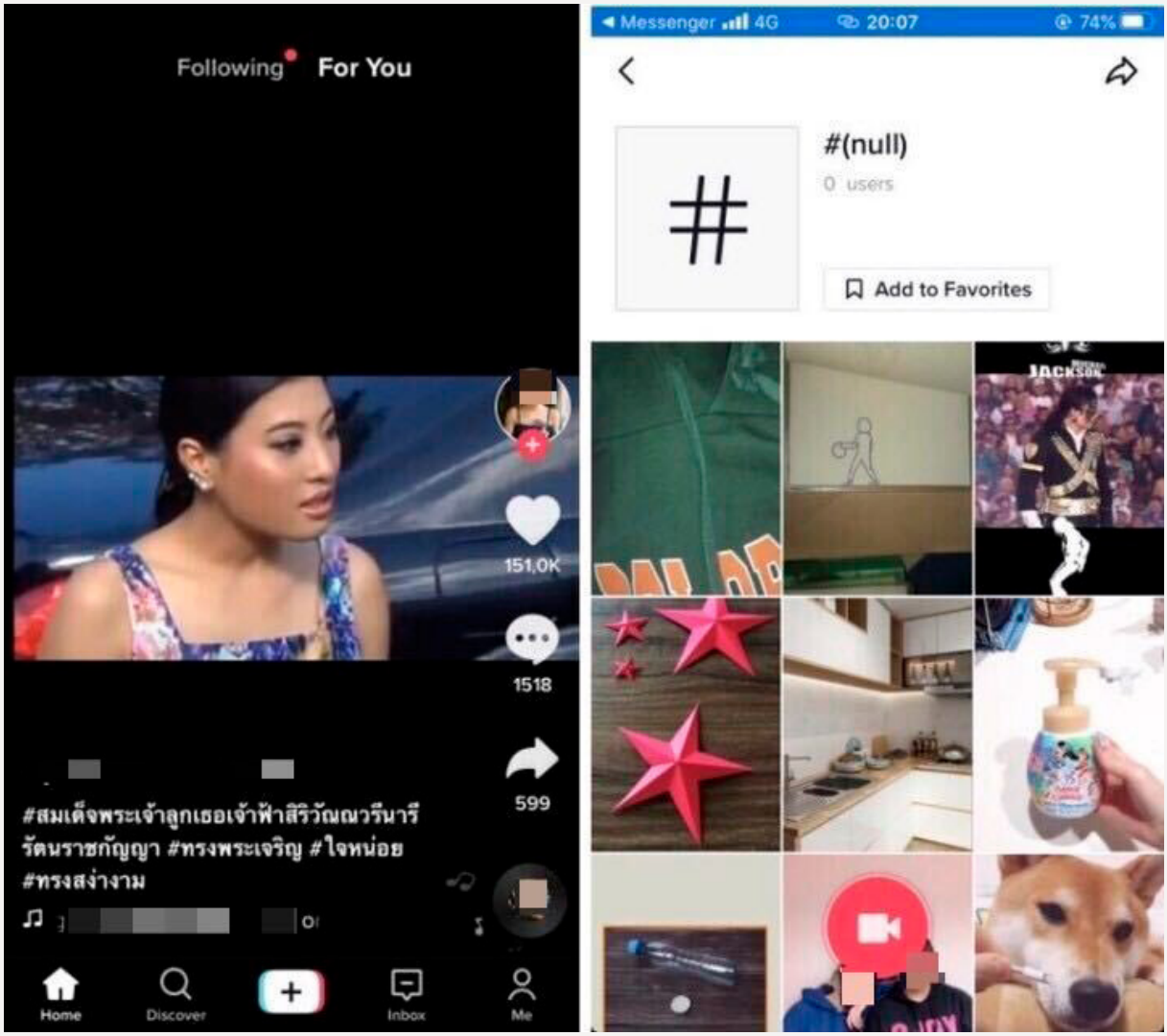
TikTok cited by *Netzpolitik* said that videos that are tagged 'Not for Feed' in the moderation process get excluded from being featured in the platform's 'For You' feed, which can then 'disadvantage discoverability in the search function and hashtags'.[14]

On 15 August, #HồChíMinh showed 63 videos visible on the web version of TikTok, but 383 videos in the code for the hashtag. It's possible that the 320 videos missing from the hashtag were absent because their content contravened TikTok's community guidelines, but there's a real possibility at least some of them were removed due to political censorship over the late communist leader of Vietnam. As *Reuters* reported in August 2020, ByteDance sought to avoid any run-ins with the Vietnamese Government by promising to make TikTok 'non-political' in the country.[15] That censorship was even extended by ByteDance to cover 'content critical of Beijing, and anything related to tensions between the two governments'.

Around the world, TikTok content guidelines have gradually become more localised for individual countries. Country-specific and so-called 'strict' content guidelines leaked to *The Guardian* suggest that the localised approach could result in more censorship than before.[16] In Thailand, where pro-democracy protests have been ongoing since June,[17] TikTok has attempted to avoid contravening the country's strict *lèse-majesté* laws, which make it illegal to insult, defame or threaten any member of the royal family, in an overly broad way. Our research shows that hashtags related to the Thai royal family are censored on TikTok, not just for Thai citizens, but for Thai-speaking people around the world.

On TikTok, #สมเด็จพระเจ้าลูกเธอเจ้าฟ้าสิริวัณณวรีนารีรัตนราชกัญญา (#PrincessSirivannavariNariratanaRajakanya) isn't just shadow banned but completely censored from the entire platform. The hashtag is used on other platforms, such as Twitter, YouTube, Facebook and Instagram, and isn't considered controversial. It's often linked to news articles about the princess or positive messages about her. On TikTok, the hashtag isn't functional on the app even when users click on the hashtag that they've tagged on their posts. While shadow-banned hashtags can be found on the app by clicking on hashtags through a video, when censored hashtags are clicked, users are redirected to a '#(null)' page with miscellaneous content in it (Figure 2).

Figure 2: A TikTok video featuring the hashtag #สมเด็จพระเจ้าลูกเธอเจ้าฟ้าสิริวัณณวรีนารีรัตนราชกัญญา (#PprincessSirivannavariNariratanaRajakanya), left. Clicking on the hashtag results in 'null' results, right



Source: TikTok.

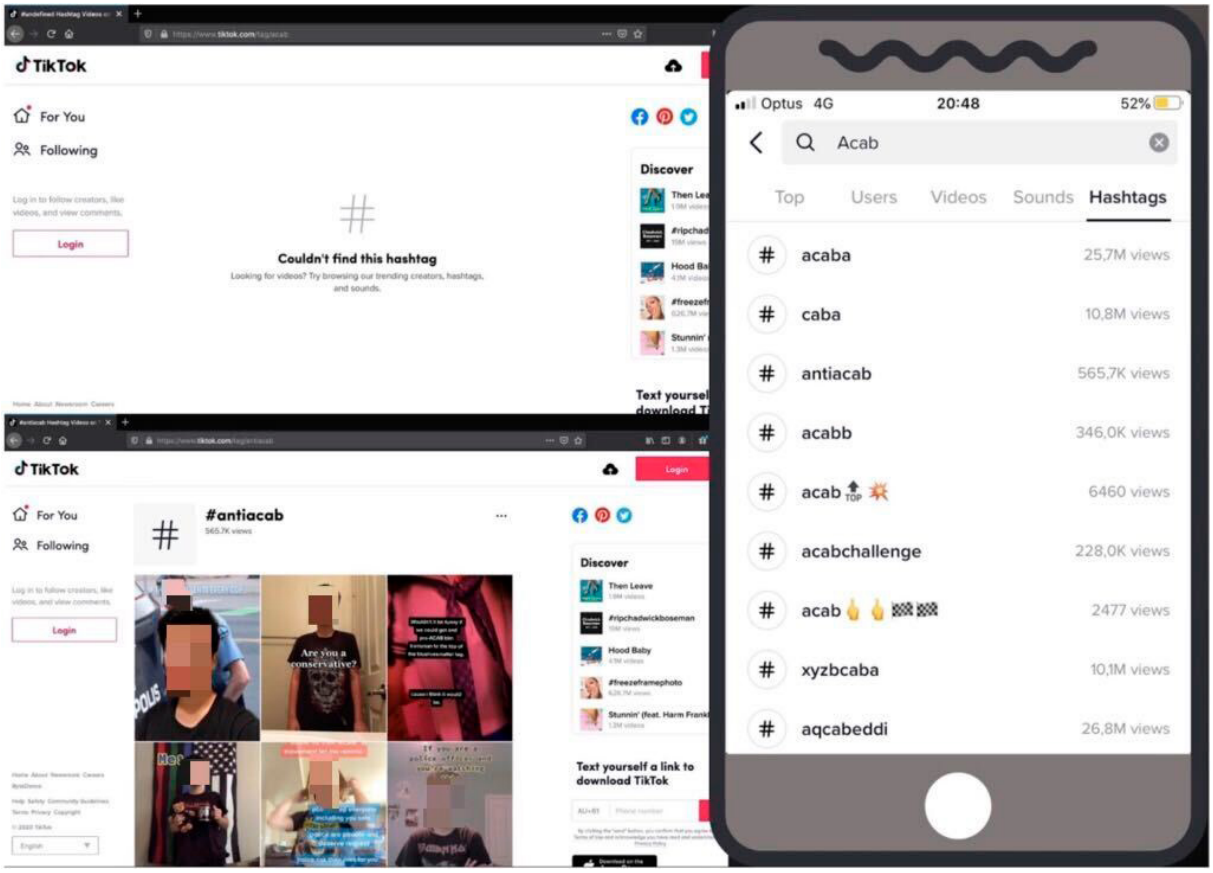
The hashtag #ไม่รับปริญญาจากสถาบันกษัตริย์ (#IWon'tGraduateWithTheMonarchy) is also censored on TikTok, in the same way as the hashtag #สมเด็จพระเจ้าลูกเธอเจ้าฟ้าสิริวัณณวรีนารีรัตนราชกัญญา (#PrincessSirivannavariNariratanaRajakanya) is. ASPI posted a test video on 25 August with this hashtag, but the hashtag search results page remained blank. When we clicked the hashtag on our post, it also redirected to a '#(null)' page with miscellaneous content in it.

Another hashtag related to the monarchy—#กษัตริย์มีไว้ทำไม (#WhyDoWeNeedAKing), —surged in popularity during the protests on other platforms like Twitter but had only 11 videos on the TikTok app on 28 August 2020. On 7 September, that number had dropped to just 7 videos. Curiously, the hashtag search results page for #กษัตริย์มีไว้ทำไม (#WhyDoWeNeedAKing) on TikTok.com on 28 August 2020 resulted in a blank search results page. On the same day, #ทรงพระเจริญ (Long live the King) had millions of views and hundreds of videos on the TikTok app. Twitter recorded more than 20,000 tweets with #กษัตริย์มีไว้ทำไม (#WhyDoWeNeedAKing) on 22 and 23 March 2020 as it trended in first place on Twitter in Thailand. The hashtag is mainly used by young Thai activists who fit TikTok's user demographics.

Protests

TikTok's strategy of blocking certain hashtags from search results continues to be deployed in the US, where hashtag search results for #acab—an acronym for 'all cops are bastards'—were suppressed in the early days of the George Floyd protests. After a public backlash, TikTok backed down, making several hashtags related to the protest, including #acab, available on 29 May. At that stage, the hashtag had garnered 96.5 million views, according to the Atlantic Council's Digital Forensic Research Lab (DFRLab).[18] But our research shows that, three months later, as anti-racism and anti-police-brutality protests took place in Kenosha, Wisconsin, following a police shooting of black man Jacob Blake, the #acab hashtag was censored once again after media scrutiny subsided (Figure 3).

Figure 3: A web search for #acab on TikTok.com (top left), a web search for #antiacab on TikTok.com, (bottom left) and a mobile search for #acab (right), all on 29 August



Source: TikTok.

It's highly unlikely that #acab, having been shadow banned, unshadow banned and now shadow banned again, is continuing to undergo a rolling 'technical glitch'. The inconsistency in TikTok's content moderation is highlighted by the fact that an opposing hashtag—#antiacab—wasn't shadow banned but readily available on both the mobile and browser versions of TikTok.[19]

A source working for TikTok cited by *Netzpolitik* in September 2019 said that protests were generally not welcome on the platform. 'Often such videos did not even make it into marketing, but would be deleted beforehand when the moderator looked at them for the first time at other locations such as Barcelona,' the German outlet reported.[20] The source said that TikTok changed its moderation rules after *The Guardian* revealed its heavy-handed political censorship in September 2019. Those rules

included instructions to "censor videos that mention Tiananmen Square, Tibetan independence, or the banned religious group Falun Gong."[21]

A former content moderator for TikTok told the *New York Times* in November 2019 that 'managers in the US had instructed moderators to hide videos that included any political messages or themes, not just those related to China.' Speaking on the condition of anonymity, the informant said that the policy was to, in the newspaper's words, 'allow such political posts to remain on users' profile pages but to prevent them from being shared more widely in TikTok's main video feed.'[22]

LGBTQ+

TikTok claims that it continues 'to see the vulnerability of LGBTQ+ rights', writing in a June 2020 blog post that 'it's important to us that the LGBTQ+ voices and stories of those who are pushing forward acceptance for all and helping to create a world where everyone has the right to be who they are and love who they love, are shared, seen and heard.'[23] Our research shows that that commitment isn't applied consistently across multiple languages.

Content moderation guidelines leaked to *The Guardian* revealed in September 2019 that LGBTQ+ content was banned on TikTok even in countries where homosexuality has never been illegal.[24] Additional reporting by *Netzpolitik* in December 2019 (also based on leaked documents from TikTok) revealed that the platform was limiting the reach of LGBTQ+ users as well as disabled and overweight people—a charge TikTok admitted to but explained away as an attempt to protect users with at high risk from bullying.[25]

According to *The Guardian*, content moderation guidelines specific to Turkey included an entire section devoted to censoring depictions of homosexuality—much of which 'went substantially further than required by law'. Censored content included 'intimate activities (holding hands, touching, kissing) between homosexual lovers', 'reports of homosexual groups, including news, characters, music, tv show, pictures', as well as 'protecting rights of homosexuals (parade, slogan, etc.)' and 'promotion of homosexuality'.

LGBTQ+ TikTok users around the world have complained about censorship of their posts, including in the UK,[26] the US[27] and Turkey.[28] Our research has found that hashtags related to LGBTQ+ issues in Russian, Arabic, Bosnian and more aren't searchable on the platform, preventing people who speak those languages all over the world from taking part in the discussion (Figure 4).

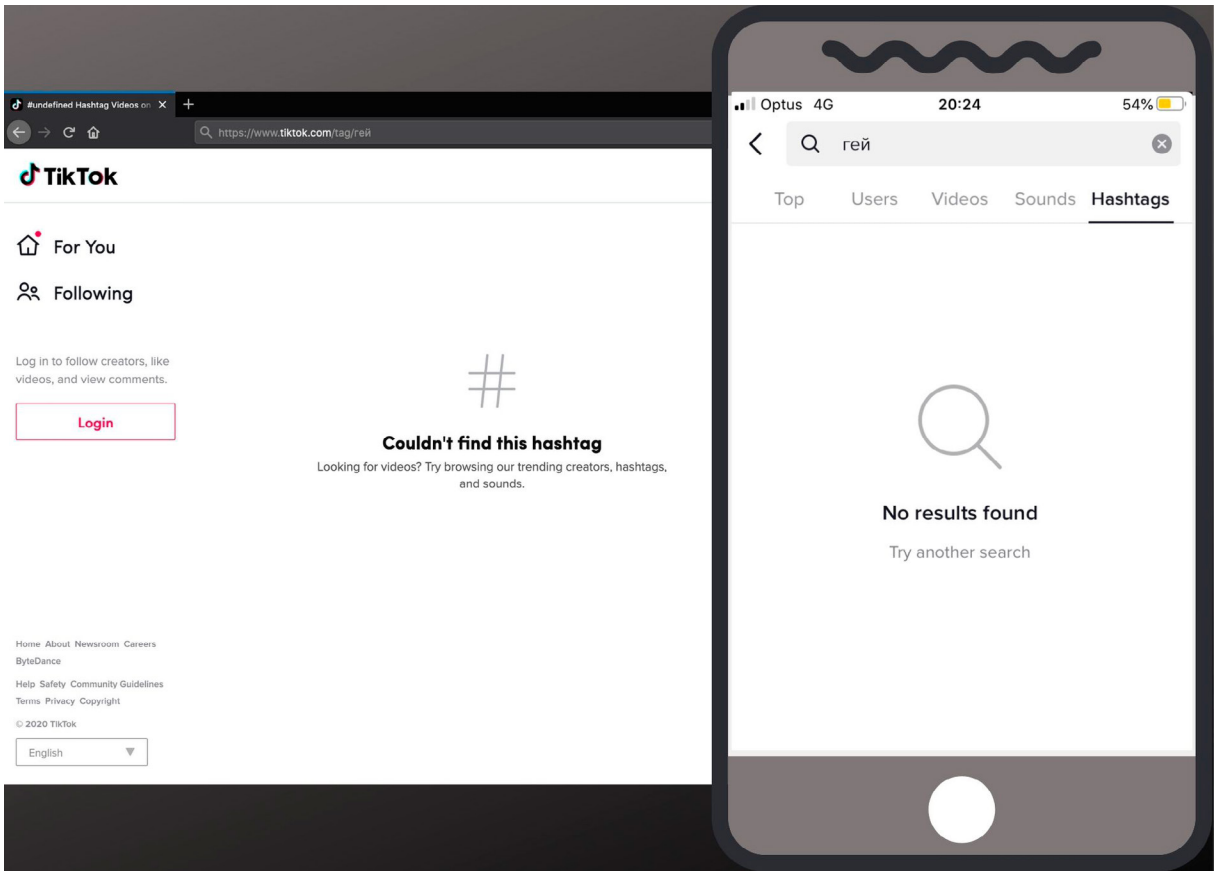
Figure 4: List of shadow-banned LGBTQ+ hashtags on TikTok

Word	Language	Translation	TikTok
гей	Russian	Gay	Shadowbanned (web + app)
ялесбиянка	Russian	I am a lesbian	Shadowbanned (web + app)
ягей	Russian	I am gay	Shadowbanned (web + app)
مثلي_الجنس	Arabic	Gay	Shadowbanned (web + app)
المتحول_جنسي	Arabic	Transgender	Shadowbanned (web + app)
التحول_الجنسي	Arabic	Transitioning (transgender)	Shadowbanned (web + app)
гей	Ukranian	Gay	Shadowbanned (web + app)
гей	Bulgarian	Gay	Shadowbanned (web + app)
гей	Kazakh	Gay	Shadowbanned (web + app)
гей	Kyrgyz	Gay	Shadowbanned (web + app)
gei	Estonian	Gay	Shadowbanned (web + app)
gej	Bosnian	Gay	Shadowbanned (web + app)

Source: ASPI ICPC.

LGBTQ+ content in Russian, for example, is shadow banned on TikTok. When Russian-speaking users—citizens and non-citizens alike—search the app for #гей (#Gay), they're met with a blank hashtag search result page (Figure 5).

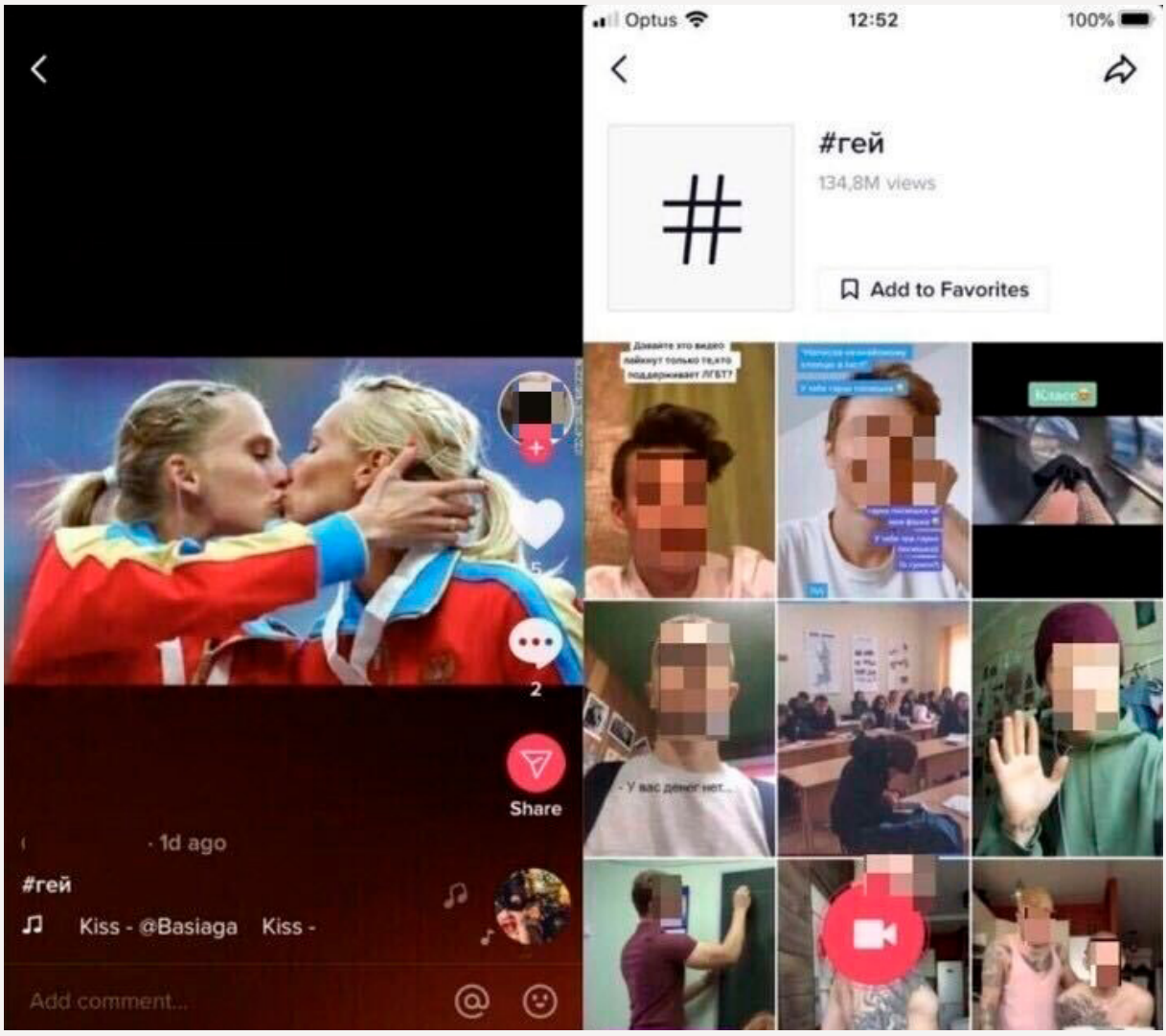
Figure 5: A web search for #гей (#Gay), left, and a mobile search for #гей (#Gay), right, both on 29 August



Source: TikTok.

Users who are motivated enough can discover other posted videos using the hashtag, but only after posting their own video featuring the hashtag and then clicking through to the content there (Figure 6). Doing so directs the user to the correct page, which does exist, but is unavailable (shadow banned) from the platform's search results. Despite being invisible in search results, the hashtag is widely used and had more than 130 million views as of 30 August 2020.

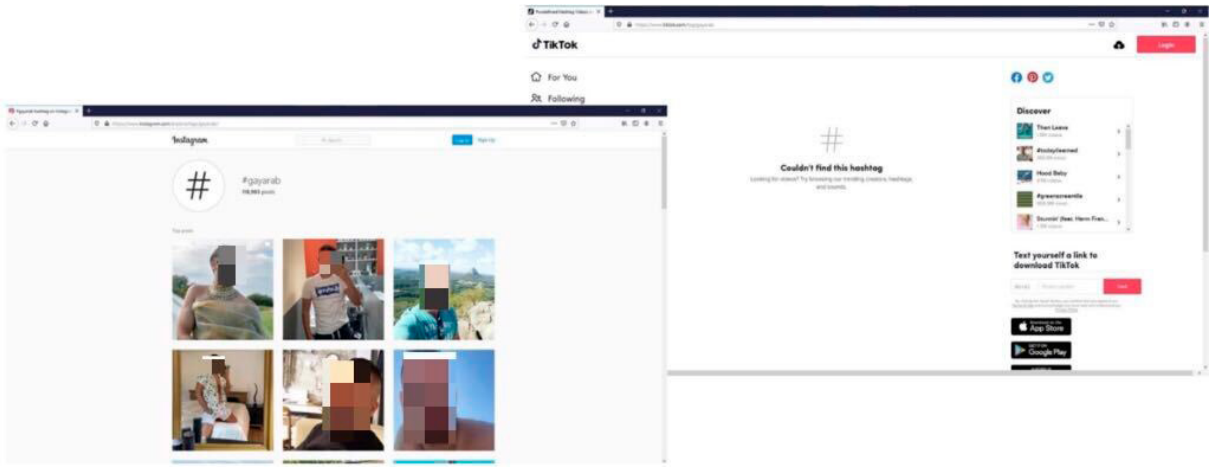
Figure 6: A test TikTok video featuring the hashtag #гей (#Gay) published on 26 August 2020 (left). The correct page (right) is revealed only after clicking on the hashtag in a posted video



Source: TikTok.

Some LGBTQ+-related hashtags face the same level of censorship outlined above in the case of Thailand's Princess Sirivannavari Nariratana Rajakanya. Clicking on #GayArab doesn't direct users to a page featuring other shadow-banned videos, but instead redirects to a '#null' page (Figure 7). On Instagram, a search for the hashtag 'Gay Arab' on 28 August resulted in a list of 118,000 tagged images.

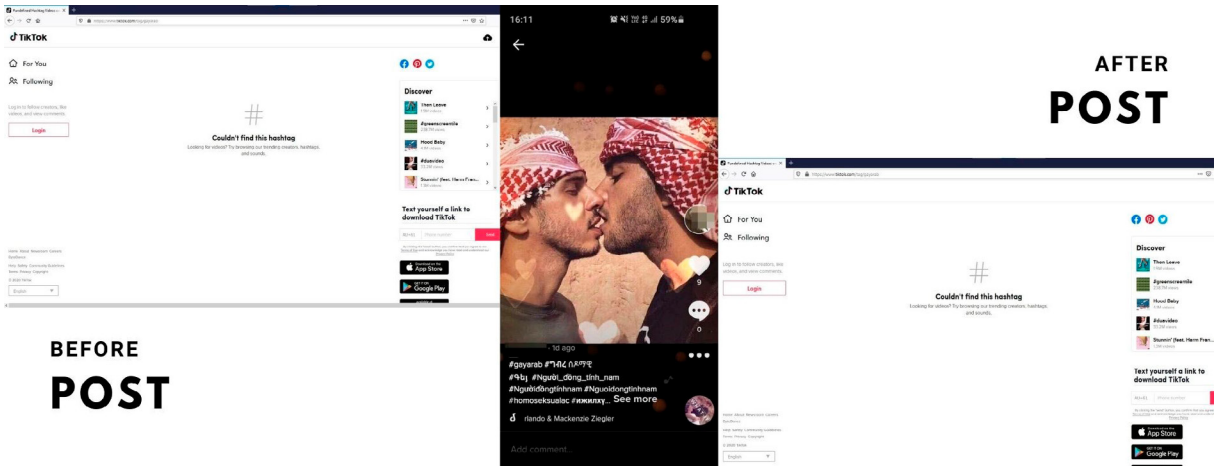
Figure 7: Web search for #GayArab on Instagram (bottom left) and web search for #GayArab on TikTok (top right)



Sources: Instagram.com and TikTok.com.

A test video posted by ASPI ICPC to #GayArab on TikTok didn't appear in the hashtag web search results, which continued to feature a 'Couldn't find this hashtag' result (Figure 8).

Figure 8: Web search for #GayArab on TikTok.com before ASPI's test video on 26 August 2020 (top left), ASPI's test TikTok video (centre) and web search for #GayArab on TikTok after ASPI's test video (bottom right)



Source: TikTok.com.

The words for 'gay' and 'transgender' in Arabic are also shadow banned. TikTok has often stated its willingness to adhere to local laws in its terms of service.[29] Homosexuality is illegal in several Arabic-speaking countries, but there are exceptions, such as Iraq and Jordan.[30] Implementing specific countries' rules across the platform means that Arabic-speaking people around the world, even those who live in countries where homosexuality is in fact legal, are prevented from accessing content related to these hashtags on TikTok.

TikTok's use of these censorship methods isn't consistently applied. A more casual term used to mean "gay" in Arabic, مثلي, (literally "like me") is not censored in the ways outlined above. ASPI ICPC also found inconsistencies in the content moderation regarding multiple terms that refer to "gay" and "transgender" in Arabic. One term in Arabic that can be translated as "transgender" and was not shadowbanned, المتحول جنسيا, demonstrates how even discrepancies in grammar can impact the censorship of a word despite having the same meaning. In Russian, #лесбиянство "lesbianism" is also

not censored in the ways outlined above, though it only had seven videos when checked on 5 August 2020.

In September 2019, *Netzpolitik*, citing leaked content moderation guidelines from a source inside TikTok, reported that LGTBQ+ content used to be marked as 'Islam Offence' by moderators. 'Content tagged with this keyword, such as two men kissing, triggered a geoblock for certain regions,' the German outlet reported. According to the publication, content that deals with sexual orientation is now tagged 'Risk 3.4' instead of 'Islam Offence', and is still used to prevent that content reaching Islamic countries.[31]

Netzpolitik's source also revealed that the platform was not only able to slow down videos from going viral, but also entire hashtags:

> In general, TikTok seems to have a system of promoting and slowing down, in which certain content is visible and viral, while others never take off and aren't visible. Control of what people see on TikTok is mostly in the hands of the company.

An ASPI ICPC analysis of the hashtags mentioned above revealed a much blunter form of censorship. In practice, the hashtags are categorised in TikTok's code in the same way that terrorist groups, illicit substances and swear words are on the platform. This blanket shadow banning of topics related to LGBTQ+ issues shows how TikTok's 'blunt approach' to content moderation continues to this day.

The same code is assigned to hashtags related to QAnon conspiracy theories, which TikTok started blocking in late July 2020.[32] These hashtags are hidden from TikTok searches, but videos with the same tags remain on the platform[33]—much like the examples listed above, such as 'gay' in Russian and Arabic. TikTok treats these hashtags in the same way as extremist content, including #Nazi, #KKK and #ISIS.

TikTok sources cited by Chinese technology publication *Pingwest* say the platform plans to localise content moderation decisions to such a point that, for example, posts about recreational marijuana use will be visible in jurisdictions where it's legal but invisible where it isn't.[34] At time of publication, #marijuana appears to be shadow banned for all users, regardless of which country or US state they reside in.

TikTok's approach to content moderation reveals a fundamental misunderstanding about the role of free speech in democracies. TikTok users should expect to be able to freely take part in conversations about issues that they, as citizens, have a role in creating laws about.

Free speech has its limits, and TikTok, like other platforms, has attempted to take a proactive approach to combating hate speech, for example.[35] However, in countries such as Vietnam and Russia, TikTok has gone beyond complying with the letter of the law and has instead seemingly offered censorship as a service to those administrations.[36]

In Russia, the use of #путинвор ('Putin Is A Thief')—a catchcry of the political opposition—could be argued to be in contravention of a 2019 law banning online insults against the Russian Government, but the law is very much in contention.[37] When it was passed in March 2019, opposition leader Alexey Navalny immediately took to Twitter to insult President Vladimir Putin's administration.[38] Twitter remains available in Russia.

Similarly, it's likely that TikTok's widespread censorship of LGBTQ+-related topics in Russian is the result of overcompliance with a 2013 law that bans disseminating 'propaganda on non-traditional sexual relations' among young Russians.[39] According to Human Rights Watch, the law 'directly harms children by denying them access to essential information and creating a stigma against LGBT children and LGBT family members.'[40] The law hasn't stopped other platforms, such as Instagram, featuring LGBTQ+ related hashtags. There have been instances in which platforms such as Twitter[41] and Instagram[42] have buckled to pressure from the Russian Government, but TikTok's approach represents a more comprehensive overreach that sides with the Russian Government against the Russian people's right to free speech.

#Xinjiang: curating propaganda

As ASPI ICPC's 2019 *Mapping more of China's tech giants: AI and surveillance report* revealed, TikTok owner and operator ByteDance collaborates with public security bureaus across China, including in Xinjiang, where it plays an active role in disseminating the party-state's propaganda concerning the region.[43]

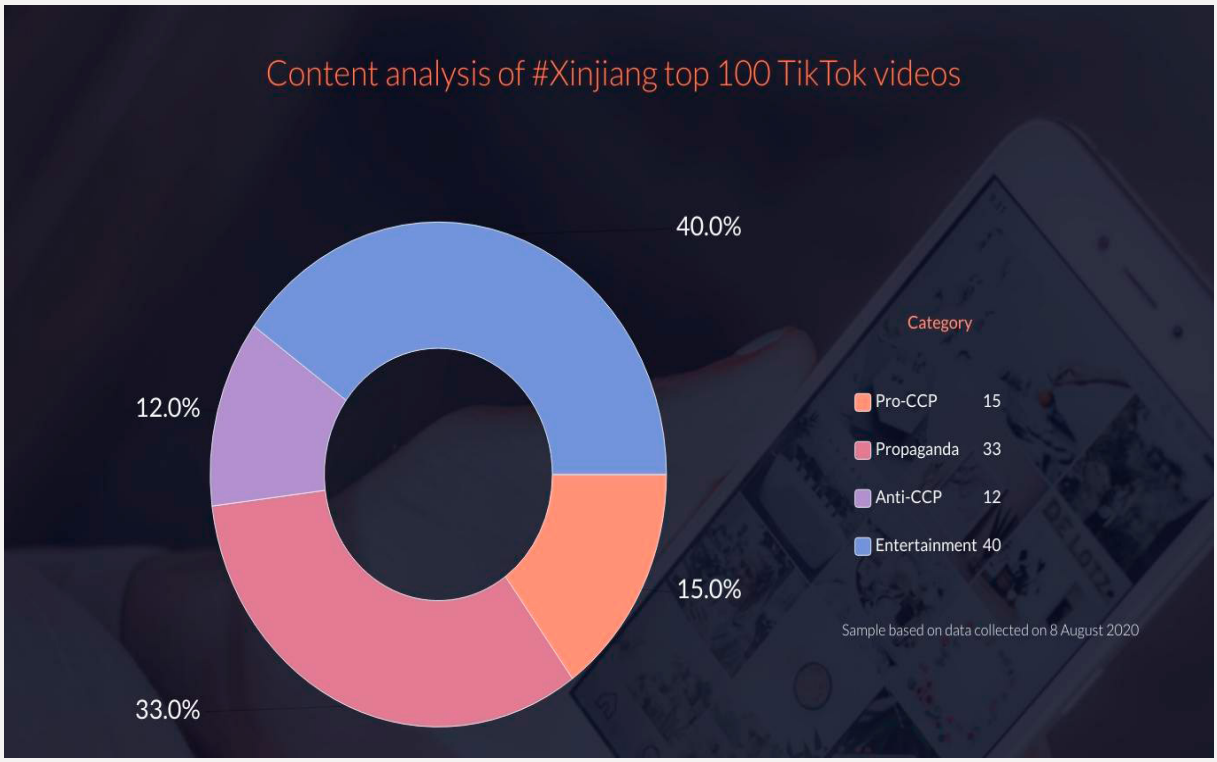
In late November 2019, a search for #Xinjiang on TikTok resulted in only two videos when *VICE Germany* journalist Sebastian Meineck posted two videos featuring the hashtag. The videos were among seven videos Meineck posted to the platform with hashtags considered politically sensitive by Beijing. The videos were posted successfully but, in at least nine cases, disappeared from the platform's hashtag search results.[44]

TikTok blamed a 'bug' for causing the videos to not show up on #freexinjiang, #uiguren, #chinacables, #xinjiang, #tiktokcensorship, #uyghur, #xijinping, #culturalgenocide and #democracy, explaining to *VICE Germany* that it was 'a technical error that has nothing to do with the moderation of content'.

In the nine months following this media scrutiny, activity on #Xinjiang initially increased. By 8 August 2020, when ASPI ICPC accessed the hashtag, 444 videos were publicly visible. Through manual content analysis, it was determined that of those 444 videos, only 5.6% were critical of the CCP's policies in the region—an unusually small number, given the debate over the topic on other platforms.

Of the top 20 videos with the highest ranking on the hashtag, only one is critical of the CCP (Figure 9). Seven are either denialist videos or videos promoting conspiracy theories about Beijing's extrajudicial incarceration of more than a million Uyghurs and members of other Turkic Muslim minorities in Xinjiang. The ranking of all of the top 20 posts on the hashtag bears no discernible connection to their number of likes, comments, shares or views, based on our analysis.

Figure 9: Content analysis of the first 100 videos on the hashtag #Xinjiang. Pro-CCP: any video that denies the persecution of Uyghurs, the camps etc. Propaganda: videos that in many cases are sourced from TikTok's PRC-based and highly censored sister app Douyin and depict Xinjiang in an exclusively idyllic way.



Source: TikTok.com, 8 August 2020.

Among the videos found on the hashtag were five by a self-described 'vlogger' who goes only by the name of Jessica.[45] Jessica's videos featured in #Xinjiang document her trip to the western region during the Covid-19 pandemic, detailing the measures China put in place to contain the spread of the virus and trumpeting their precision and safety.[46]

Vloggers, photographers, Chinese state media reporters and online influencers are among the groups of people who have been dispatched to the region as part of an extended propaganda campaign dubbed 'Xinjiang is a good place'.[47] Since 2018, the campaign, organised by the Xinjiang Uyghur Autonomous Region Party Committee Cyberspace Office and the Xinjiang Propaganda Department, has sent more than 150 influencers and more than 150 Chinese state media reporters to the region.[48]

It isn't clear whether Jessica was part of that particular campaign, but analysis of her online presence on social media and mentions of her in the Chinese media reveal her to be Zang Shijie (臧诗洁, Jessica Zang)—an employee at state media China Central Television (CCTV)[49] and a CCP member.[50]

Another account featured on the hashtag is @guanvideo, which is a video production company headed by Pan Xiaoli (潘小璃), who is a researcher affiliated with the China Institute (a think tank at Shanghai's Fudan University). The company produces videos that it says 'adhere to positive energy guidance and provide high-quality knowledge and ideological content', including for Hu Xijin, the editor of the *Global Times* (the staunchly nationalistic CCP-run tabloid).[51]

TikTok user @aygul_uyghur has 10 videos in #Xinjiang. She describes herself as 'just a simple Uyghur girl from Xinjiang' in her bio. Views on all of her videos, which mostly feature her dancing, smiling and showing off produce such as watermelons, are in their thousands. Her most viewed video has been watched 109,700 times.

The hashtag has also been flooded with content sourced from TikTok's PRC-based sister app Douyin depicting an idealised version of the region. Uyghurs had, for a time, been able to use Douyin to shine a light on their persecution at the hands of the PRC state,[52] but, following ByteDance's formal cooperation with the Ministry of Public Security's Press and Publicity Bureau in April 2019,[53] it's now the site for organised and slick propaganda campaigns.[54]

The result, even for TikTok users perusing the topic, is a depiction of Xinjiang that glosses over the human rights tragedy unfolding there and instead provides a more politically convenient version for the CCP, replete with smiling and dancing Uyghurs.

The transformation of #Xinjiang coincided with a period of experimentation in Beijing's propaganda efforts as the PRC struggled to regain control of the narrative after the outbreak of Covid-19.[55] Non-Chinese platforms such as Twitter,[56] Facebook[57] and Google[58] have all confirmed PRC state-backed attempts to manipulate their platforms to project the CCP's political power.

In May, the Chinese Academy of Social Sciences (a prominent think tank) was one organisation proposing this strategy for Beijing's external communications. It recommended, among other things, that Beijing use WeChat, Weibo and TikTok to counterbalance Twitter, Facebook and YouTube.[59]

Leaked moderation documents obtained by The Intercept indicate that TikTok "has influenced content on its platform not just by censoring videos and disappearing users, but by padding feeds with content from "shadow accounts" operated by company employees posing as regular users."[60]

The apparent manipulation of content on #Xinjiang suggests that state-linked information campaigns are highly likely to be taking place on TikTok as well. Given the ByteDance CEO's commitment to advancing CCP propaganda and the fact that the company already works closely with PRC public security bureaus to produce and disseminate that propaganda, it's highly likely that Beijing would make such an attempt and even less likely that ByteDance would conduct any transparent investigation to stop state-actor manipulation of its platform.

Non-Chinese social media platforms are now expected to investigate and root out state-actor manipulation of their platforms, even if they are not legally forced to. Regulatory frameworks need to be strengthened to ensure all social media companies are required, by law, to prevent their platforms from being manipulated in the same way.

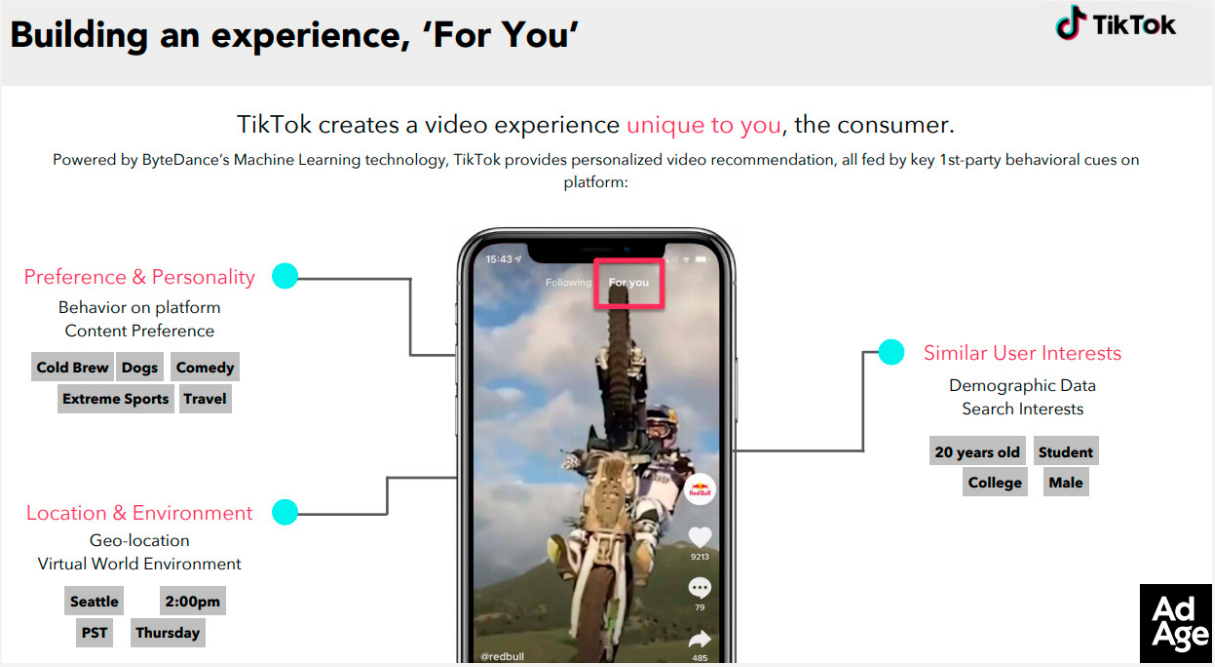
An algorithm with CCP characteristics

The shadow banning and censoring of hashtags removes one of the main ways users have of finding and interacting with content on TikTok, but the main way they receive content is via the app's algorithmically curated 'For You' feed.

When users open TikTok, they're immediately served up an endless feed of short, full-screen immersive videos that quickly becomes personalised to each individual user. On other social media apps such as Facebook and Twitter, users generally only see content from accounts that they've subscribed to. On TikTok, the 'For You' page serves up videos from creators you haven't followed but that the recommendation algorithm predicts you'd be interested in. As one observer noted, 'When you gaze into TikTok, TikTok gazes into you.'[61]

Faced with criticism about its lack of transparency over how the feed works, TikTok published a blog post in June 2020 that revealed some of the more obvious inputs that determine what content is promoted.[62] Those inputs include what the platform calls '1st-party behavioral cues', such as which videos users engage with, the duration of their engagement, and their interactions with the video, such as liking, commenting and sharing. It also uses data obtained from the users' devices, such as geolocation, and data obtained from users themselves, such as their age and gender (Figure 10).

Figure 10: A TikTok pitch deck shows that TikTok's recommendation engine is trained using data obtained from the user, their interactions and the user's device, from which TikTok can determine such things as user content preferences, demographics and geolocation



Source: Ad Age.

There are likely many other advanced inputs that go into TikTok's core algorithm—some of them sensitive enough to cause Beijing to add content-recommendation technology to its export control rules in late August 2020.[63] Facial recognition and even sentiment analysis[64] are among some of the more advanced inputs that are potentially used, via a process known as 'deep learning', to personalise users' feeds.

Another input into ByteDance's core algorithms—mandated by PRC law—is the CCP's propaganda agenda. In December 2019, new internet censorship rules issued by the Cyberspace Administration of China bolstered restrictions on 'negative' content and encouraged posts that focus on 'Xi Jinping thought' and 'core socialist values' or content that increases the 'international influence of Chinese culture'.[65] Significantly, the new rules call on platform operators to ensure that the algorithms undergirding their apps promote CCP propaganda.

This followed guidelines released in January 2019 by the China Netcasting Services Association at the PRC Government's direction that banned 100 types of inappropriate content and called on platform operators to review every piece of content that goes online. More specifically, the guidelines called for platform operators to build content management systems that are capable of screening headlines, introductions, screen 'bullets' and comments before they're published.[66]

There's strong evidence that the guidelines have already informed TikTok's global content moderation efforts. Moderation guidelines that were in use through at least late 2019 and were leaked to *The Intercept* referred to content that harmed 'national honor' or included 'state organs such as police', 'defamed civil servants', or anything that might threaten 'national security' as being worthy of censorship.[67] Those categories line up with the China Netcasting Services Association guidelines, rule 42 of which bans 'malicious slander' of, among other things, 'national security', 'police' and 'justice and other national public servants'.[68]

ByteDance executives, including CEO Zhang Yiming, have stated on the record that they'll ensure that their products serve to promote the CCP's propaganda agenda. Crucially, key executives have made it clear that the party line should be integrated into the company's apps down to the level of the algorithm.

Zhang Yiming has made it abundantly clear that the company is more than willing to manipulate the algorithm in favour of the CCP. On 11 April 2018, after regulators suspended ByteDance's flagship news aggregator *Jinri Toutiao* (*Today's Headlines*), Zhang announced that the company was shutting down another app, on the regulators orders, because it had deviated from the party line. 'The product has gone astray, posting content that goes against socialist core values,' Zhang wrote about the joke sharing app. 'It's all on me. I accept all the punishment since it failed to direct public opinion in the right way.'

In the letter, published at 4 am on Chinese social media, Zhang apologised for failing to respect the CCP's 'socialist core values' and for 'deviating from public opinion guidance'. 'In the past, we have placed too much emphasis on the role of technology, and failed to realise that socialist core values are the prerequisite to technology,' Zhang wrote. 'We need to spread positive messages in line with the requirements of the times while respecting public order and good practice.'

Zhang's strategy for righting the ship, outlined in the letter, included the hiring of 4,000 extra censors, integrating 'socialist core values' into the company's technology and products and investing more money in developing algorithms to screen posts. Zhang explicitly stated in his apology that this ideological readjustment was necessary to 'build a global platform for creating content and exchanges', highlighting the international implications of the policy change.[69]

At an internal CCP meeting hosted by the ByteDance Party Committee in April 2018, Zhang Fuping, the secretary of the committee and editor-in-chief at the company, stressed that the committee should improve its standing in the company and 'take the lead' across 'all product lines and business lines' to ensure that the algorithm is informed by the 'correct political direction' and 'values'.[70] At the same meeting, Chen Lin, vice president of products, and the executive in charge of optimising ByteDance's algorithm recommendations across all of the company's products, said that its apps should not only serve users the content that they want, but also content that would 'spread positive energy', and 'highlight socialist core values'.[71]

The result inside China is what veteran Chinese journalist and media researcher at the University of Pennsylvania, Kecheng Fang, refers to as 'a super algorithm' that ensures that content about the CCP, and Xi Jinping in particular, is always prominently displayed on Chinese platforms.[72] While it's unlikely that ByteDance would manipulate TikTok's algorithm as blatantly as it does on its PRC-based

equivalent, Douyin, there's ample room for it to covertly tweak users' feeds, subtly nudging them towards content favoured by governments and their ruling parties—including the CCP.

ASPI ICPC's analysis of ByteDance's own career page shows that the company has continued to advertise for TikTok content monitoring positions that are based in the PRC. ByteDance's career page in Chinese also includes postings for Beijing-based TikTok positions for jobs related to other geographical markets, such as one for a data operations manager for the Middle East and a senior operations strategy manager for Latin America, *The Information* reported in late July 2020.[73] As of August 2020, ByteDance also advertised for a Shanghai-based TikTok content operations manager to cover the eastern EU, according to our analysis.

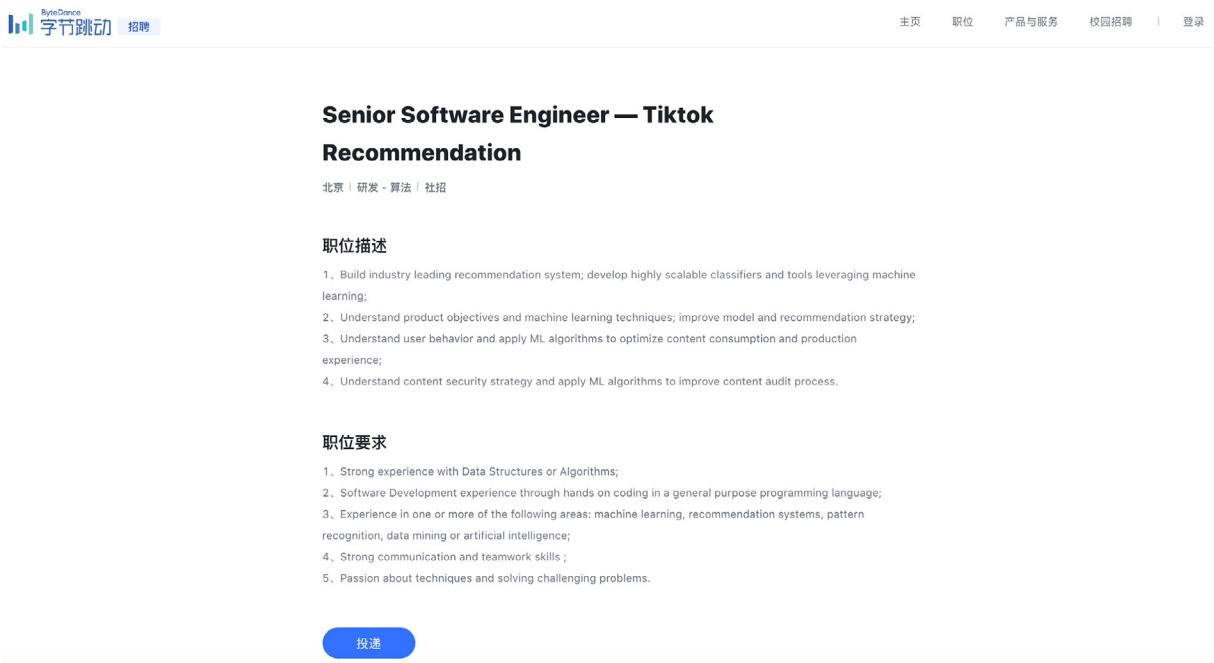
Even if ByteDance successfully ringfences TikTok from its China operations, censorship and information control can still be achieved via the app's opaque algorithm, which is developed by ByteDance's China-based engineering teams.[74] TikTok does employ engineers based in Mountain View, California, but they report to senior executives in China.[75] The company's algorithms enable TikTok and other ByteDance apps to select videos to recommend, target ads and detect content for moderation or deletion.[76] China-based researchers at ByteDance's Artificial Intelligence (AI) Lab are also developing speech recognition algorithms that are able to screen videos for illicit content for use in all ByteDance apps.[77]

A 2019 white paper produced by ByteDance outlined how the contents of users' livestream videos are fed into a social credit system, which assigns a rating to users based on the content they produce. Content that promotes 'positive energy' is boosted, including—the white paper notes—content that 'passes on the Communist Party spirit'.[78]

TikTok's algorithms continue to be controlled from the PRC, where its server code remains partially shared across other ByteDance products, according to *Reuters*. That code provides basic functionality of the apps such as 'data storage, algorithms for moderating and recommending content and the management of user profiles'.[79]

Job ads analysed by ASPI ICPC indicate that ByteDance intends to continue to develop and control its core algorithms from the PRC. The company continues to advertise for PRC-based R&D positions that work on the TikTok algorithm, including one still visible on the ByteDance recruitment site in late July for a senior software engineer who would be responsible for the app's content recommendation system (Figure 11).[80]

Figure 11: Example of a TikTok PRC-based R&D position advertised by ByteDance as of August 2020



Several other Beijing- and Shenzhen-based R&D positions advertise for back-end and algorithm roles with responsibilities covering ByteDance's multiple platforms TikTok, Douyin and Toutiao. Such positions include a back-end development engineer for Douyin, Toutiao and TikTok as well as an algorithm engineer for Douyin, Toutiao and TikTok.

In late August 2020, China updated its export control rules for the first time since 2008 to include content-recommendation technology.[81] The extent to which 'Xi Jinping thought' and 'core socialist values' are mixed into the secret sauce of TikTok's algorithms may never be known now that Beijing has deemed it a matter of state security.

A politics-free zone

TikTok executives have long been upfront about their desire for the app to be a politics-free zone. In 2018, when Raj Mishra, then TikTok's head of operations in India, was asked by *Bloomberg* if TikTok would allow criticism of Indian Prime Minister Narendra Modi to be prominently featured in the app, he replied 'No'. TikTok's ambition, Mishra explained, was to be a 'one-stop entertainment platform where people come to have fun rather than creating any political strife'.[82] Blake Chandlee, Vice President Global Business Solutions, has talked about TikTok's decision not to accept political advertising on the app as a decision designed to ensure that the app's 'environment' didn't become 'a negative one'.[83] TikTok global chief security officer Roland Cloutier told *PBS Newshour* as recently as 25 August 2020 that TikTok is 'not the go-to platform for robust political debates at all'.[84]

In the US, that approach was made untenable after the killing of George Floyd galvanised Black Lives Matter protesters, some of whom flocked to TikTok to use it for their activism. Some of those users have reported that they experienced noticeable declines in viewership and engagement on their videos or even that their videos were taken down, muted or hidden from followers.[85] The director of TikTok's Creator Community, Kudzi Chikumbu, told *TIME* that TikTok 'unequivocally' doesn't engage in shadow banning. On 1 June 2020, TikTok attributed the decline in viewership and engagement with

videos of Black Lives Matter protestors to a 'technical glitch' and apologised for that glitch, pledging to better support its Black community and take steps toward a more inclusive environment.[86]

Political content from all ideological persuasions is now increasingly common on TikTok, especially in the lead-up to the 2020 US presidential elections. It is, as the *New York Times* put it in late June 2020, a place where teens 'are forming political coalitions to campaign for their chosen candidates, post news updates, and fact-check opponents'. The result is that a platform over which Beijing has enormous leverage is now in a position in which it could easily, and surreptitiously, promote or demote content about either presidential candidate.[87]

In India, ByteDance has used its ability to promote, demote and suppress content in ways that not only affect what TikTok users see, but also what content they produce.

Ajay Barman

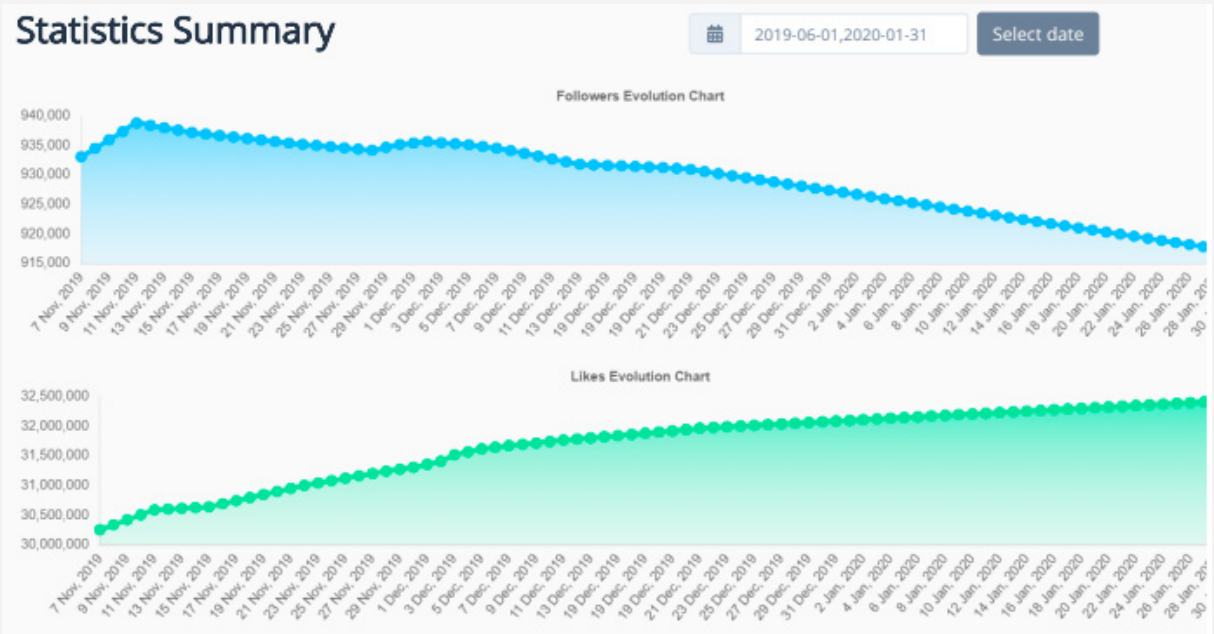
Indian TikTok user who believes he was shadow banned after posting about politics.

Indian TikTok user Ajay Barman abandoned posting about social and political topics after it appeared that the platform had shadow banned his videos. Barman told *BBC News* that his videos dropped from an average of 200,000 views down to around 8,000 views after he started posting about Hindu–Muslim unity.[88] Barman's follower count also dropped by 25,000 users, *BBC News* reported.

Barman said the drop in views and followers came around the time a backlash began against the Citizenship Amendment Act—a controversial law passed by India's Hindu nationalist government in December 2019 that offered Indian citizenship only to non-Muslims fleeing religious persecution in surrounding countries.

Fully verifying Barman's claims is difficult, given the opaque nature of TikTok's algorithm, but data we sourced from CloutMeter for Barman's TikTok account from 7 November to 31 January 2019 showed that his follower numbers were indeed declining, even as his 'likes' continued to rise (Figure 12).

Figure 12: CloutMeter statistics for @ajaybarman.official, 7 November 2019 to 31 January 2020



Source: ASPI ICPC.

Saloni Gaur

Indian TikTok user who was censored at least three times on the platform.

Saloni Gaur is an undergraduate student of political science at Delhi University and a comedian who posts satirical videos under the *nom de guerre* 'Nazma Aapi'. She gained a sizable following on TikTok due to her videos about protests against the Citizenship Amendment Act and Delhi police's actions against protesters, but told ASPI ICPC she was censored at least three times on the platform.

On 23 April 2020, Gaur posted a satirical video about a feud between India's main opposition leader Sonia Gandhi and prominent journalist Arnab Goswami to TikTok, Instagram, Twitter and YouTube. The video uploaded to TikTok had its sound muted by the platform and its share link disabled.

Another video, posted by Gaur on 19 May 2020, in which she roundly criticised a news channel that she said was spreading hatred for Muslims, was also muted on the app before a frustrated Gaur deleted it. The comedian maintains that she never violated any of the app's community guidelines and the video remains on Instagram,[89] Twitter[90] and YouTube.[91]

On 30 May 2020, Gaur announced on Twitter that a video of hers in which she had joked about China's handling of Covid-19 as well as about the country's activities along its border with India in Ladakh had been removed by TikTok (Figure 13). Gaur's announcement caused a media storm and TikTok backed down, reinstating the video hours after it was taken down.

Figure 13: Tweet by Saloni Gaur

Source: Saloni Gaur. 'So @TikTok_IN has removed my last video which had jokes on China, the app is like the country, there's no freedom of speech', *Twitter*, 30 May 2020, online.

In response to Gaur's tweet, TikTok claimed that her video was 'reinstated after being flagged and a further review' that was done in the context of a 'a more rigorous review process' due to Covid-19. There was no explanation for the previous instances of apparent censorship of her account.

Feroza Aziz

US TikTok user who was censored by TikTok after posting about the plight of the Uyghurs in China.

In November 2019, TikTok found itself in a media storm for censoring the accounts of Feroza Aziz, an Afghan-American teenager who used 'make-up tutorial' videos to draw attention to the plight of Uyghurs interned in China's far-western Xinjiang region.

The three-part video series was disguised as a make-up tutorial to avoid being censored. In the videos, Aziz initially provides tips on eyelash curling as a ruse to discuss China's oppression and maltreatment of the Uyghurs. The first video was viewed more than 1.6 million times before TikTok blocked it and temporarily suspended her account.

TikTok blamed a 'human moderation error' for the removal of Aziz's video and asserted that the suspension was the result of an earlier satirical video of hers referencing Osama bin Laden being mistakenly flagged for violating the app's anti-terrorism policy.[92] Content moderation guidelines leaked to *The Guardian* two months before revealed that TikTok had been censoring 'highly controversial topics, such as separatism, religion sects conflicts, conflicts between ethnic groups', among other clauses.[93]

On 28 November 2019, Aziz confirmed on Twitter that her account had been unblocked but cast doubt on the company's explanations, writing 'Do I believe they took it away because of an unrelated satirical video that was deleted on a previously deleted account of mine? Right after I finished posting a 3-part video about the Uighurs? No.'[94]

WeChat censorship

The distortion of social and political discussion that's taking place on TikTok would be more than familiar to members of the Chinese diaspora who use WeChat, the Tencent-owned and -operated messaging app that has long been subject to strict censorship constraints.

Previous scholarship by the University of Toronto's Citizen Lab has demonstrated that WeChat operates different censorship systems for Chinese and overseas-based users.[95] According to its groundbreaking 2016 *One app, two systems* paper, content is censored for all users registered with Chinese phone numbers on the PRC-based version of the app Weixin, even if they travel overseas or switch to an international number.

Theoretically, under this dual system only Chinese users who register with a Chinese number and therefore use the sister app Weixin are meant to be heavily censored, while less restrictive rules apply for overseas users who access the same ecosystem using WeChat. While the two versions of the app operate on different servers, in practice, WeChat users have increasingly had their messages censored and their accounts disabled.

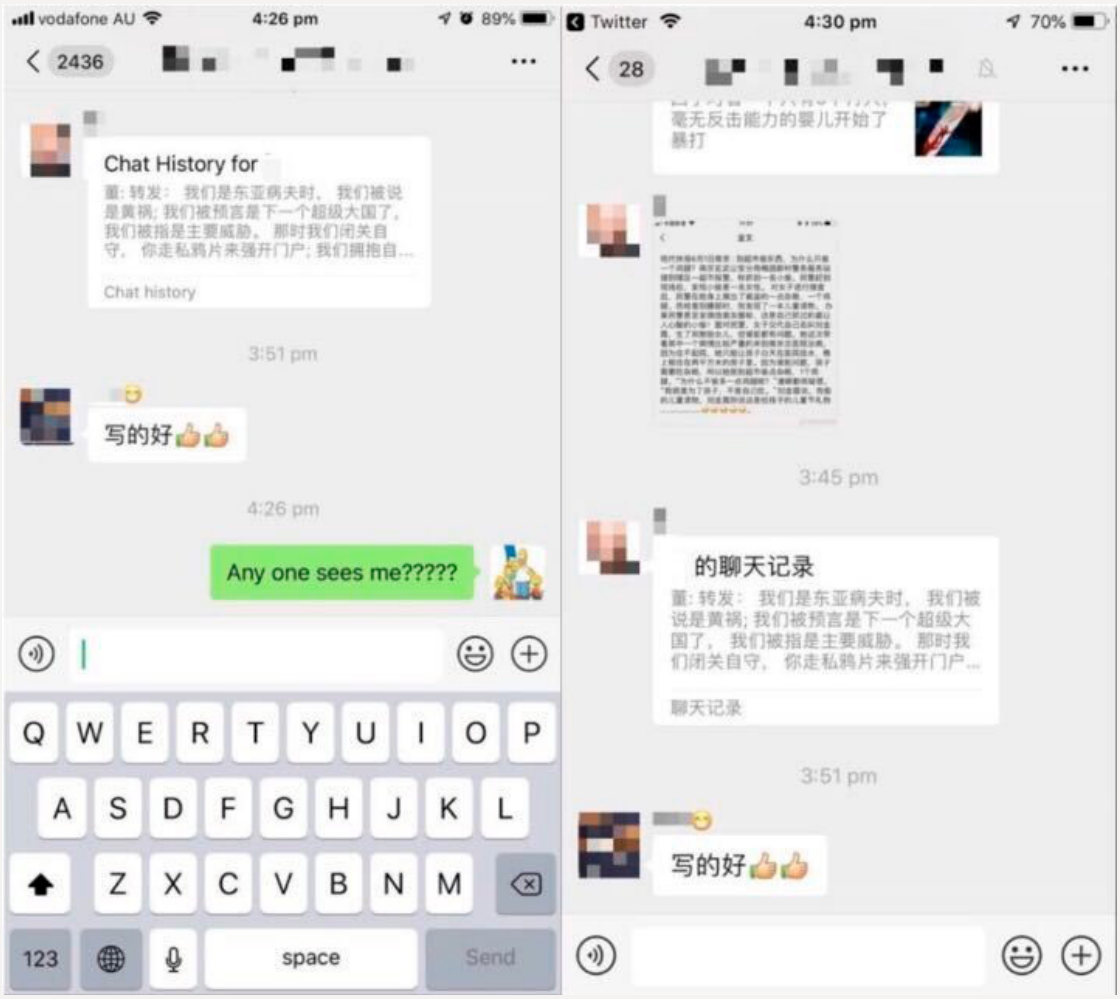
Zhou Fengsuo, a US-based activist and former Tiananmen student leader, told *Bloomberg Businessweek* that his WeChat account has been temporarily suspended numerous times over the past seven years. 'WeChat censorship is so obvious that people are no longer sensitive about it,' he told the magazine. 'My account is dealt with in the same way as Chinese accounts, which are under surveillance all the time.'

Zhou Fengsuo was also one of four WeChat users with whom *NPR* spoke regarding surveillance on the app. Although all four users are US citizens and registered with WeChat using US phone numbers, they're still blocked from sending certain messages in WeChat groups and have all had their accounts temporarily suspended.[96]

In fact, as a more recent Citizen Lab report revealed, both PRC-based users of Weixin and overseas users of WeChat are under constant surveillance. As Citizen Lab demonstrated in May 2020, the posts of WeChat users registered abroad are systematically surveilled, scanned for politically sensitive terms and used to train WeChat's political censorship system.[97] The platforms do this by 'screening images and documents shared by accounts registered outside China after they're sent, then add the digital signature—or "hash"—of any files deemed sensitive to a blacklist. Those files then cannot be sent or received by China-registered users.'

Australian WeChat user Yan Hang believes his Australia-registered WeChat account was suspended for sharing images related to the 30th anniversary of the Tiananmen Square massacre in 2019. He can only guess, because repeated attempts to seek clarification from WeChat owner Tencent were ignored. Before Yang was suspended, his messages in group chats were hidden from other users. A message sent by Yang to a group containing an ASPI researcher with a PRC-registered version of the app on 6 June 2019 was only visible on his own phone (Figure 14). Yan Hang received no indication or notification that such filtering was taking place.

Figure 14: A screenshot by Yan Hang of a message he posted to a WeChat group containing an ASPI researcher (left). Yan Hang's message wasn't visible on the ASPI researcher's PRC-registered version of the app (right)



Source: WeChat.

Yan Hang's experience mirrors that of dozens of WeChat users in the US, Canada, the UK, France, Spain, Australia, Germany and Malaysia interviewed by *VICE News*, who said their WeChat contacts in China weren't seeing any of their posts in group chats at the start of the Covid-19 outbreak in February 2020.[98] The restrictions placed on their accounts prevented them from sending information to contacts in China, and some international users also had their accounts suspended or blocked. WeChat users based in the US also reportedly had posts they made in approval of pro-democracy candidates in Hong Kong's elections in November 2019 censored and their accounts disabled.[99]

A Citizen Lab report published in August 2020, *Censored Contagion II*, tracked censored keywords related to Covid-19 on WeChat and found that WeChat censored 2,174 keywords between January 18 through May 14. Instances of censorship and surveillance of overseas users during the pandemic have been so numerous that Citizen Power Initiatives for China, a not-for-profit based in Washington DC, has teamed up with a law firm to launch a class action lawsuit on behalf of US WeChat users against Tencent.[100]

Tighter censorship, including this uptick in censorship of overseas users, followed a meeting of the Politburo on 3 February to discuss the epidemic. Two days after that meeting, a notice released by the Cyberspace Administration of China admonished a number of WeChat publications for having 'illegally

carried out reporting activities' and instructed the country's biggest internet companies, including Tencent and ByteDance, to 'conduct special supervision' on epidemic-related news.[101]

Censors soon began deleting messages and suspending accounts in large numbers, causing users to complain via the microblogging platform Weibo using the hashtag 'WeChat Blocked Account', posts which in turn were censored.[102] According to China Human Rights Defenders, as of 1 April, 206 of 897 arrests related to online posts regarding the Covid-19 outbreak were for materials published on WeChat.[103]

Under normal circumstances, WeChat operates a 'one app, two systems' system of censorship that distinguishes between PRC-based users of Weixin and foreign WeChat users, but, as the above cases highlight, Tencent can and does censor foreign users if Beijing decides 'special supervision' is required.

Harassment of dissidents and other overseas users

Several instances of the harassment of overseas Chinese—including those who aren't Chinese citizens—can be traced back to WeChat. Citizen Power Initiatives for China claims that 'the People's Armed Police uses the information provided by WeChat to harass, threaten, suppress, and prosecute the families of overseas Chinese activists.'[104]

In particular, Uyghurs living abroad face continued harassment and intimidation. The Chinese Government mobilises Chinese authorities to harass Uyghur-Americans via WeChat, often threatening to place family members in mass detention camps in Xinjiang.[105] One Uyghur-American who was previously contacted by Chinese Ministry of State Security agents told the Uyghur Human Rights Project, 'they are just telling us, "we are watching you. Wherever you go, still you are a Chinese." Even though abroad, it doesn't mean they can't do something to you. Because they have your friends, your relatives.'[106]

The severity of surveillance on Uyghurs is exemplified in the case of Erpat Eblekrem, a 24-year-old Uyghur who was sent to a 're-education' camp for using WeChat to contact his family members, who had left China.[107] In another instance, a US citizen and Uyghur activist was threatened by a man who identified himself as a 'high-ranking officer in China's security forces in the Xinjiang region'. After the activist's mother contacted him following her release from a mass detention camp, he received messages from the high-ranking officer via WeChat ordering him to quieten his reporting on the camps if he wanted his mother to be able to join him in the US.[108]

This consciousness of being watched even while abroad is also evident among Chinese university students studying outside of China. A survey conducted in 2017 by Cheryl Yu, then a graduate student in the US, found that, among 72 Chinese respondents from 31 American universities, 58% were aware of Chinese Government surveillance. One mode of government surveillance known to students abroad included the monitoring of WeChat accounts.[109]

When the *New York Times* spoke with a Chinese immigrant who had lived in Toronto before returning to China in 2018, she recounted her realisation during the 2016 US presidential election that WeChat is filled with 'gossip, conspiracy theories and lies'. Upon returning to China, however, she experienced the consequences of sharing sources from outside of WeChat on the app itself. She was taken into custody and interrogated regarding her WeChat contacts overseas.[110]

Instances such as these demonstrate the access that China's law enforcement has to WeChat and also exemplify the ways in which law enforcement collects information on overseas WeChat users tied to domestic Chinese residents.

The Chinese Government's apparent surveillance on WeChat manifests itself in self-censorship among WeChat users globally, ultimately creating a trap for many of its users. Due to WeChat's centrality in communication among Chinese diasporas, free speech implications aren't restricted to only those inside China's borders. In fact, WeChat's compliance with Chinese law enforcement enables the Chinese Government to track details of people who have left China, including details as specific as who they're meeting, at what time, and where.[111] Despite their physical location outside of China's borders, when a user is monitored on what they read, write and text and even where they go while abroad, that hinders their ability to access a free environment.

Political interference

WeChat is a powerful vector for influence in the politics of liberal democracies with sizable Chinese diasporas because it's a major source of news for those communities. So-called 'self-media' (*zi meiti*) publications have in recent years become extremely popular and influential on WeChat. They can be avenues for critical journalism—referred to as 'edge ball' content in China—that otherwise wouldn't be found in traditional media. More often, these publications are incentivised to chase clicks with sensational clickbait headlines. WeChat's tight censorship ensures that, for the vast majority of the time, these news sources only report news that serves the CCP's strategic objectives.

Aspects of WeChat's design exacerbate the misinformation problem that's produced in these publications. For instance, publishers are banned from embedding hyperlinks in their articles, making it difficult for readers to cross-reference any of the information they're receiving. For the most part, these publications are registered with Tencent via Chinese phone numbers, and basic details such as a physical address for their operations aren't made available.[112] Wu Bofeng, an employee at one of the largest WeChat public accounts in Australia, told *Quartz* that her publication takes its cues from Chinese state media and self-censors anything considered politically sensitive by the CCP.[113]

In addition to the platform's misinformation problem, there's widespread censorship. A 2018 study of Australian Chinese-language news sources on WeChat compared the output of three prominent news publications with that of the Australian Government-funded Special Broadcasting Service and found that there's little to no political coverage in them. Strikingly, none of the news sources published a single article on Chinese politics and foreign affairs from March 2017 till 1 August 2017. Even before the outlets stopped covering politics, the content they were running was largely copy-and-paste jobs from Chinese state media.[114]

The combination of clickbait news, tight censorship and the 'walled garden' in which WeChat users consume news almost entirely within the platform creates an environment in which even the members of the Chinese diaspora find themselves trapped in a mobile extension of the Great Firewall of China under which they're subjected to the same censorship and propaganda as PRC citizens.

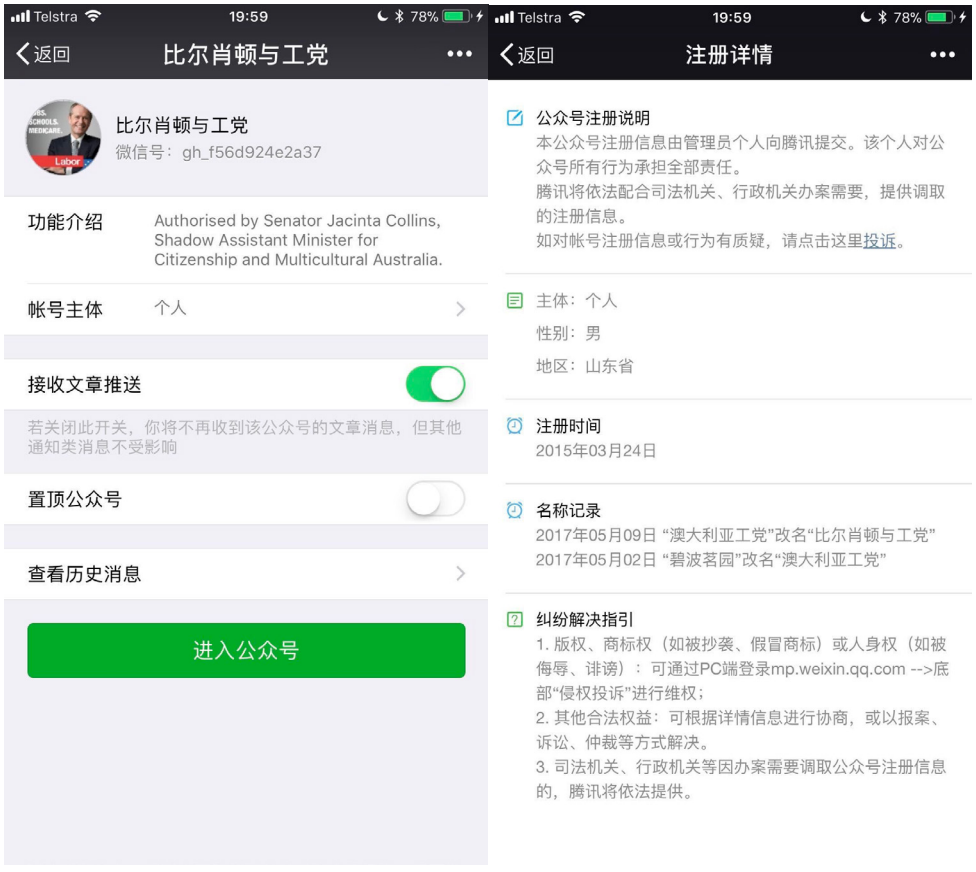
In liberal democracies around the world, WeChat is the primary organising platform for social and political campaigns conducted by the Chinese diaspora. In the US, the app helped propel an anti-affirmative-action movement led by conservative Chinese Americans.[115] In 2016, a demonstration

involving tens of thousands of people in more than 40 cities over the unfair prosecution of a Chinese-American police officer was largely organised on WeChat.[116]

During the 2019 Australian federal election, the WeChat publication 'Melbourne WeLife' featured a photo of then Labor opposition leader Bill Shorten with a made-up quote saying he planned to give 'green cards for all refugees'.[117] A doctored tweet purporting to come from Shorten's Twitter account stating 'Immigration of people from the Middle East is the future Australia needs' also circulated on the platform at the time. When Shorten's Australian Labor Party complained directly to Tencent about the proliferation of misinformation on the platform, the company didn't even respond.

Despite these issues, politicians in countries such as Australia, Canada, the US and New Zealand continue to flock to WeChat to communicate with their ethnic Chinese voters. In order to use official accounts with special functionality on the platform, many of these politicians use accounts set up and registered to Chinese citizens. As Chinese-registered accounts, they're subject to heavier censorship than those registered internationally. Australian Prime Minister Scott Morrison's official WeChat account is registered to an unknown Chinese citizen in Fujian Province.[118] A WeChat account for Bill Shorten, used during a crucial federal by-election in 2017 and again in the 2019 federal election, was registered to an unknown PRC national (Figure 15). Canadian Prime Minister Justin Trudeau's WeChat account is registered to an unnamed woman in Jiangsu Province.

Figure 15: The 'Bill Shorten & Australian Labor Party' WeChat account was registered in Shandong Province. It was a group for green tea drinkers before it was rebranded in May 2017



Source: WeChat.

Communications between politicians with their constituencies using these accounts are subject to CCP censorship by default. In September 2017, Canadian parliamentarian Jenny Kwan posted a WeChat message of support for Hong Kong's Umbrella Movement—a series of pro-democracy protests that took place in 2014—only to have it censored by WeChat.

Even if politicians' messages aren't censored, there's a real risk they could self-censor to stay on WeChat to reach key voters. In a live forum on WeChat during the 2019 federal election, Bill Shorten was asked 'a series of questions relating to Huawei, Chinese interference in Australia, the billionaire businessman and political donor Huang Xiangmo, and perceived negatives [*sic*] views of the Chinese Communist Party in Australia,' the ABC reported, adding that he didn't answer any of those questions.[119]

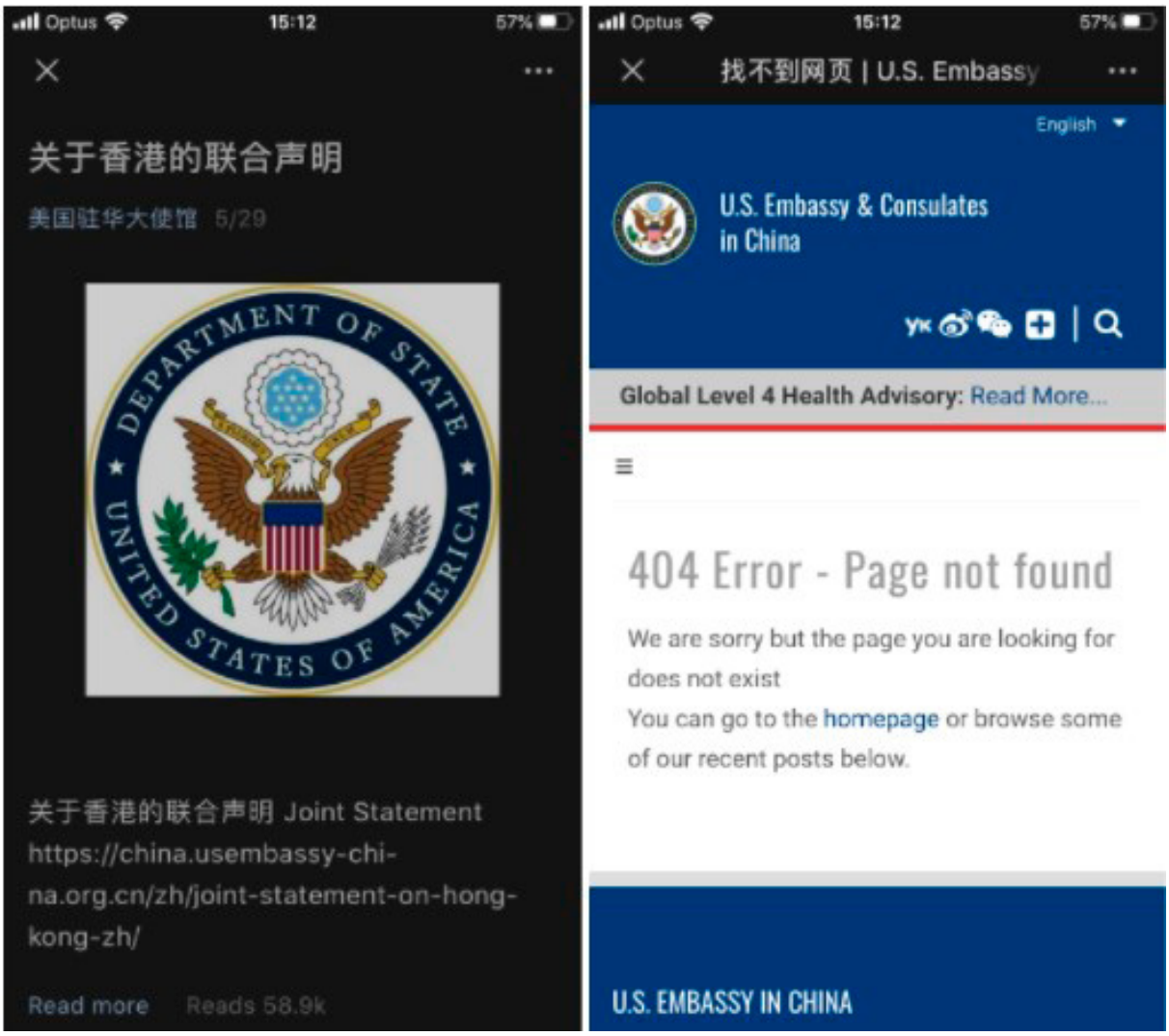
In addition to well-known politically sensitive topics such as the Tiananmen Square massacre and the plight of Uyghurs in so-called re-education camps in China, WeChat has censored a broad range of topics directly relevant to members of the Chinese diaspora. Those topics have included coverage of the US–China trade war, Huawei and the #MeToo movement, according to WeChatscope, which is a research project at the University of Hong Kong's Journalism and Media Studies Centre.[120]

Censorship of foreign countries' diplomatic posts on WeChat

In the same way that Chinese government departments, spokespeople, embassies and diplomats use Twitter and Facebook to promote messaging overseas, diplomatic missions in China use platforms like WeChat to promote messaging and publish official government statements. Our research has found that WeChat posts published by the US, UK and Indian diplomatic missions to China are being censored in several ways, and that the bulk of this censorship took place after the global spread of Covid-19 (specifically, from April 2020).

We found 14 cases of censored posts on the US Embassy's account, 11 of which were published in 2020 alone. We detected three different levels of censorship of the account. The most common one is an alteration of links intended to direct to the embassy's website. The US Embassy often publishes briefs on WeChat and then adds a 'Read more' tab at the bottom of the post. While most of those links work across the embassy's account, several links related to topics sensitive to the CCP are faulty and redirect to a '404 not found' page (Figure 16).

Figure 16: WeChat post mentioning a diplomatic joint statement on Hong Kong (left) and censored statement (right)



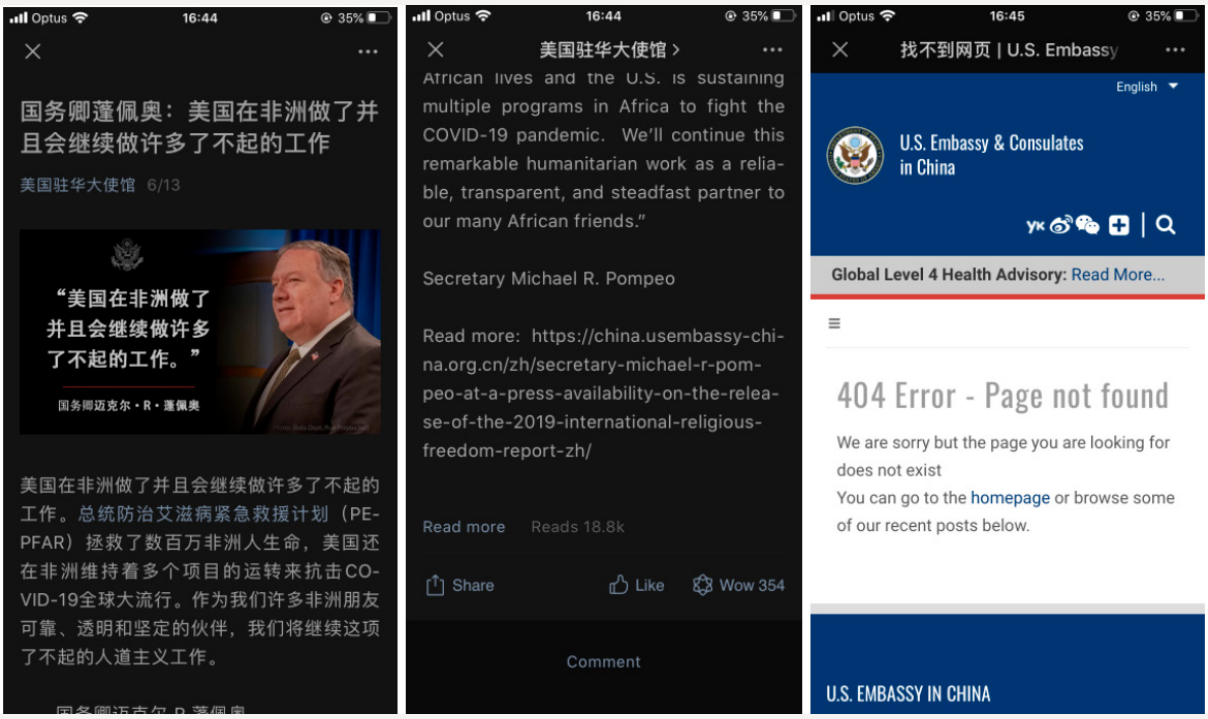
Source: WeChat.

Among the censored topics are the new national security laws imposed on the city of Hong Kong, disputes in the South China Sea and China's mishandling of the coronavirus pandemic, as well as a mention of the late Dr Li Wenliang, whose death sparked public outrage and became a symbol of China's failure to address the spread of Covid-19.[121]

Another widespread method by which WeChat censors sensitive diplomatic statements is by disabling the share function on those posts. Posts that received this particular type of censorship are related to the US's China policy and the US–China trade war.

The topic that we found to be the most heavily censored is religious freedom and the CCP's persecution of the Uyghurs and other ethnic minorities (Figure 17). In fact, we found three occasions in which posts mentioning the Uyghurs are censored on the US Embassy's WeChat account. In one case, the 'Read more' tab redirects to a '404 not found' page and the sharing function is disabled. In two other cases, the censorship concerns only the sharing function.

Figure 17: WeChat post mentioning a statement on religious freedom (left and centre) and censored statement (right)



Source: WeChat.

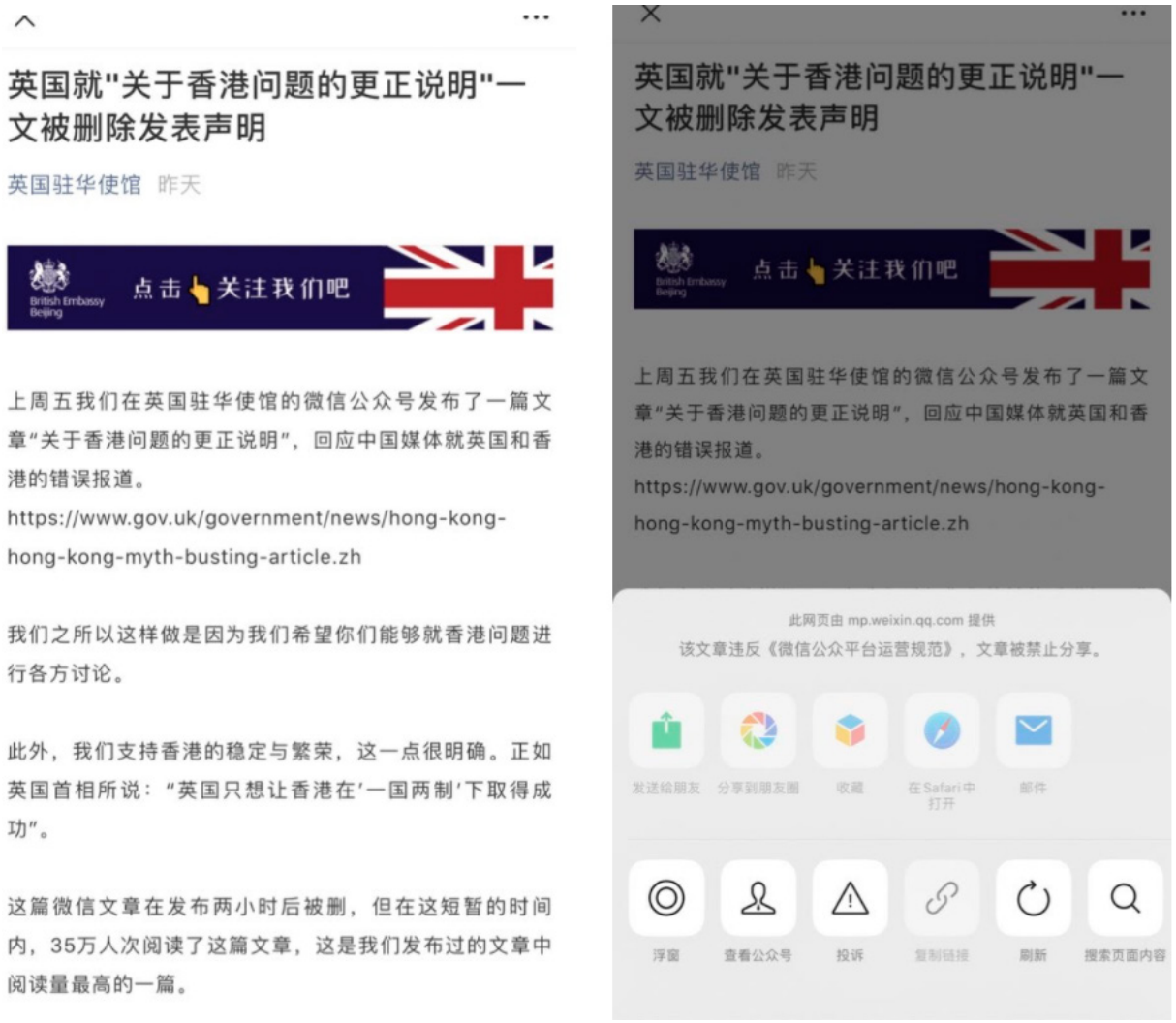
We also found one instance in which the ‘Read more’ tab redirects to an English article, despite the embassy’s posted link being to the same article, but in Chinese. In this case, the article is related to the US Government’s designation of Confucius Institutes as Chinese diplomatic missions.

The number of censored posts on the US Embassy’s account drastically increased during Covid-19. In fact, ASPI detected no instance of censorship between June 2019 and April 2020 and then found 11 cases of censorship between April and August 2020. The uptick in censorship frequency comes as tensions between the US and China continue to escalate, especially in relation to issues such as Covid-19, Hong Kong, human rights, trade and the South China Sea.[122]

In addition, we detected two censored posts on the British Embassy’s WeChat account. On 19 June, the embassy published an article on its WeChat official account in response to Chinese media reports.[123] The article aimed to dismantle ‘misinformation’ about the involvement of the UK in the Hong Kong issue. It was read more 350,000 times within two hours and then censored by WeChat.[124]

On 29 June, the embassy published another article, titled ‘Hong Kong response is censored’,[125] that denounced the incident and further explained the UK’s position on Hong Kong (Figure 18). This time, the post wasn’t removed, but its sharing function was disabled.

Figure 18: UK Embassy's WeChat post in response to censorship of Hong Kong post (left). All sharing functions are disabled (right)



Source: Bill Birtles. 'WeChat diplomacy: British embassy statement on #HongKong gets deleted, so it reposts with headline explaining it was censored and had high user engagement. WeChat this time leaves it up but bans users from sending it to others or posting it on their moments', *Twitter*, 30 June 2020, online.

Finally, several Indian media outlets have reported that an 18 June speech by Prime Minister Narendra Modi about the clashes between the Indian and Chinese armies at the contested Ladakh border had been censored from the Embassy of India in Beijing's official WeChat account.[126] Embassy officials reported that WeChat removed the post for 'divulging state secrets and endangering national security'.[127]

We have contacted all three embassies to verify our findings. A US Embassy spokesperson confirmed that it 'did not delete or alter the WeChat links'. An official from the British Embassy said, 'the Hong Kong WeChat article was the first time that we have used this account to talk about "sensitive" topics and the first time we have been censored on this channel. The follow up article we wrote on the censorship was also censored with people stopped from sharing it.'

We didn't receive a response from the Indian Embassy in Beijing.

The censored articles on the US Embassy's WeChat account that we found are listed in Table 1, in reverse chronological order from the most to least recent.

Table 1: Censored articles on the WeChat account of the US Embassy in Beijing

Title	Translation	Date	Censorship method	Source
美国国务院将孔子学院美国中心认定为中华人民共和国驻外使团	The US State Department designated the Confucius Institute US Center as a diplomatic mission of the PRC	14 August 2020	'Read more' tab redirects to English article[a]	Online[b]
国防部长埃斯帕出席香格里拉对话视频会议时发表讲话	Defense Minister Esper delivered a speech during the video conference at the Shangri-La Dialogue	25 July 2020	'Read more' tab redirects to a 404 error page[c]	Online[d]
[摘译] 常务副国务卿比根在参议院外交关系委员会的讲话	Deputy Secretary Biegun's remarks to the Senate Foreign Relations Committee	23 July 2020	Sharing function disabled	Unavailable[e]
蓬佩奥国务卿就联合国人权理事会发表声明	Secretary of State Pompeo issued a statement on the UN Human Rights Council	22 June 2020	'Read more' tab redirects to a 404 error page[f]	Online[g]
国务卿蓬佩奥：美国在非洲做了并且会继续做许多了不起的工作	Secretary of State Pompeo: The US has done and will continue to do a lot of great work in Africa	13 June 2020	'Read more' tab redirects to a 404 error page[h]	Online[i]
在出席2019年度国际宗教自由报告新闻发布会时发表的讲话	Speech at the press conference of the 2019 International Religious Freedom Report	11 June 2020	Sharing function disabled	Unavailable[j]
关于香港的联合声明	Joint statement on Hong Kong	29 May 2020	'Read more' tab redirects to a 404 error page[k]	Online[l]
国务卿蓬佩奥声明：美国保护国家安全和5G网络的完整性	Secretary of State Pompeo stated: The US protects national security and the integrity of 5G networks	18 May 2020	'Read more' tab redirects to a 404 error page[m]	Online[n]
国务卿蓬佩奥在出席记者会时发表的讲话	Speech by Secretary of State Pompeo at press conference	8 May 2020	'Read more' tab redirects to a 404 error page[o]	Online[p]
布兰斯塔德大使谈世界知识产权日：为了更光明的未来，强化知识产权保护	Ambassador Branstad on World Intellectual Property Day: Strengthening intellectual property protection for a brighter future	25 April 2020	'Read more' tab redirects to a 404 error page[q]	Online[r]
国务卿蓬佩奥在记者会上发表讲话	Secretary of State Pompeo delivered a speech at press conference	24 April 2020	'Read more' tab redirects to a 404 error page[s]	Online[t]

Title	Translation	Date	Censorship method	Source
布朗巴克大使在《国际宗教自由报告》发布会上的讲话	Ambassador Brownback's speech at the press conference of the International Religious Freedom Report	25 June 2019	Sharing function disabled	Unavailable[u]
塞缪尔•布朗巴克大使关于确认宗教自由表现的特别简报会 (摘译)	Special briefing by Ambassador Samuel Brownback on confirming religious freedom designations (excerpt)	13 December 2018	Sharing function disabled	Unavailable[v]
新闻秘书关于总统与中方共进工作晚宴的声明	Press Secretary's statement on President's working dinner with China	2 December 2018	Sharing function disabled	Unavailable[w]

a Michael R Pompeo, 'Designation of the Confucius Institute US Center as a Foreign Mission of the PRC', US Embassy and Consulates in China, 13 August 2020, online.
b US Embassy Beijing (美国驻华大使馆). 'The US State Department recognised the Confucius Institute's American Centre as a diplomatic mission of the People's Republic of China' (美国国务院将孔子学院美国中心认定为中华人民共和国驻外使团), *Weixin*, 13 August 2020, online.
c Archived link, online.
d US Embassy Beijing (美国驻华大使馆). 'Defense Minister Esper delivered a speech at the Shangri-La Dialogue Video Conference' (国防部长埃斯帕出席香格里拉对话视频会议时发表讲话), *Weixin*, 25 July 2020, online.
e When the sharing function is disabled, it's impossible to retrieve the links to the WeChat post.
f Archived link, online.
g US Embassy Beijing [美国驻华大使馆], 'Secretary of State Pompeo issued a statement on the UN Human Rights Council' (蓬佩奥国务卿就联合国人权理事会发表声明), *Weixin*, 22 June 2020, online.
h Archived link, online.
i US Embassy Beijing (美国驻华大使馆). 'Secretary of State Pompeo: The United States has done and will continue to do a lot of great work in Africa' [国务卿蓬佩奥 : 美国在非洲做了并且会继续做许多了不起的工作], *Weixin*, 13 June 2020, online.
j When the sharing function is disabled, it's impossible to retrieve the links to the WeChat post.
k Archived link, online.
l US Embassy Beijing (美国驻华大使馆). 'Joint statement on Hong Kong' (关于香港的联合声明), *Weixin*, 29 May 2020, online.
m Archived link, online.
n US Embassy Beijing (美国驻华大使馆). 'Secretary of State Pompeo stated: The United States protects national security and the integrity of 5G networks' (国务卿蓬佩奥声明 : 美国保护国家安全和5G网络的完整性), *Weixin*, 18 May 2020, online.
o Archived link, online.
p US Embassy Beijing (美国驻华大使馆). 'Speech by Secretary of State Pompeo at Press Conference' (国务卿蓬佩奥在出席记者会时发表的讲话), *Weixin*, 8 May 2020, online.
q Archived link, online.
r US Embassy Beijing (美国驻华大使馆). 'Ambassador Branstad on World Intellectual Property Day: Strengthening intellectual property protection for a brighter future' (布兰斯塔德大使谈世界知识产权日 : 为了更光明的未来 · 强化知识产权保护), *Weixin*, 25 April 2020, online.
s Archived link, online.
t US Embassy Beijing (美国驻华大使馆). 'Secretary of State Pompeo delivered a speech at press conference' (国务卿蓬佩奥在记者会上发表讲话), *Weixin*, 24 April 2020, online.
u When the sharing function is disabled, it's impossible to retrieve the links to the WeChat post.
v When the sharing function is disabled, it's impossible to retrieve the links to the WeChat post.
w When the sharing function is disabled, it's impossible to retrieve the links to the WeChat post.

TikTok privacy concerns and data collection

China's access to TikTok data

In TikTok's early years of operation, data was sent to and processed in China–a fact the company has admitted to. [128] The extent to which TikTok user data was sent to the PRC is the subject of a class-action lawsuit, brought by a California college student in December 2019 that alleges that TikTok 'vacuumed up and transferred to servers in China vast quantities of private and personally-identifiable user data'.[129]

Despite admitting that some TikTok user data was processed in China, ByteDance also argued that:

> there's a difference between data being physically processed in China and data being processed by systems designed and operated by one of our China registered entities. As a general practice, TikTok is not a service offered in China and as a result there has not been personal and un-aggregated data physically processed there.[130]

Growing public concern over TikTok's data at the time saw the platform employ contractors from a cybersecurity firm to assess its app's source code and data storage practices.[131] The cybersecurity firm conducted analysis from July to October 2019, for which it interviewed TikTok employees and reviewed the app's source code. According to the vice president of the firm, his team 'found no way TikTok could send data to China during those months'.[132] The assessment only lasted for the duration declared by the vice president, and the statement only addresses data being sent *to* the PRC, not whether it's being accessed *from* the PRC.

In an April 2020 blog post, TikTok's Chief Information Security Officer, Roland Cloutier, said that TikTok's goal was to minimise China-employee access to TikTok user data (for example, from the US and the EU).[133] He failed to mention, however, whether TikTok intended to cease such regional data access.

It isn't clear whether or not TikTok intends to cease non-US access to the data in the near future. In a lawsuit that TikTok and ByteDance filed against the Trump administration, TikTok stated that it had erected 'software barriers' around US user data stored outside China to separate the data from other ByteDance products. However, software barriers still permit ByteDance's China-based engineers supporting TikTok to gain controlled access to decrypted US user data, which includes names, birthdays, home addresses, phone numbers, emails, passwords, PayPal account information, contact lists, private videos, direct messages and parts of the log-in history.[134]

ByteDance couldn't realistically refuse a request for TikTok user data. China has a suite of national security laws that effectively compel individuals and companies to participate in 'intelligence work'. Alibaba, which provides cloud services to TikTok in Singapore, also falls under those laws. For example, Article 7 of the National Intelligence Law states that: 'Any organisation and citizen shall, in accordance with the law, support, provide assistance, and cooperate in national intelligence work, and guard the secrecy of any national intelligence work that they are aware of. The state shall protect individuals and organisations that support, cooperate with, and collaborate in national intelligence work.'[135] In other

words, if the Chinese Government requested TikTok user data, the company would be required by law to assist the government and then would be legally prevented from speaking publicly about the matter.

Like all major Chinese tech companies, ByteDance headquarters in Beijing houses a Chinese police cybersecurity team, according to the *Wall Street Journal*.[136] That arrangement allows employees to hand over user data and other sensitive information without due process.

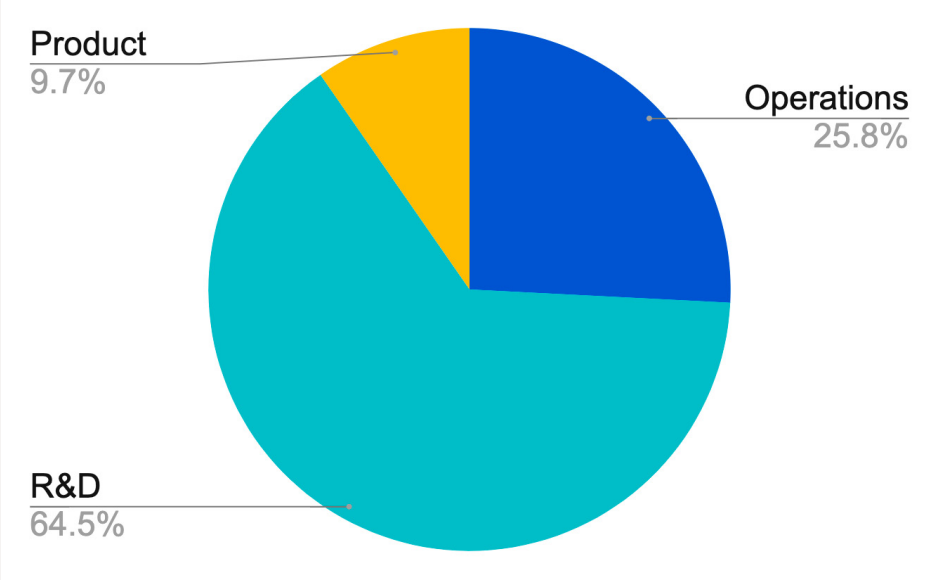
According to three sources cited by *Reuters*, PRC-based engineers support TikTok as well as its Chinese equivalent, Douyin. Both TikTok and Douyin share some infrastructure, making any complete separation 'nearly impossible'.[137] This is congruent with findings reported in a July 2020 article by *The Information* that says China-based engineers and researchers developed TikTok's core software code. This source code, which is shared with other ByteDance apps, is known internally as *zhongtai*, or 'central platform', and so detaching TikTok from ByteDance would be 'a time-consuming and difficult maneuver'.[138] This may help to explain TikTok's reluctance or difficulty in fully separating from its Chinese support engineers.

The Information also revealed that ByteDance has made efforts to remove China-based engineers' access to US-based servers on certain projects with limited success. The difficulties associated with limiting access to those engineers are exemplified in one project, conducted in early 2020, which faced technical problems that couldn't be solved by the company's overseas engineers. As a result, temporary access was reinstated to the China-based engineers. Another challenge facing engineers outside China is that the software used to manage these servers is developed in China and written mainly in Chinese, making it difficult for TikTok's non-Chinese-speaking employees to know how the servers are managed.

In line with efforts to separate TikTok's engineering team from China, a small engineering corps has been established in Mountain View, California. However, instead of reporting to the TikTok CEO in the US, the engineers report to senior executives at ByteDance in China (Yang Zhenyuan and Hong Dingkun).[139] Although TikTok's engineering team both inside and outside China previously reported to managers in China, as of May 2020 ByteDance was in the process of recruiting an executive to run the US-based engineering department.[140]

As is evident from ByteDance's efforts to separate the US and China engineering departments, the company has made a series of moves to steadily decouple TikTok from its China operations. By August 2020, only 22 PRC-based jobs were being advertised by ByteDance, of which a mere three were for content-related positions in the Middle East, Latin America and the eastern EU (Figure 19).[141] Instead, most of the remaining PRC-based TikTok positions were for R&D, such as roles for a senior software engineer responsible for the app's content recommendation system, as well as a product manager responsible for TikTok's search function.[142] Despite ByteDance continuing to advertise for those PRC-based positions, particularly for R&D, it is evident that the TikTok Careers job page has instead become the primary platform for advertising TikTok positions.

Figure 19: Distribution of PRC-based TikTok positions advertised by ByteDance and TikTok



Note: Several of the jobs analysed in this chart are listed in Appendix 4. Source: ASPI ICPC.

As a result of efforts to increase the divide between TikTok and its parent company, TikTok has been on a hiring blitz for engineers, strategists and executives around the world.[143] In the US, it tripled the number of its US-based employees in 2020 and plans to add another 10,000 jobs over the next three years, according to the company.[144] Before these changes, there was a 'free flow of colleagues from China coming into the LA office or vice versa', as described by a TikTok US content team member in 2019.[145] Meanwhile, ByteDance employees in the PRC are now required to write all TikTok-related internal documents in English.[146]

ByteDance's decision to dissolve its Beijing-based Trust and Safety (TnS) Department in March 2020 signalled another action the company was taking to separate TikTok from its Chinese operations. The TnS Department in Beijing was responsible for TikTok's content moderation system and employed approximately 100 employees, most of whom each had capabilities in three different languages.[147]

Based on the company's careers page, TikTok positions associated with the TnS Department are now located throughout the US, Dublin, London, Berlin, Singapore, Moscow and Seoul. By August 2020, only one Beijing-based TnS Department position remained, for an algorithm engineer responsible for the 'ByteDance short-video algorithm, including content understanding and user modeling'.[148] Previously in May, however, that same job ad stated that the hire would be 'responsible for the content understanding and user modeling of ByteDance's overseas products (TikTok, Vigo …)'.[149]

User privacy – Technical observations

Our primary privacy concerns with TikTok, outside Bytedance engineers access to TikTok data, lies in the amount of data collected by TikTok as defined in their Privacy Policy, and in the data that we were not able to see during our technical analysis. This included items that were encrypted, code that was obfuscated, and the fact that we only inspected TikTok from the client-side (the Android apps and the web platform TikTok.com). We did not investigate or have access to any of TikTok's internal systems.

Over the course of a few months, we have observed TikTok's platform evolve. Of TikTok's two Android packages,[150] we conducted a time-boxed analysis on com.zhiliaoapp.musically v17.3.3 (v17), the version available in Australia, and compared it with our observations from previous versions and packages of the app as well as the web platform.

Between v15 and v17, we observed that ongoing public scrutiny of TikTok has seen TikTok's apps generally reduce their data collection types, collection frequency as well as the number of permissions they request. We also observed in v17 that code had been cleaned up to remove references to Chinese domains, IP addresses and developer comments in Chinese. We found that the US version is faster to implement and resolve privacy issues than the rest-of-world app.

These moves put TikTok more in line with collection practices of other large-data driven AI companies that partake in targeted advertising revenue. For example, TikTok collects a large amount of data from its users as is stated in the company's privacy policy. The data collected ranges from individual tracking information to messages and related metadata.

During our analysis we did not observe v17 carrying out any overtly malicious activity (akin to spyware). One questionable outlier relates to TikTok's collection of "keystroke patterns or rhythms" as per their Privacy Policy. The app has a relatively large and obfuscated code base, and some encrypted transmissions that were inaccessible to us. There are parts of the app we did not have time to cover that are worth investigating further. These have been outlined in Appendix 2 and primarily cover areas where there are potential for security vulnerabilities.

Data collection and logging

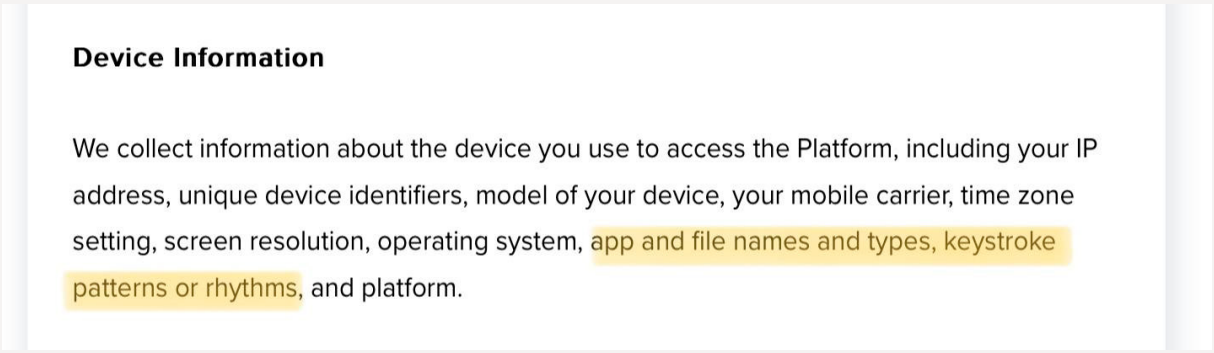
To observe data collected by TikTok we used a HTTP web proxy to intercept and view data sent from the device with TikTok app installed on it. This allowed us to observe what kind of data was being sent, when it was being sent, and determine the pattern of data transmission.

Analysing the traffic from v17, we saw that all transmissions were encrypted. But we noticed that the data of some requests were curiously encrypted beneath this already encrypted transmission channel. It is industry best practice to encrypt the transmission with TLS so that user information is protected, however it is unusual for an app to encrypt the data beneath this secure link as well. We were unable to determine why this extra encryption was necessary and only implemented for data sent to particular servers.

The remaining TikTok servers did not encrypt their underlying data and we observed user and device identifiers sent with every request. This type of data is likely used for tracking individuals and their actions on the platform. This also occurs on the web platform. For some examples, see Appendix 2.

TikTok's Privacy Policy says that it collects "keystroke patterns or rhythms". In our analysis of the source code we identified a number of locations where KeyEvent parameters are being passed to various functions. KeyEvents are Java objects that hold keystroke information. The (KeyEvent keyEvent) format is commonly used in, but not exclusively by, keyloggers. It depends on how the KeyEvent is used. However due to the time limitations we did not investigate all instances of this parameter. Additionally, and due to the double layer of encryption of some TikTok traffic, we were not able to verify whether or not the recorded keystrokes are being transmitted out of the app, or how the keystroke data is being used.

Figure 20: Extract from TikTok's privacy policy, 1 January 2020



Device Information

We collect information about the device you use to access the Platform, including your IP address, unique device identifiers, model of your device, your mobile carrier, time zone setting, screen resolution, operating system, app and file names and types, keystroke patterns or rhythms, and platform.

Source: 'Legal—Privacy Policy', TikTok, 1 January 2020, online.

In v15 of the app, although the privacy policy (depicted in the above image) was applicable, TikTok did not explicitly state it was collecting the details of the local network used by the device, including any web proxies or virtual private networks (VPNs) used in the network (see Appendix 2). This information is sensitive, as it discloses data about the network architecture in use on the device. Version 17 still collects internal internet protocol (IP) addresses and domain name system (DNS) addresses, and contains Appsflyer software development kit (SDK) code that is specifically checking for the use of a 'tun0' interface (see Appendix 2), which is often used by VPNs.

This is not the first time third-party libraries have caused privacy concerns. In March 2020, it was discovered that TikTok, along with other developers, were identified to be reading the user clipboard on iOS (the Apple operating system) - a practice that could lead to sensitive user information such as credit card details and passwords being captured by the app. In March TikTok told The Telegraph that they would disable clipboard-reading in the coming weeks,[151] but a new feature in iOS 14 showed that TikTok was still monitoring the clipboard in June.[152] Researchers discovered that TikTok read the clipboard everytime the app was opened.[153] According to a TikTok blogpost at the end of June, the issue was caused by a third-party SDK and a self-developed anti-spam feature and it has since resolved the issue.[154]

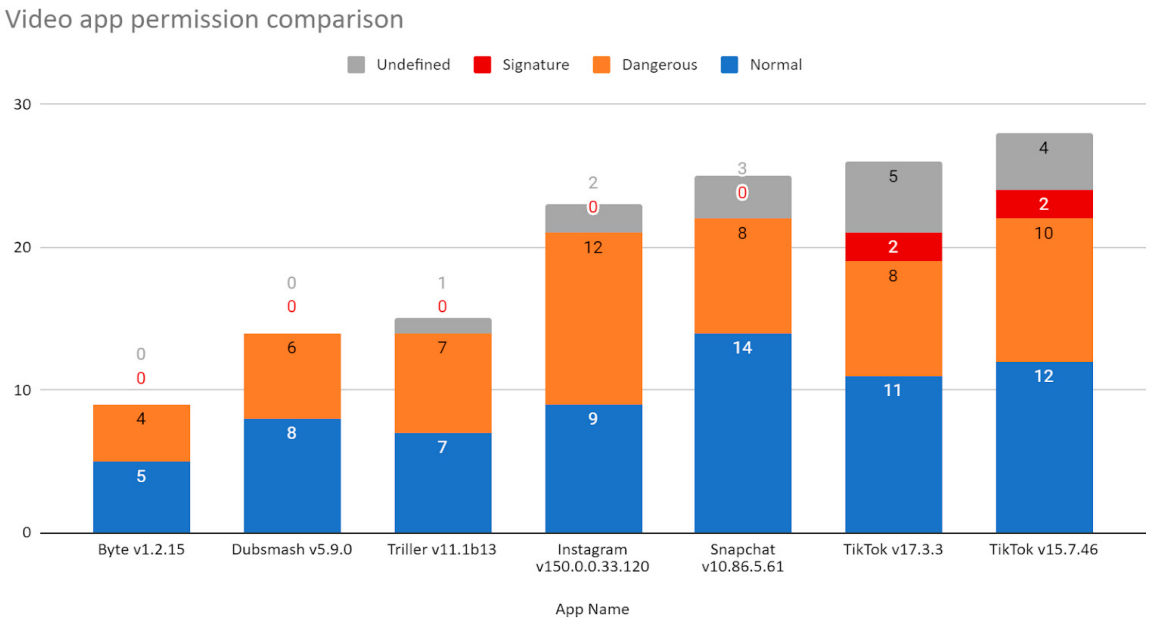
TikTok has progressively cleaned up some of its code, but only after lawsuits and continual media attention. Late last year TikTok was found to be collecting a significant amount of user information using a variety of methods. To uniquely identify users, it used audio and canvas fingerprinting (a method that combines hardware and browser characteristics)[155] and through the app, collected device MAC addresses (a unique network card hardware identifier), a method that the Wall Street Journal reports was banned by Google.[156] And, in a class action lawsuit filed in November 2019, the plaintiff alleges that TikTok used device identifiers including phone IMEI (international mobile equipment identity) and IMSI (international mobile subscriber identity) numbers,[157] and sent the data to China. As of August 2020, according to our own research, the latest iterations of both the app and the web platform, appear to have ceased all these practices.

Further trying to distance itself from China, Tiktok has removed references to domains and IPs in China in v17, which were present in v15 and v16.[158] But traffic from the app does go to servers in Singapore hosted by Alibaba's cloud and to servers in the US, hosted on ByteDance's network,[159] both with parent companies in China. TikTok's own privacy statement states that TikTok user data may be shared "with a parent, subsidiary, or other affiliate of our corporate group."[160]

App permissions

Permissions define what an app can do or access on a device. We compared the standard Android permissions of TikTok and its short-form video competitors - Byte, Dubsmash, Triller, Instagram and Snapchat. TikTok declares slightly more permissions than its competitors (see Figure 21). But a noticeable difference is its declaration of two permissions with a “signature” level of protection level. These are higher-risk permissions, but to determine how these permissions are used would require more analysis of the application. See Appendix 2 for more detail.

Figure 21: A comparison of the permission list of six different short video apps (Byte, Dubsmash, Triller, Instagram, Snapchat, TikTok).



Source: ASPI ICPC. See Appendix 2 for methodology

Protection Level

Normal: A lower-risk permission. The system automatically grants this type of permission to a requesting app at install time.

Dangerous: Permissions that could potentially affect users’ privacy or device operation. The user must explicitly grant the permission to the app.

Signature: Higher-risk permission. Granted to an app at install time, but only when the app that attempts to use the permission is signed by the same certificate as the app that defines the permission.

Undefined: Permissions where we could not find official Android or developer-written documentation on protection level

TikTok has made an effort to reduce its permission list which does reduce the risk of misuse. Between version 15 and version 17, it standardised the permission list between the two packages of its app and removed permissions to obtain user locations, modify accounts and monitor the phone state.[161] The user’s approximate location is still collected and still forms part of the options used for targeted

advertising to TikTok users. The information probably comes from the device details that are logged by the TikTok app, which include SIM card operator details, system region and time zone. It may be possible that the user's IP address, which is collected by TikTok,[162] could also be used for this purpose.

WeChat privacy concerns and data collection

The primary privacy concern with WeChat stems from the amount of personal user, device and platform data it has access to through the legitimate functionality it provides. The vulnerability then becomes the ability of a third party to intercept this data due to a lack of end-to-end encryption on the app.

We conducted a time-boxed analysis of the WeChat app (v7.0.16) and its traffic targeting any privacy or security concerns. We also looked at how the Official Account Platform censorship might be occurring to aid in discovering any other cases.[163] We found its extensive list of permissions concerning, as well as code that may lead to keylogging and clipboard monitoring code both of which will require further investigation to verify. The codebase of the WeChat app is large, obfuscated and it communicates using a custom protocol. All of which contributes to the difficulty and time-intensive nature of getting a clear picture of its capabilities.

App permissions and data collection

The WeChat Android app declares 72 permissions. This is extensive. With those permissions, the app is able to carry out actions such as recording audio, getting the Wi-Fi MAC address, identifying network operator related data, reading the device ID (for example, the IMEI), querying the phone location (GPS) and monitoring the phone (user's) physical activity. While recording audio, obtaining the user's location and activity monitoring are required for the functions offered by the app, the others serve to uniquely identify the user.

The danger with permissions is that they may be misused, if not by the app itself, the potential is there for third-party code within the app to misuse the permissions. For instance, while activity monitoring would be a required permission for WeRun (WeChat's fitness activity tracker), the permission enables an app to classify a user's physical activity, such as whether they're walking or biking but also whether they're moving in a vehicle. Once the app is granted this permission, any code within the app can use the permission.

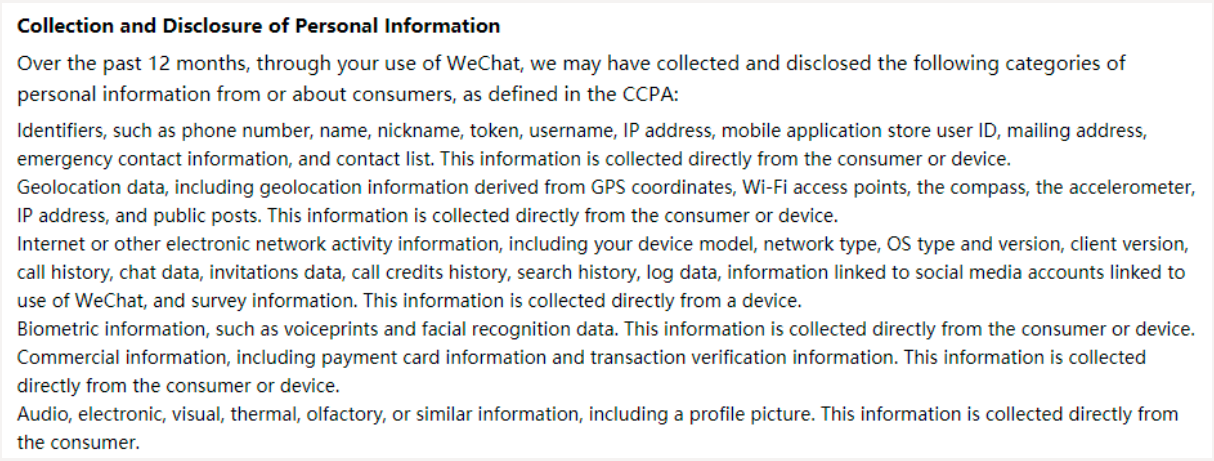
During our technical investigations into the WeChat app, our ability to evaluate the integrity of chat data and observe what data was logged by the app was relatively low due to the implementation of WeChat's custom protocol, called 'mmtls', which we didn't decrypt.

We identified that the app was collecting the device identifiers including device model, operating system, IMEI, IMSI and contained code to retrieve network interface information. Further to this we identified 5 places in the code where the clipboard can be read by the app. Although this is a common functionality in a chat messaging application, at this time we have not been able to verify whether or not the code at these locations is being used or whether the clipboard data is being sent to WeChat servers.

The extent of data that WeChat is capable of collecting can be seen in WeChat's privacy policy under the section addressing the California Consumer Privacy Act (Figure 22). It includes user and device identifiers and other information collected from the user. Phrases such as 'electronic network activity information' and 'similar information' are ambiguous about what conduct those terms cover. Of particular concern is chat data, as the privacy policy states that WeChat doesn't permanently store

chat data on their servers, but in this section (in Figure 22) it suggests that this data is disclosed by WeChat. A curious and rather suspicious admission by WeChat is the possible collection of thermal and olfactory information from the user. While it's possible to obtain ambient temperature, device temperature, relative humidity and ambient air pressure from the device's environmental sensors, it isn't clear how or why olfactory information is obtained.

Figure 22: WeChat's privacy policy shows the information from users in California that WeChat may collect and disclose



Collection and Disclosure of Personal Information

Over the past 12 months, through your use of WeChat, we may have collected and disclosed the following categories of personal information from or about consumers, as defined in the CCPA:

Identifiers, such as phone number, name, nickname, token, username, IP address, mobile application store user ID, mailing address, emergency contact information, and contact list. This information is collected directly from the consumer or device.
Geolocation data, including geolocation information derived from GPS coordinates, Wi-Fi access points, the compass, the accelerometer, IP address, and public posts. This information is collected directly from the consumer or device.
Internet or other electronic network activity information, including your device model, network type, OS type and version, client version, call history, chat data, invitations data, call credits history, search history, log data, information linked to social media accounts linked to use of WeChat, and survey information. This information is collected directly from a device.
Biometric information, such as voiceprints and facial recognition data. This information is collected directly from the consumer or device.
Commercial information, including payment card information and transaction verification information. This information is collected directly from the consumer or device.
Audio, electronic, visual, thermal, olfactory, or similar information, including a profile picture. This information is collected directly from the consumer.

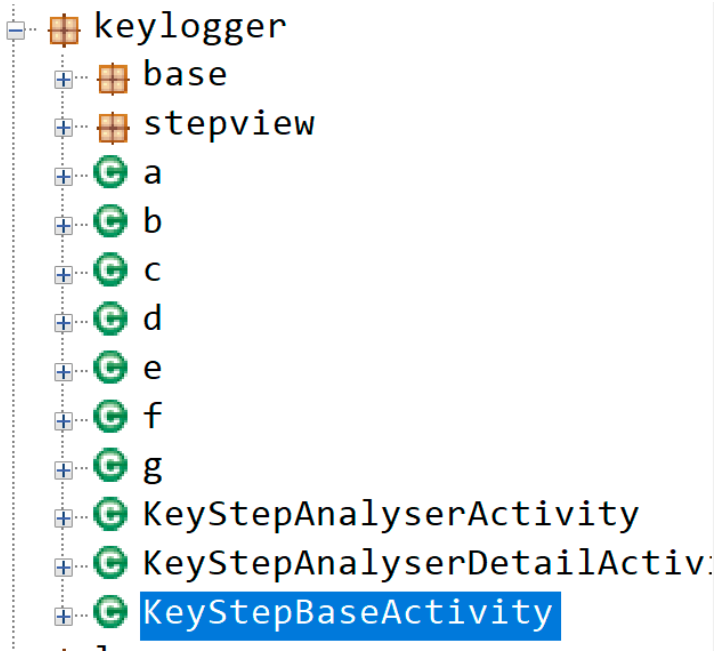
Source: WeChat privacy policy, under the heading 'Addendum for California residents'.

Security

The findings of our technical analysis aren't comprehensive, and we have identified several areas of concern worth further investigation. During the sign-up process, for example, the WeChat app downloaded an .apk file (Android package file). While no malicious behavior was identified, and it's possible this is related to software updates, this activity is unusual and deserves further investigation as to why WeChat is downloading this file and what it is being used for.[164]

When we investigated the decompiled Android app package for WeChat, a class named "keylogger" was identified, as well as several hundred locations in the codebase that use the format of (KeyEvent keyEvent). This code is common for passing keyboard presses to a function. The act of collecting keystrokes is not necessarily malicious, but can be depending on the use of the collected keystrokes. A malicious keylogger is a tool for recording a user's keystrokes, often without their knowledge. Keyloggers are often used in malware to capture passwords and sensitive information. Further testing would be required to verify if a keylogger is in use, and if it poses any extra privacy risk. Tencent already has access to all messages sent via WeChat as they are sent via Tencent's servers, but this has the potential to capture text that was not ever intended to be sent via WeChat.

Figure 23: Keylogger class in WeChat code



Source: WeChat 7.0.16 Android .apk file.

Privacy and surveillance

Although chat messages are secured with encryption, the foundation architecture of WeChat's messaging system does not adequately secure messages from sender-to-receiver, meaning that it does not restrict third party access to its content.

With messaging apps, it's reasonable for users to desire that their private conversations carried out on the app are indeed private. With WeChat, based on the messaging architecture it's built upon, as well as the well-documented censorship of the content of chat conversations, the confidentiality and integrity of communications sent over WeChat can't be guaranteed.

WeChat uses client-to-server (C2S) encryption to protect the transmission of chat messages. This protects the messages from third parties, except the service provider, Tencent. Unlike privacy-focused apps such as Signal and Wickr, WeChat doesn't use end-to-end (E2E) encryption, which would protect the message contents from sender to receiver. In a C2S architecture, anyone with physical or digital access to the central messaging server has access to the messages on the network. By running its chat service using a C2S architecture, Tencent has positioned itself between the sender and recipient, granting it full access to the data and communications. WeChat's ability to censor or filter chat content between the two communicating parties is evidence that it processes the communications unencrypted.

Victor Gevers conducted research where he revealed that WeChat filters billions of messages for review based on keyword triggers. These messages contained GPS coordinates that were not exclusively located in China. In fact, although the majority of messages that triggered for review were sent within China, around 19 million English-language messages were captured from users around the world, including people in North America, Europe, South America, Taiwan and Australia.[165]

Tencent states that it doesn't store chat histories.[166] That's somewhat misleading. The privacy policy better articulates that chat data is semi-permanently stored for 120 hours (or 72 hours for media and location data) before being permanently deleted.[167] As a positive sign that this is likely to be true, chat histories aren't transferred when you log on to the service from a new phone. But, if a user 'Favourites' a message, then those messages will be stored on WeChat's servers.[168]

Regardless of whether Tencent stores user messages, WeChat uses a C2S encryption architecture which enables messages to be intercepted. Furthermore, according to a 2016 Amnesty International survey of the privacy of messaging apps, Tencent was the 'only company which has not stated publicly that it will not grant government requests to access encrypted messages by building a "backdoor".'[169]

Tencent also states that it does not conduct automated big-data analysis of user data, such as analysis of the content of chat messages.[170] There is no reference to their treatment of metadata which is just as valuable. Chat metadata can reveal such things as whom people are communicating with, their location and the dates, times and frequency of the contact.

Conclusion

The Chinese state has demonstrated a propensity for controlling and shaping the information environment of the Chinese diaspora—including via WeChat. The meteoric growth of TikTok has now put the CCP in a position from which it can shape the information environment on a largely non-Chinese-speaking platform—with the help of the highest valued start-up in the world and its opaque advanced AI-powered algorithm.

Chinese party-state leverage over these companies is considerable, is exercised internally via CCP committees and is enforced by a suite of cybersecurity and intelligence laws.[171] As Chinese companies, Tencent and ByteDance are not only required to participate in intelligence work, but they're also legally mandated to promote CCP propaganda.

China's censorship and propaganda apparatus is a responsibility that's pushed down to media and technology companies such as Tencent and ByteDance.[172] As Chinese companies, they're obligated to comply with strict government regulations on what content is allowed to be published on their platforms, and they both invest heavily in automated systems for content filtering and human curation.

The demands of the PRC's surveillance and propaganda apparatus on these technology companies are such that, at least in the case of WeChat, they're even prepared to surveil the foreign users of their apps in order to better train the censorship algorithms used on Chinese citizens within the PRC.

The censorship and surveillance detailed in this report most probably represent only a fraction of the total activity that's taking place on these social media platforms. At the same time as the apps compete on user growth, ad sales and investment, they're also posing a challenge to liberal democratic ideals such as freedom of political expression and free speech.

As the underlying technology used in these apps continues to advance, the ability of these companies to monitor dissent and shape narratives globally will grow exponentially.

Recommendations

1. To the extent that the censorship practices outlined in this report represent breaches of current law in liberal democracies around the world, governments should launch legal investigations.

2. In an effort to train AI algorithms that help to curate, filter and moderate content and enable targeted advertising, users' data privacy has fallen by the wayside. Governments should introduce transparent user-data privacy and user-data protection frameworks that apply to all social media and internet companies, regardless of their country of origin and ownership.[173] If companies refuse to comply with such frameworks, they shouldn't be granted licences to operate.

3. Governments should mandate that all social media platforms publicly disclose, in detail, all the content they censor and make it an offence to censor content where that has not been publicly disclosed to users.

4. Independent audits of the algorithms of all social media companies should be conducted. Included in those assessments should be transparency about the guidelines that human moderators use and what impact their decisions have on the algorithms.

5. Governments should require that all social media platforms investigate and disclose information operations (also known as 'coordinated inauthentic behaviour') being conducted on their platforms by state and non-state actors. Disclosures should include publicly releasing datasets linked to those information campaigns

6. Finally, all of the above recommended actions would benefit from multilateral collaboration that includes participation from governments, the private sector and civil society actors. For example, independent audits of algorithms could be shared by multiple governments that are seeking the same outcomes of accountability and transparency; governments, social media companies and research institutes could share data on information operations; all stakeholders could share lessons learned on data frameworks.

Appendix 1: Tencent and ByteDance CCP connections

ByteDance's CCP connections

The CCP's values are at the core of ByteDance's mindset covering content control across its platforms. This is exemplified in the company's establishment of CCP branches within its corporate structure. ByteDance first established a party branch in October 2014 and later established a party committee in April 2017, with cells within its Public Affairs Department, Technical Support Unit and Compliance Operations Unit.[174]

The Constitution of the CCP clearly outlines its expectations for party units, which it refers to as 'lower Party organisations', within private enterprises. Beginning in 2001, private entities that employed at least three CCP members are required to have a party unit installed within their corporate structure[175] and to 'firmly implement the decisions of higher Party organisations'.[176]

In particular, larger scale internet companies are known for having established CCP committees within their corporate structures.[177] This move enables internet companies, which are largely apolitical, to demonstrate their loyalty to the CCP by showing their dedication to serving the party's political mission. ByteDance is certainly no exception. In June 2018, the ByteDance Party Committee jointly held Party Day activities with the Party School of the Central Committee of the CCP, at which ByteDance employees pledged their CCP membership as they 'faced the Party flag, raised their right hands, clenched their fists and renewed their Party membership pledge', vowing to 'always be ready to sacrifice everything for the Party and the people, and to never betray the Party.'

At a live viewing of the 40th anniversary of the Reform and Opening Up movement organised by the ByteDance Party Committee, CCP member employees reflected on a speech by Xi Jinping, sharing perspectives on party ideology from the viewpoint of internet practitioners. One employee stated that, 'as a Party member and internet industry practitioner, we should begin with ourselves to integrate the spirit of reform into our daily work and studies, and be a "screw" that will never rust.'[178]

ByteDance has also taken an approach to propaganda and ideology unique for an internet company. Following the National Propaganda and Ideology Work Conference in 2018, the ByteDance Party Committee organised party lessons focusing on topics from the conference. In those lessons, the company's vice-president, Zhang Fuping, emphasised that, as an internet company, ByteDance should make use of its advantages in technology and talent, actively spread positive energy, tell China's story well and do its best to promote the internet for social development.[179]

Using ByteDance's unique position as a leading internet company for improving propaganda and ideological work demonstrates how the company can leverage its platforms to prove its loyalty to the CCP while also shaping narratives. This was reflected when the Minister of the Fujian Provincial Party Committee Propaganda Department visited ByteDance facilities in Fujian. During the visit, the minister told ByteDance that he hoped the company would use its advantages in new media and new technologies to further propagate and interpret 'Xi Jinping thought'.[180] Already, ByteDance has used its platforms, particularly Douyin, to assist provinces and cities in disseminating 'authoritative and accurate propaganda'.[181]

ByteDance's connections with the CCP also extend to its collaborations with law enforcement. Like all major Chinese tech companies, ByteDance headquarters in Beijing houses a Chinese police cybersecurity team, according to the *Wall Street Journal*.[182] That arrangement allows employees to hand over user data and other sensitive information without due process.

Tencent's CCP connections

Similarly to ByteDance, Tencent also has CCP organisations embedded within its corporate structure. As recently as April 2020, Tencent was reported to house 13 CCP general branches, more than 200 party branches and thousands of party small groups.[183] Tencent's Party Committee also became the only party committee inside internet companies to be designated as an outstanding grassroots party organisation in 2016.[184] Tencent's CCP involvement doesn't end here. Its party committee established an annual Party Day on 15 July, with the intention to both educate party members and attract non-party members to participate.[185]

Tencent's dedication to the CCP is also reflected in its compliance with public security directives. In 2015, the Deputy Minister for Public Security, Chen Zhimin, announced a plan to establish network security offices within major internet companies, including Tencent.[186] The offices are intended to provide public security entities with more direct access to illegal internet activity, enabling a quicker response to such activities. More recently, in 2017, Tencent was one of three companies that are required to assist China's government in tracking criminal suspects and silencing political dissent.[187]

Tencent's participation in the country's public security efforts stems from Chief Executive Ma Huateng's support of private companies cooperating with the government on law enforcement.[188] By 2017, Tencent had even agreed to work with the Guangzhou police to construct a cloud-based early-warning system that would enable the police to track and predict the size and movement of gatherings.[189]

Tencent's collaboration with law enforcement is also congruent with its investment in constructing smart cities. The company has plans to construct what it calls a WeCity and proposes ways in which people become 'users' within newly developed smart cities. In a WeCity, data introduces a new dimension of wealth, whereby an individual's digital behaviour becomes an asset. As a company that claims to provide continuous momentum for the government's digital transformation and smart city development, its advances in surveillance become deeply intertwined with the PRC Government's strategies.[190]

Despite its support to the government, Tencent has received criticism from the CCP pertaining to its gaming development. After Tencent released the 'Honour of Kings' game, the company was denounced by the *People's Daily*, which called the game 'poison'.[191] In contrast, Tencent's more recent release in 2019, 'Homeland Dream', was developed in collaboration with the *People's Daily* and provides patriotic references throughout the game, including slogans such as 'make army strong and prosperous', 'made in China' and 'one country, two systems'.[192] Tencent's development of what's been called 'playable propaganda' demonstrates the company's willingness to yield to the government's censorship and control.[193]

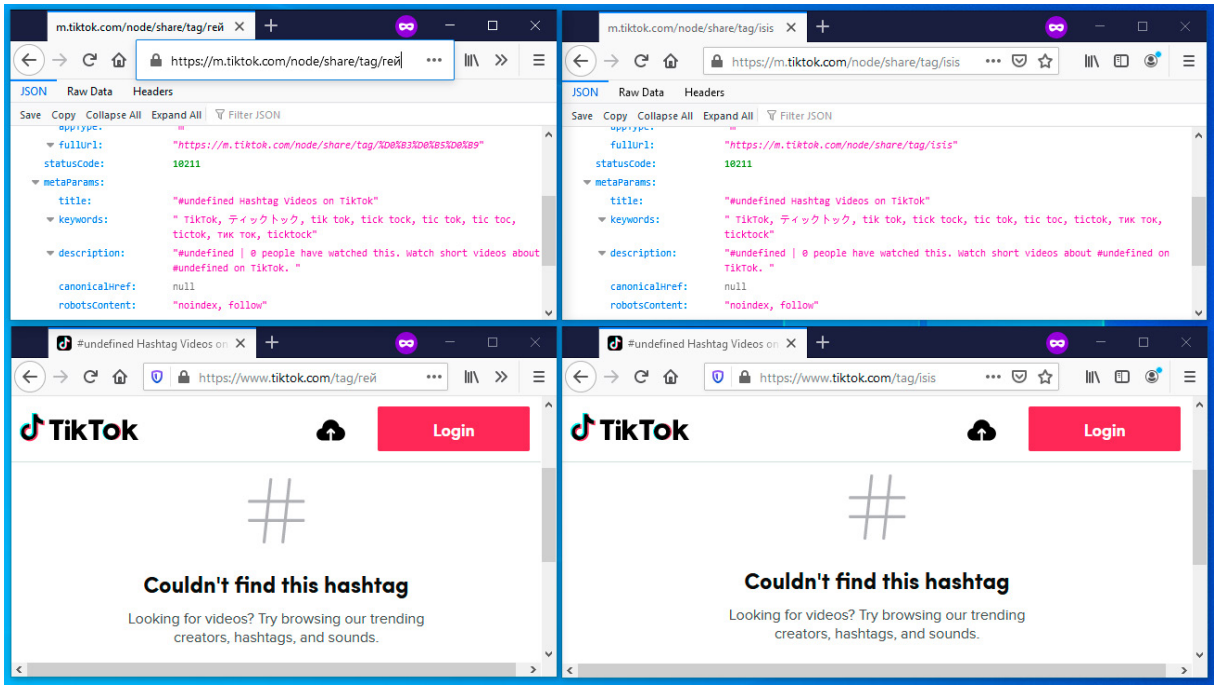
Appendix 2: TikTok data privacy and collection

statusCode

The hashtag ‘gay’ in Russian (гей) is invisible to the typical user. On the app, searching for ‘гей’ presents no results. But if you happen to come across a video with that hashtag and click on the hashtag, the hashtag exists and you can view the videos in that hashtag.

On the web platform, there is no functionality to search for hashtags, but if you visit the hashtag though the URL https://www.tiktok.com/tag/гей, you are presented with a “Couldn’t find hashtag” error, just as one would with the hashtag ‘isis’.

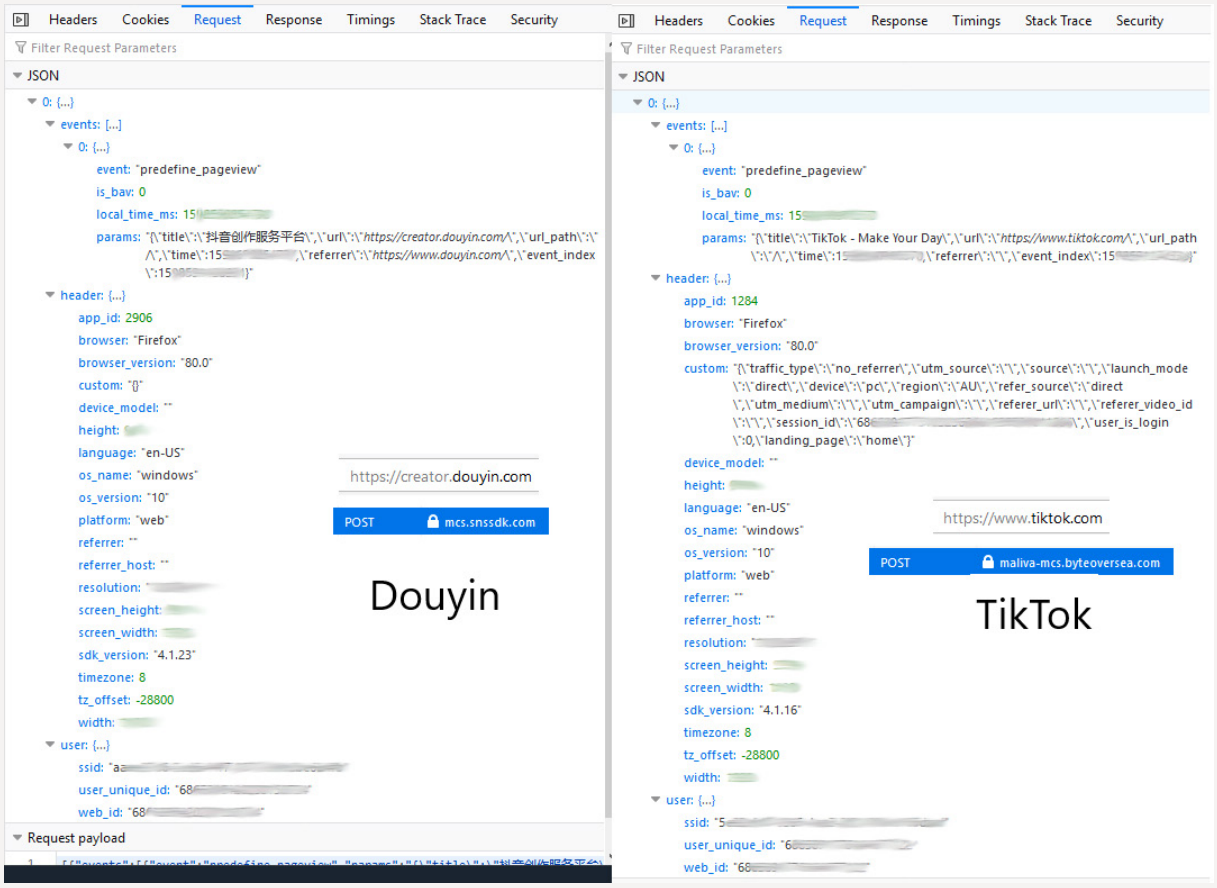
When we looked at the source code for the hashtag, we found that гей and isis shared the same statusCode - 10211.



Douyin and TikTok JSON schema

TikTok and Douyin websites are by no means identical. However we did find a lot of similarities in the JSON schema used when presenting videos and, as in the example below, in tracking users. In the image below, under “user”, you can see the individual tracking ids of the user that has been redacted.

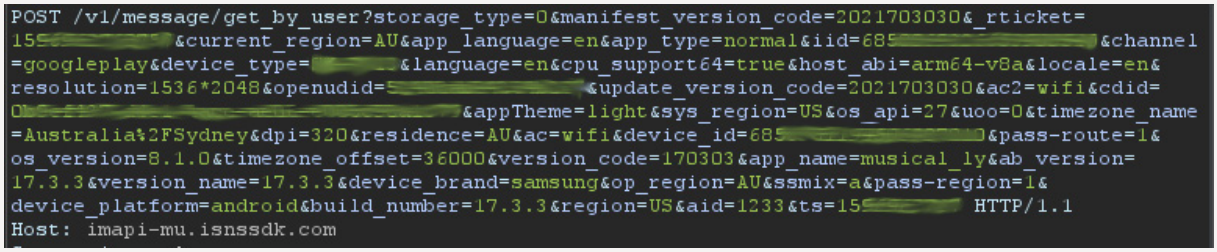
Near identical JSON schema that used to track users, used on both Douyin and TikTok websites.



Source: Douyin.com, TikTok.com.

User and Device identifiers in TikTok app request

The following images are examples of the headers of requests sent by the TikTok app containing user and device details. Every packet sent to TikTok servers has this type of information attached to it.



Targeted advertising

The following table is sourced from TikTok Ads website. It is designed to show advertisers which targeting options they can use to pinpoint their desired audience.

Audience	Include	Create a Lookalike or Custom Audience (Customer file, Engagement, App Activity, Website Traffic).
	Exclude	Exclude Lookalike or Custom Audiences
Demographics	Gender	Male, Female
	Age	13-17, 18-24, 25-34, 35-44, 45-54, 55+
	Location	country/region, state/province, or city (city targeting only available in India).
	Language	Delivery to users based on app language.
	Interest	Deliver to users based on interests. e.g. “Gaming”
Device	Connection Type	WIFI, 2G, 3G, 4G
	Operation System	iOS & Android
	Operation System Version	Deliver ads to users based on software version. e.g. iOS 10.0 or above, Android 4.0 or above.
	Device Price	Deliver ads to users based on device pricing, ranging from no limit to $1000+.
	Carrier	Deliver ads to users based on mobile phone carriers.

TikTok logging in the background

The TikTok application was tested by closing it in one instance through the Android task manager and another by force closing the process via a root shell.

In the first case, TikTok was observed to reopen with a new process ID (signifying it was a new process) and weblogs were sent from the new process (below). This is normal Android functionality for apps that run in the background, however it is not necessarily clear to users that the application is still running even after being closed.

After being closed by a root shell, the app remained closed. However we found that this wasn’t the case for the “trill” v 17.2.1 package which reopened after shell close.

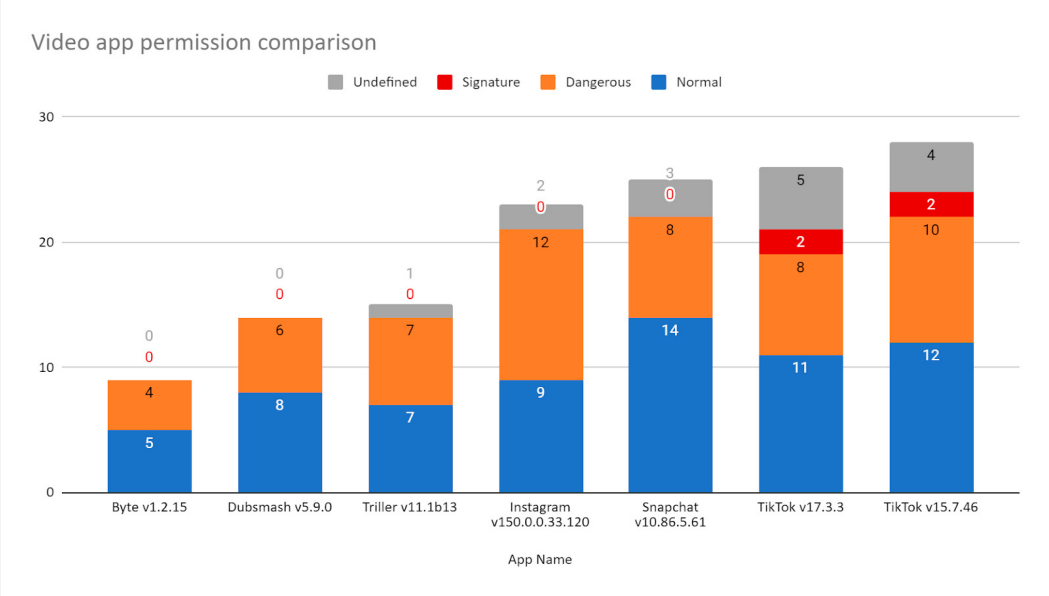
This is the log of transactions when the app was closed as described above

Time	Host	Method	URL	Length	IP	Status
13:44:29 7 Se...	https://hotapi-va.isnssdk.com	POST	/video/live/qos/v2/ipSettings?webcast_sdk_version=1620&webcast_l...	3035	203.134.79.58	200
13:39:13 7 Se...	https://hotapi-va.isnssdk.com	POST	/video/live/qos/v2/ipSettings?webcast_sdk_version=1620&webcast_l...	3189	203.134.79.73	200
13:33:56 7 Se...	https://hotapi-va.isnssdk.com	POST	/video/live/qos/v2/ipSettings?webcast_sdk_version=1620&webcast_l...	3193	203.134.79.56	200
13:33:50 7 Se...	https://dm16-useast1a.tiktokv.com	GET	/get_domains/v4/?version_code=2021703030&device_id=6856951...	26278	203.134.79.72	200
13:33:50 7 Se...	https://hotapi-va.isnssdk.com	GET	/video/live/qos/v2/ipSettings?webcast_sdk_version=1620&webcast_l...	2325	203.134.79.56	200
13:33:49 7 Se...	https://api16-normal-c-useast1a.tiktokv.com	GET	/ies/speed/?aid=1233&source_type=0&group_id=101_15994496288...	1184	203.134.79.74	200
13:33:49 7 Se...	https://webcast16-normal-c-useast1a.tiktokv.com	GET	/webcast/tab/?show_location=0&webcast_sdk_version=1620&webca...	1968	203.134.79.56	200
13:33:49 7 Se...	https://webcast16-normal-c-useast1a.tiktokv.com	GET	/webcast/setting/i18n/package/?locale=en_&locale=en&cur_version...	88081	203.134.79.56	200
13:33:11 7 Se...	https://xlog-va.tiktokv.com	POST	/v2/r?os=0&ver=0.6.11.29.19-MT&m=2&app_ver=17.3.3&region=en...	1060	23.192.108.186	200
13:33:09 7 Se...	https://hotapi-va.isnssdk.com	POST	/video/live/qos/v2/ipSettings?webcast_sdk_version=1620&webcast_l...	3189	203.134.79.56	200

Permissions

Short video app permission comparison

To compare the permissions requested by comparable short-video apps, we extracted permissions using mostly MobSF (Mobile Security Framework - https://github.com/MobSF/Mobile-Security-Framework-MobSF). Drozer (https://github.com/FSecureLABS/drozer) was used for Instagram as we were not able to extract its permissions with MobSF. In order to normalise the permissions, we removed all the custom permissions from all the applications being compared. Then categorised the protection level of the permissions based on the Android Developer documentation (https://developer.android.com/reference/android/Manifest.permission). We categorised those permissions that were deprecated, by their original protection level assignment . Those Android permissions that we couldn't find, we marked as undefined.



Signature permissions in use

Unique to TikTok against its competitors is its use of two permissions with a "signature" level of protection. This type of permission is only granted by the system if the requesting application is signed with the same certificate as the application that declared the permission. We would need to perform further analysis to determine what it is used for within the TikTok app.

Permission	Protection Level	Notes
android.permission.GET_TASKS	deprecated (signature|privileged)	Allows application to retrieve information about currently, and recently, running tasks. May allow malicious applications to discover private information about other applications (source:Mob SF). But because this permission is deprecated, this permission may or may not work.
android.permission.REQUEST_INSTALL_PACKAGES	signature	Allows an application to request installing packages (Android Developer doc).

Comparison between TikTok packages and versions

TikTok has two packages on the Google Play store - com.ss.ugc.android.trill published by TikTok Pte Ltd (Singapore) and com.zhiliaoapp.musically published by TikTok Inc (US). The likely reason for this is the transition to integrate Bytedance's original TikTok with the acquisition of Musical.ly. A user's location will determine which Google Store they are presented with and thus which TikTok package they will download. Based on the text strings within the different packages, TikTok Inc is designed for an English speaking audience and the TikTok Pte Ltd app, the rest of the world.

In version 15 (v15) of both packages, there were differences in the servers the app sends data to. Permissions for user location were removed in the US version of the app, but remained in the other version of the app. In version 17 (v17) the permissions are identical across both packages.

1 Permissions

a. Comparing the permissions requested in v15 of these packages, the com.ss.android.ugc.trill package designed for rest-of-world (excl USA) requested three more permissions.

The additional three permissions declared by com.ss.android.ugc.trill, not in com.zhiliaoapp.musically		
Permission	**Protection level**	**Definition**
android.permission.ACCESS_FINE_LOCATION	Dangerous	Allows an app to access precise location.
android.permission.ACCESS_COURSE_LOCATION	Dangerous	Allows an app to access approximate location.
android.permission.READ_PHONE_STATE	Dangerous	Allows read only access to phone state, including the current cellular network information, the status of any ongoing calls, and a list of any PhoneAccounts registered on the device.

b. In v17, the above 3 permissions have been removed from the permission list, along with 3 others, reducing the overall permissions list to 63 for both packages.

Permissions in v15, no longer in v17		
Permission	**Protection level**	**Definition**
android.permission.ACCESS_FINE_LOCATION	Dangerous	Allows an app to access precise location.
android.permission.ACCESS_COURSE_LOCATION	Dangerous	Allows an app to access approximate location.
android.permission.READ_PHONE_STATE	Dangerous	Allows read only access to phone state, including the current cellular network information, the status of any ongoing calls, and a list of any PhoneAccounts registered on the device.
android.permission.EXPAND_STATUS_BAR	Normal	Allows application to expand or collapse the status bar.
android.permission.MANAGE_ACCOUNTS	Dangerous	Allows an application to perform operations like adding and removing accounts and deleting their password.
android.permission.USE_CREDENTIALS	Dangerous	Allows an application to request authentication tokens.

2 Hosts

Comparing hosts in the AndroidManifest.xml. It is likely that t ~ tiktok, m~ musical.ly, va ~ Virginia, USA

com.ss.android.ugc.trill	com.zhiliaoapp.com
vt.tiktok.com	vm.tiktok.com
t.tiktok.com	m.tiktok.com
	v16.musical.ly
	app-va.musical.ly

Although some places in the code, such as the AndroidManifest file, still make reference to the musical.ly domain, actual network traffic out of the app has transitioned away from the musical.ly domain by v17.

3 Version 16

A French researcher looking into com.zhiliaoapp.com v16.6.52 found the following in the code.

We can see that although it is designed for a US market, there are configurations that remain in the code to send data elsewhere, including China.

```
        UrlConfig.CHINA = new UrlConfig("https://log.snssdk.com/service/2/app_log/",
"https://rtlog.snssdk.com/service/2/app_log/", new String[]
{"https://log.snssdk.com/service/2/device_register/",
"https://log.snssdk.com/service/2/device_register/"},
"https://ichannel.snssdk.com/service/2/app_alert_check/",
"https://log.snssdk.com/service/2/log_settings/", "https://log.snssdk.com/service/2/app_log/",
"https://log.snssdk.com/service/2/log_settings/");
        UrlConfig.AMERICA = new UrlConfig("https://log.isnssdk.com/service/2/app_log/",
"https://rtlog.isnssdk.com/service/2/app_log/", new String[]
{"https://log.isnssdk.com/service/2/device_register/",
"https://log.isnssdk.com/service/2/device_register/"},
"https://ichannel.isnssdk.com/service/2/app_alert_check/",
"https://log.isnssdk.com/service/2/log_settings/", "https://log.isnssdk.com/service/2/app_log/",
"https://log.isnssdk.com/service/2/log_settings/");
        UrlConfig.AMERICA_HTTP = new UrlConfig("https://log.isnssdk.com/service/2/app_log/",
"https://rtlog.isnssdk.com/service/2/app_log/", new String[]
{"https://log.isnssdk.com/service/2/device_register/",
"https://log.isnssdk.com/service/2/device_register/"},
"https://ichannel.isnssdk.com/service/2/app_alert_check/",
"https://log.isnssdk.com/service/2/log_settings/", "https://log.isnssdk.com/service/2/app_log/",
"https://log.isnssdk.com/service/2/log_settings/");
        UrlConfig.SIG_AWS = new UrlConfig("https://log.sgsnssdk.com/service/2/app_log/",
"https://rtlog.sgsnssdk.com/service/2/app_log/", new String[]
{"https://log.sgsnssdk.com/service/2/device_register/",
"https://log15.byteoversea.com/service/2/device_register/",
"https://log.sgsnssdk.com/service/2/device_register/",
"https://log15.byteoversea.com/service/2/device_register/"},
"https://ichannel.sgsnssdk.com/service/2/app_alert_check/",
"https://log.sgsnssdk.com/service/2/log_settings/", "https://log.sgsnssdk.com/service/2/app_log/",
"https://log.sgsnssdk.com/service/2/log_settings/");
        UrlConfig.SIG_ALIYUN = new UrlConfig("https://log.byteoversea.com/service/2/app_log/",
"https://rtlog.byteoversea.com/service/2/app_log/", new String[]
{"https://log.byteoversea.com/service/2/device_register/",
"https://log.byteoversea.com/service/2/device_register/"},
"https://i.byteoversea.com/service/2/app_alert_check/",
"https://log.byteoversea.com/service/2/log_settings/",
"https://log.byteoversea.com/service/2/app_log/",
"https://log.byteoversea.com/service/2/log_settings/");
        UrlConfig.MUSICALLY = new UrlConfig("https://applog.musical.ly/service/2/app_log/",
"https://rtlog.musical.ly/service/2/app_log/", new String[]
```

Source: https://medium.com/@fs0c131y/tiktok-logs-logs-logs-e93e8162647a

Logging of internal network details

1 This is an extract from traffic captured from TikTok (com.ss.android.ugc.trill) v15.7.45 sending traffic to host: mon.tiktokv.com. It collected details on the VPN tunnel being used, and in another instance, the proxy being used. This did not occur in version 17. However, the internal IP and DNS settings were still captured in version 17.


```
},
\"ifconfig\":{
        \"interfaces\":[
                {
                        \"addr\":\"10.[redacted].2\",
                        \"name\":\"tun0\"
                },
                {
                        \"addr\":\"192.168.[redacted].1[redacted]\",
                        \"name\":\"wlan0\"
                },
                {
                        \"addr\":\"[redacted]\",
                        \"name\":\"wlan0\"
                },
                {
                        \"addr\":\"[redacted]\",
                        \"name\":\"wlan0\"
                }
        ],
```



```
POST /monitor/collect/?sdk_version=400&storage_type=0&manifest_version_code=2021703030&_rticket=1599447[redacted]&current_region=AU&app_language=en&app_type=normal&iid=
[redacted]&channel=googleplay&device_type=SM-[redacted]&language=en&cpu_support64=true&host_abi=arm64-v8a&locale=en&resolution=1536*2048&openudid=52408[redacted]&
update_version_code=2021703030&ac2=wifi&cdid=e1e8d5f1-eab1-[redacted]&sys_region=US&appTheme=light&os_api=27&uoo=0&timezone_name=Australia%2FSydney&dpi=320&
residence=AU&ac=wifi&device_id=[redacted]&os=Android&pass-route=1&os_version=8.1.0&timezone_offset=36000&version_code=170303&app_name=musical_ly&ab_version=17.3.3&
version_name=17.3.3&device_brand=samsung&op_region=AU&ssmix=a&pass-region=1&device_platform=android&build_number=17.3.3&region=US&aid=1233&ts=1599447556 HTTP/1.1
Host: mon-va.tiktokv.com
Connection: close
Content-Length: 29870
Cookie: store-idc=maliva; store-country-code=au; install_id=[redacted]; ttreq=1$cf48dfa[redacted]; odin_tt=
5dbcc57ff4fc4fc52091c596ff6aa9e130a04edaf2571ff90edef0c684ea4eae42c8be863793df15655982db1b[redacted]
Version-Code: 1
Accept-Encoding: gzip, deflate
X-SS-REQ-TICKET: 1599447648921
Content-Type: application/json; charset=utf-8
X-SS-STUB: C2970116F5BE2DCE90F28D77[redacted]
x-tt-store-idc: maliva
x-tt-store-region: au
x-tt-trace-id: 00-6682c15105f28c8c81ec78602a004d1-66824c[redacted]
User-Agent: com.zhiliaoapp.musically/2021703030 (Linux; U; Android 8.1.0; en_US; SM-[redacted]; Build/OPM2.171019.029.B1; Cronet/TTNetVersion:[redacted]0c 2020-08-05
QuicVersion:0144d358 2020-03-24)
X-Khronos: 1599447[redacted]
X-Gorgon: 840440e600015fc5f7572f1a47db4871ad4df4ea5[redacted]

{"data":[{"log_type":"api_error","duration":81,"uri":"https:\/\/p16.muscdn.com\/obj\/tiktok-obj\/benchmark_video_2s.mp4?73a925431aac3cf511e0fb73158c5be8","timestamp":
1599447[redacted],"status":4,"ip":"0","trace_code":"","cronet_error_code":"11","cronet_internal_error_code":"-2","nt_band_width":"G00D","cdn_nt_band_width":"UNKNOWN",
"cronet_open":true,"cronet_plugin_install":false,"requestStart":1599447[redacted],"responseBack":0,"completeReadResponse":0,"appLevelRequestStart":1599447[redacted],
"beforeAllInterceptors":1599447[redacted],"requestEnd":1599447[redacted],"recycleCount":0,"timing_dns":72,"timing_connect":0,"timing_ssl":-1,"timing_send":-1,"timing_waiting":-1,
"timing_receive":-1,"timing_total":77,"timing_isSocketReused":false,"timing_totalSendBytes":0,"timing_totalReceivedBytes":0,"timing_remoteIP":"0","request_log":
"{\"ab_test\":{\"hit\":[\"755335\",\"1926451\",\"1325014\",\"1979306\",\"1939716\",\"1974588\",\"70001528\",\"1580466\",\"1932931\",\"1949702\",\"1942130\",\"1775999\",\"17
69083\",\"1816574\",\"1897614\",\"1932042\"]},\"base\":{\"has_upload\":false,\"is_pending\":true,\"load_flags\":16,\"load_state\":0,\"method\":\"GET\",\"net_error\":-3,\"or
igin_url\":\"https:\/\/p16.muscdn.com\/obj\/tiktok-obj\/benchmark_video_2s.mp4\",\"redirect_times\":0,\"status\":\"FAILED\",\"traffic_annotation\":77012883},\"dns\":{\"addr
ess_list\":[],\"cache_source\":-1,\"cache_stale_reason\":-1,\"hijacked_error\":0,\"nameservers\":[\"192.168.43.207:53\"],\"queried_with_cip\":\"\",\"source\":0},\"event\":{
\"engine_startup\":1599447538.8134,\"network_change\":0.0},\"header\":{\"x-tt-trace-id\":\"00-6680ccc6105f28c8c81ec78602d604d1-6680ccc6105f28c8-01\"},\"ifconfig\":{\"ipv4_r
eachable\":true,\"ipv6_reachable\":false},\"nqe\":{\"downlink_throughput\":1400,\"effective_net_type\":4,\"group_rtt_estimate\":[],\"http_rtt\":662,\"tcp_rtt\":10},\"other\
":{\"core_ver\":\"77.0.3844.0\",\"is_background\":false,\"is_keep_referrer\":false,\"is_main_process\":true,\"libcore\":\"cronet\",\"net_thread_priority\":0,\"quic_commit\"
```


2 Appsflyer code in TikTok v17 checking for a VPN.

```
} else if (Build.VERSION.SDK_INT >= 16) {
    ArrayList arrayList = new ArrayList();
    try {
        Iterator<T> it2 = Collections.list(NetworkInterface.getNetworkInterfaces()).iterator();
        while (it2.hasNext()) {
            NetworkInterface networkInterface = (NetworkInterface) it2.next();
            if (networkInterface.isUp()) {
                arrayList.add(networkInterface.getName());
            }
        }
        return arrayList.contains("tun0");
```

App Analysis Areas Worth Further Investigation

Data logged to SD card -- There is a potential for data leak. During app usage, data was found to be logged to the SD card. This data is not deleted when the app is uninstalled. It can be easily accessed by other applications with SD card permissions.

Opaque areas of the application -- The app uses Java reflection, operating system commands and shared libraries (arm64 version). While these have legitimate uses in a standard application, they are also areas where potential security and privacy concerns may exist.Time limitations prevented us from fully investigating these areas.

Keylogging -- The KeyEvent parameter was observed being used at several points in the application. This is worth investigating further for potential keylogging, especially as the privacy policy says that TikTok collects 'keystrokes'.

Appendix 3: WeChat

Investigating how the censorship on Official Account Platforms is occurring

After we noticed WeChat incorrectly redirecting links on the Official Accounts Platform, we used an HTTP web proxy to analyse the webpage code to try to see if we could determine how this was occurring, so as to assist with discovering more cases. Our investigations lead us to believe that the content marking and filtering process occurs on the server-end and likely occurs upon submission of an article. This way, by the time any user requests that webpage, the way that it will function has already been determined.

404 error

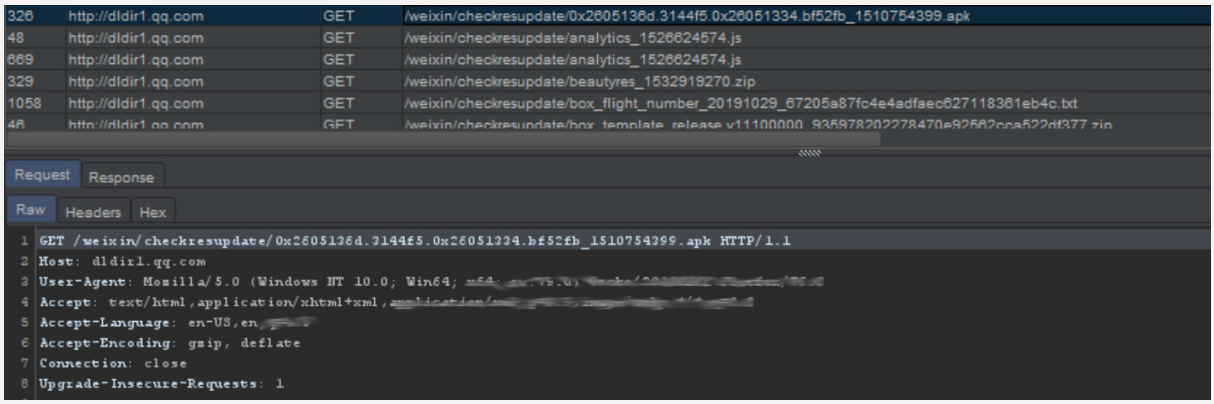
It is possible that the redirection to a 404 page is a website coding error, but because this only occurred to articles with content sensitive to Beijing, this seems unlikely. In either case, as it currently stands, these articles are being censored.

Share button

For some articles, the Share button was ghosted out and thus the user was not able to click the button. We found code related to the webpage that ghosted the Share button and modified it to re-enable the Share button locally on the testing mobile device. However, when we clicked the Share button, WeChat presented us with an error message “Cannot share this content”. Although we enabled the functionality to click the Share button, there are likely other factors that we were not able to determine that are preventing the function. Below is an image of the error message.

APK downloaded by WeChat during signup

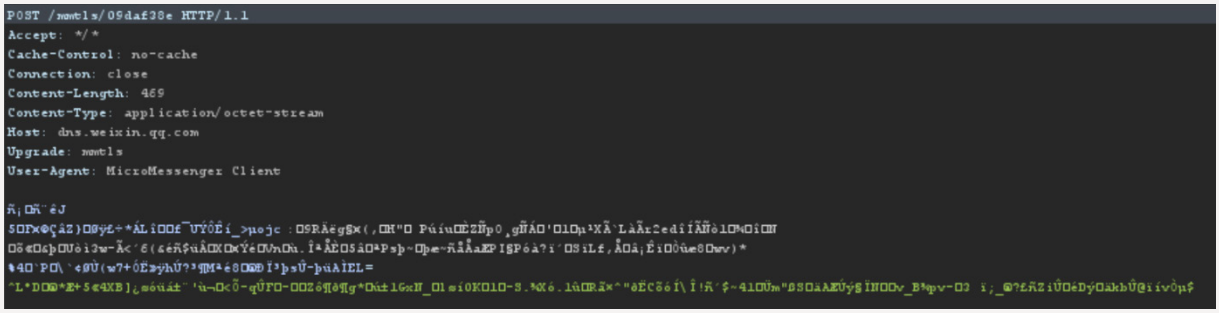
During the sign-up process the WeChat app downloaded an .apk file via HTTP. Below is an image of the web request for the download that was captured by the software we used to analyse the traffic out of WeChat.



WeChat's custom protocol mmtls

WeChat uses a custom protocol for some of its traffic. The requests are sent over plaintext but the underlying data is encrypted.

Specifications matching this format were found online here: https://gitlab.com/iamfaith/article/-/blob/master/基于TLS1.3的微信安全通信协议mmtls介绍.md



App analysis - areas worth further investigation

Further to the items mentioned in the body of the report, we also believe these areas are worth further investigation.

Opaque areas of the application -- The app uses Java reflection, operating system commands, runtime dex loading and shared libraries (arm64 version). While these have legitimate uses in a standard application, they are also areas where potential security and privacy concerns may exist. Time limitations prevented us from fully investigating these areas.

Keylogging -- The KeyEvent parameter was observed being used at several points in the application. This is worth investigating further for potential keylogging, especially as there was a class named 'keylogger' identified in the app.

Appendix 4: Examples of PRC-based TikTok jobs advertised by ByteDance

Table 2: PRC-based TikTok jobs advertised by ByteDance

Title	Location	Category	Description
Senior software engineer—TikTok recommendation	Beijing	R&D	1. Build industry leading recommendation system; develop highly scalable classifiers and tools leveraging machine learning. 2. Understand product objectives and machine learning techniques; improve model and recommendation strategy. 3. Understand user behaviour and apply ML algorithms to optimise content consumption and production experience. 4. Understand content security strategy and apply ML algorithms to improve content audit process.
iOS business development/ architecture—TikTok	Shanghai	R&D	1. Responsible for TikTok's iOS app technology pre-research and architecture design. 2. Abstract platform technology components. 3. Project reconstruction, code review, performance optimisation, quality control. 4. Conduct research on new technology directions, overcome technical difficulties and train new employees.
TikTok Ads advertising system architecture (senior) engineer	Beijing	R&D	1. Design and optimise TikTok advertising system-related services, including but not limited to advertising CTR/CVR estimation services and advertising recall services. 2. Design and implement flexible, extensible, stable, and high-performance computing models and frameworks. 3. Troubleshoot the production system; design and implement the necessary mechanisms and tools to ensure the stability and efficiency of the overall operation of the production system.
TikTok Ads advertising algorithm (senior) engineer	Beijing	R&D	1. Use various strategies to improve the monetisation efficiency and user experience of international products, and design and implement an efficient strategy for mixing articles and advertisements. 2. Improve the prediction accuracy of the CTR/CVR advertising model, data analysis, modelling and feature engineering. 3. Advertisement-targeted mining to build user portraits. 4. Optimising a GD advertising scheduling system. 5. Research and implement traffic control, an advertising pacing algorithm and an advertising bidding mechanism.
Server leader—TikTok live stream	Beijing	R&D	1. Responsible for TikTok live-stream-related business development. 2. Responsible for continuously improving existing services, optimising system weaknesses, and improving system performance and stability. 3. In-depth exploration and analysis of business needs, writing technical solutions and system designs. 4. Improve base component support, better support business iteration and introduce new technologies and solutions for the team based on business needs. 5. Responsible for technical team building, talent training and team management.

Title	Location	Category	Description
Senior server architect—TikTok	Shanghai	R&D	1. Responsible for participating in and guiding server-side business R&D work in one or more subfields, including but not limited to TikTok's core modules such as basic business, security, user growth and service architecture. 2. Analyse and thoroughly explore the shortcomings of the existing system, locate system bottlenecks, and improve system performance and stability. 3. Think about various issues in the R&D process and promote the improvement of team work efficiency and development quality. 4. Based on actual business needs, introduce new technologies and new solutions to the team. 5. With good project management, coordination and communication skills, be responsible for the promotion of cross-team key projects.
Android architecture leader—Douyin/ TikTok	Shenzhen	R&D	1. Responsible for R&D and management of Douyin/TikTok's Android infrastructure. 2. Responsible for the construction and management of the Douyin/TikTok Android infrastructure team; responsible for the quality and efficiency of the team's output. 3. Responsible for architecture optimisation, performance optimisation, experience optimisation etc. of the Douyin/TikTok Android client.
Back-end core R&D engineer—TikTok	Shanghai	R&D	1. Responsible for the research and development of TikTok's server, including but not limited to core modules such as basic business, security, user growth, and service architecture. 2. In-depth exploration and analysis of business requirements, writing technical solutions and system design. 3. Carry out system design and coding according to product requirements. 4. Continue to transform and optimise the system architecture.
Algorithm engineer—Douyin/Toutiao/ TikTok Search	Beijing	R&D	1. Participate in the R&D of the ByteDance search engine, use cutting-edge machine learning algorithms and massive data to make the most exciting technology and give users the best search experience. 2. Participate in the R&D of core products such as Toutiao / Douyin / TikTok and serve hundreds of millions of global users. 3. Participate in improving the core algorithm for search.
Back-end development engineer—Douyin/Toutiao/ TikTok Search	Beijing	R&D	1. Participate in Toutiao/Douyin/TikTok search service optimisation. 2. Responsible for searching online system architecture construction, optimising system stability, performance, capacity, throughput, and designing flexible strategy architecture to support rapid strategy iteration and upgrades. 3. Responsible for the construction of the offline search system architecture; optimise the stability and efficiency of offline data flow, and promote the rapid and accurate application of offline data to online. 4. Abstract and general offline search system architecture and strategy architecture, used for quickly supporting major vertical search engines.

Title	Location	Category	Description
Algorithm engineer—TnS	Beijing	R&D	1. Responsible for content understanding and user modelling of ByteDance overseas products (TikTok, Vigo, …). 2. Have a deep understanding of content security strategies, combined with machine learning and other technologies to optimise content security business processes and efficiency. 3. Have a deep understanding of business and machine learning technology, optimise short video understanding and modelling, and improve recommendation results and content ecology. 4. Have a deep understanding of business and machine learning technology, optimise user/creator understanding and modelling, and improve recommendation results and creative ecology.
Senior operations strategy manager—TikTok Latin America	Beijing	Operations	1. Assist in the formulation of localised content strategies for short videos according to product features, user portraits and development stages. 2. Participate in content strategy and operation target design, task disassembly, monitoring, attribution and review. 3. Responsible for important content analysis projects, and coordinate the team and cross-departmental implementation and project follow-up. 4. Through analysis and research on content, users, target market, combined with data, make recommendations on business directions.
TikTok operations intern—Middle East	Beijing	Operations	1. Mine users' video content consumption needs, build a content operation library, improve video quality, and enrich the community content. 2. Responsible for the maintenance and management of core users in the community, as well as the mining and introduction of intelligent off-site users. 3. Responsible for event operations, planning online events, and evaluating the results. 4. Responsible for updating and maintaining official social media content, planning social media activities, and operating core user communities.
TikTok content operation manager—East EU	Shanghai	Operations	1. Deep understanding of content market in Russia; familiar with most recent trending videos consumed by young audience, 2. Choose qualified videos and promote on social media platforms and be responsible for in-app content. 3. Participate in launching and operating 'hashtag', follow up the hot spots in the country and carry out innovative publicity. 4. Monitoring local content ecosystem, collaborate with data team to improve the diversity of in-app content, give feedback/guidelines to user operations to acquire right content needed in the community. 5. Possess a strong understanding of our product, our competition in the industry and position to leverage them into impactful marketing activities. 6. Research new market trends as well as user insights to leverage them into impactful marketing activities.

Source: *ByteDance Referral*, online; *ByteDance*, online.

Notes

1 Lai Lin Thomala, 'Number of active WeChat messenger accounts Q2 2011-Q2 2020', *Statista*, 20 August 2020, online.
2 Ronald Deibert, 'WeChat users outside China face surveillance while training censorship algorithms', *Washington Post*, 8 May 2020, online.
3 Paul Mozur, 'Forget TikTok. China's powerhouse app is WeChat, and its power is sweeping', *New York Times*, 4 September 2020, online.
4 Alex Sherman, 'TikTok reveals detailed user numbers for the first time', *CNBC*, 24 August 2020, online.
5 Alex Hern, 'Revealed: how TikTok censors videos that do not please Beijing', *The Guardian*, 20 August 2019, online.
6 David Bandurski, 'Tech shame in the new era', *China Media Project*, 11 April 2018, online.
7 Sam Biddle, Tatiana Dias, Paulo Victor Ribeiro, 'Invisible censorship: TikTok told moderators to suppress posts by "ugly" people and the poor to attract new users', *The Intercept*, 16 March 2020, online.
8 Vanessa Pappas, Kudzi Chikumbu, 'A message to our black community', *TikTok Newsroom*, 2 June 2020, online.
9 Fanny Potkin, 'TikTok booms in Southeast Asia as it picks path through political minefields', *Reuters*, 28 August 2020, online. Alex Hern, 'Revealed: how TikTok censors videos that do not please Beijing', *The Guardian*, 20 August 2019, online.
10 Appendix 2, 'statusCode'.
11 'Statement on TikTok's content moderation and data security practices', *TikTok Newsroom*, 25 October 2019, online.
12 Leo Kelion, 'Teen's TikTok video about China's Muslim camps goes viral', *BBC News*, 26 November 2019, online.
13 Alex Hern, 'Revealed: how TikTok censors videos that do not please Beijing', *The Guardian*, 20 August 2019, online.
14 Markus Reuter, Chris Köver, 'TikTok's criticism and competition guidelines', *Netzpolitik*, 29 November 2019, online.
15 Potkin, 'TikTok booms in Southeast Asia as it picks path through political minefields'.
16 Alex Hern, 'TikTok's local moderation guidelines ban pro-LGBT content', *The Guardian*, 26 September 2019, online.
17 Zaheena Rasheed, 'Why are Thai students protesting against King Vajiralongkorn?', *al-Jazeera*, 26 August 2020, online.
18 Alyssa Kann, 'Popular hashtag hidden from TikTok during anti-police protests in the United States', *DFRLab*, 2 June 2020, online.
19 The hashtag was available on Twitter and Instagram when ASPI ICPC checked on 29 August and remains available on both. On 7 September a TikTok spokesperson told ASPI ICPC that #acab had been "incorrectly moderated" and that they had "resolved the error". On 9 September, a reader brought to ASPI ICPC's attention that #acab was blocked on Facebook. Searching for the hashtag on the Facebook app results in a message from the platform that reads "Keeping our community safe. Posts with #ACAB are temporarily hidden here. Some content in those posts goes against our Community Standards".
20 Markus Reuter, Chris Köver, 'Cheerfulness and censorship', *Netzpolitik*, 23 November 2019, online.
21 Alex Hern, 'Revealed: how TikTok censors videos that do not please Beijing', *The Guardian*, 20 August 2019, online.
22 Jack Nicas, Mike Isaac, Ana Swanson, 'TikTok said to be under national security review', *New York Times*, 7 August 2020, online.
23 '#MyPride: Celebrating authenticity and inclusivity', *TikTok Newsroom*, 23 June 2020, online.
24 Hern, 'TikTok's local moderation guidelines ban pro-LGBT content'.
25 Chris Köver, Markus Reuter, 'TikTok curbed reach for people with disabilities', *Netzpolitik*, 2 December 2019, online.
26 Cristina Criddle, 'Transgender users accuse TikTok of censorship', *BBC*, 12 February 2020, online.
27 Lily Wakefield, 'Man "devastated" after TikTok removed video of him kissing his boyfriend because it "violated community guidelines"', *Pink News*, 8 January 2020, online.
28 Ragip Soylu, '"They delete everything": Former TikTok moderator reveals China app censorship', *Middle East Eye*, 19 December 2019, online.
29 Lavanya Mahendran, Nasser Alsherif, 'Adding clarity to our community guidelines', *TikTok Newsroom*, 8 January 2020, online.
30 'Audacity in adversity: LGBT activism in the Middle East and North Africa', *Human Rights Watch*, 16 April 2018, online.
31 Markus Reuter, Chris Köver, 'Gute Laune und Zensur' [Good mood and censorship], *Netzpolitik*, 23 November 2019, online.
32 Marianna Spring, 'QAnon: TikTok blocks QAnon conspiracy theory hashtags', *BBC News*, 24 July 2020, online.
33 Spring, 'QAnon: TikTok blocks QAnon conspiracy theory hashtags'.
34 Guang Pu, '独家| 内部员工揭秘 : TikTok 竟然这么审核内容' [Exclusive: Internal staff reveals how TikTok actually reviews content], 品玩 [*Ping West*], 14 June 2020, online.
35 Eric Han. 'Countering hate on TikTok', *TikTok Newsroom*, 21 August 2020, online.
36 Potkin, 'TikTok booms in Southeast Asia as it picks path through political minefields'.
37 'Is "Putin is a thief" a (potentially illegal) insult? Putin's press secretary thinks so', *Meduza*, 31 May 2019, online.
38 'Navalny defies Russia's new law against insulting authorities online', *Radio Free Europe / Radio Liberty*, 29 March 2019, online.
39 'Russian lawmakers approve anti-gay bill in 436–0 vote', *France 24*, 12 June 2013 ,online.
40 'Online and on all fronts', *Human Rights Watch*, 18 July 2017, online.
41 Carl Schreck, 'Twitter restores suspended Putin parody account after outcry', *Radio Free Europe / Radio Liberty*, 1 June 2016, online.
42 'Instagram submits to Russia censor's demands', *BBC News*, 15 February 2018, online.
43 Danielle Cave et al., 'ByteDance', *Mapping China's tech giants*, ASPI, Canberra, 19 April 2019, online and please see Appendix 1.
44 Sebastian Meineck, 'TikTok: Ich habe China kritisiert, dann wurden meine Videos versteckt', *VICE*, 13 December 2019, online.
45 @themomentj_1018, 'Profile', *TikTok*, online.
46 @themomentj_1018, 'Vlog: Trip to Xinjiang (3)—Thanks to all the frontier workers! Full version on YouTube, #xinjiang #jessicatalks #china', *TikTok*, online.
47 Li Li [李莉], '新疆给我的感觉太好" "达人西游"全网总传播量超80亿人次' ['Xinjiang gives me such a great feeling Influencers head west campaign exceeds 8 billion views], 新疆日报 [*Xinjiang Daily*], 12 January 2020, online.
48 Li Li 'Xinjiang gives me such a great feeling" Influencers head west campaign exceeds 8 billion views'.
49 Zang Shijie (臧诗洁), 'Profile', *LinkedIn*, online.
50 Department of Foreign Language (外国语学部). 'The Department of Foreign Language's undergraduate third Party branch held a full membership admission plenary session for probationary Party members' [外国语学部本科生第三党支部预备党员转正大会举行], Beijing Language and Culture University (北京语言大学), 26 May 2015, online.
51 'Guan Video: Using academic short films to tell Chinese stories' [观视频工作室 : 用学术短视频讲述中国故事], *Observer Network* [观察者网], 20 June 2019, online.
52 Isobel Cockerell, 'How TikTok opened a window into China's police state', *Coda*, 25 September 2019, online.

53 'News and Propaganda Bureau of the Ministry of Public Security signed a strategic cooperation agreement with ByteDance—and also ceremony for new media of police department across the nation to arrive at Jinri Toutiao, Douyin' [公安部新闻宣传局与字节跳动战略合作签约；暨全国公安新媒体矩阵入驻今日头条抖音仪式举行], *China Police Net* [中国警察网], 25 Apr 2019, online.
54 Isobel Cockerell, 'Xinjiang's TikTok wipes away evidence of Uyghur persecution—Coda follows up', *Coda*, 24 January 2020, online.
55 Jacob Wallis et al., *Retweeting through the Great Firewall*, ASPI, Canberra, 12 June 2020, online.
56 Twitter Safety, 'Disclosing networks of state-linked information operations we've removed', *Twitter Blog*, 12 June 2020, online.
57 Nathaniel Gleicher, 'Removing coordinated inauthentic behavior from China', *Facebook News*, 19 August 2019, online.
58 Raphael Satter, 'Google pulls 2,500 China-linked YouTube channels over disinformation', *Reuters*, 6 August 2020, online.
59 Lin Yueqin [林跃勤], 'Focus on improving the ability to respond to external public opinion attacks against China' [着力提升因应外部对华舆论攻击能力], *Chinese Social Sciences Net* [中国社会科学网], 24 April 2020, online.
60 Sam Biddle, Tatiana Dias and Paulo Victor Ribeiro. 'Invisible Censorship: TikTok told moderators to suppress posts by "ugly" people and the poor to attract new users', The Intercept, 16 March 2020, online.
61 Liza Lin, Aaron Tilley, Georgia Wells, 'TikTok deal talks are snarled over fate of app's algorithms', *Wall Street Journal*, 2 September 2020, online.
62 'How TikTok recommends videos #ForYou', *TikTok Newsroom*, 19 June 2020, online.
63 'Announcement of the Ministry of Commerce and Science and Technology no. 38 of 2020 on adjusting and releasing the catalogue of China's prohibited and restricted export technologies' [商务部 科技部公告2020年第38号 关于调整发布《中国禁止出口限制出口技术目录》的公告], Ministry of Commerce of the People's Republic of China (MOFCOM), 28 August 2020, online.
64 Rebecca Heilweil, 'TikTok offered details about how its most popular feed works. Experts seem unimpressed', *Recode*, 23 June 2020, online.
65 'Regulations on Ecological Governance of Network Information Content' [网络信息内容生态治理规定], Cyberspace Administration of China, 15 December 2019, online.
66 'Detailed Rules for Auditing Standards of Network Short Video Content' [网络短视频内容审核标准细则], China Netcasting Services Association, 9 January 2019, online.
67 Biddle et al., 'Invisible censorship: TikTok told moderators to suppress posts by "ugly" people and the poor to attract new users'.
68 'Detailed Rules for Auditing Standards of Network Short Video Content'.
69 David Bandurski, 'Tech shame in the new era', *China Media Project*, 11 April 2018, online.
70 Beijing Internet Association [首都互联网协会党委], 'ByteDance Party Committee: We must give priority to stressing the correct guidance' [字节跳动党委：要把讲导向守责任放首位], *Sina Finance* [新浪财经], 29 April 2018, online.
71 Beijing Internet Association, 'ByteDance Party Committee: We must give priority to stressing the correct guidance'.
72 Mercy A Kuo, 'China's media market competition', *The Diplomat*, 5 December 2017, online.
73 Juro Osawa, Yunan Zhang, Amir Efrati, 'Breaking off TikTok will be hard to do', *The Information*, 29 July 2020, online.
74 Osawa et al., 'Breaking off TikTok will be hard to do'.
75 Juro Osawa, Yunan Zhang and Amir Efrati. 'Breaking Off TikTok Will Be Hard to Do' *The Information*, 29 July 2020, online.
76 Juro Osawa, Yunan Zhang and Amir Efrati. 'Breaking Off TikTok Will Be Hard to Do' *The Information*, 29 July 2020, online.
77 Osawa et al., 'Breaking off TikTok will be hard to do'.
78 '平台直播自律白皮书' [*Platform live broadcast self-discipline white paper*], online.
79 Echo Wang, Paresh Dave. 'Exclusive: Microsoft faces complex technical challenges in TikTok carveout', *Reuters*, 10 August 2020, online.
80 Osawa et al., 'Breaking off TikTok will be hard to do'.
81 Announcement of the Ministry of Commerce and Science and Technology no. 38 of 2020 on adjusting and releasing the catalogue of China's prohibited and restricted export technologies'.
82 David Ramli, Shelly Banjo, 'The kids use TikTok now because data-mined videos are so much fun', *Bloomberg*, 18 April 2019, online.
83 Pierre Bienaimé, 'TikTok's Blake Chandlee on working with US brands despite conflict with the White House', *Digiday Podcast*, 4 August 2020, online.
84 'TikTok "absolutely not" a US security risk, says top executive', *PBS*, 25 August 2020, online.
85 Megan Mccluskey. 'These TikTok creators say they're still being suppressed for posting Black Lives Matter content', *TIME*, 22 July 2020, online.
86 Pappas, 'A message to our black community'.
87 Jordan Schneider, 'What to do about TikTok and WeChat', *ChinaTalk*, 21 July 2020, online.
88 Nilesh Christopher, 'Censorship claims emerge as TikTok gets political in India', *BBC News*, 31 January 2020, online.
89 Saloni Gaur, 'Nazma Aapi on corona at Zee News', *Instagram*, 20 May 2020, online.
90 Saloni Gaur, 'Nazma Aapi on corona at Zee News', Twitter, 20 May 2020, online.
91 Saloni Gaur, 'Nazma Aapi on corona at Zee News', YouTube, 19 May 2020, online.
92 Eric Han, 'An update on recent content and account questions', *TikTok Newsroom*, 28 November 2019, online.
93 Hern, 'Revealed: how TikTok censors videos that do not please Beijing'.
94 Feroza Aziz, 'Update: tik tok has issued a public apology and gave me my account back. Do I believe they took it away because of a unrelated satirical video that was deleted on a previous deleted account of mine? Right after I finished posting a 3 part video about the Uyghurs? No.', *Twitter*, 28 November 2019, online.
95 Lotus Ruan et al., 'One app, two systems' *Citizen Lab*, 30 November 2016, online.
96 Emily Feng, 'China intercepts WeChat texts from US and abroad, researchers say', *NPR*, 29 August 2019, online.
97 Jeffrey Knockel et al. 'We chat, they Watch', *Citizen Lab*, 7 May 2020, online.
98 David Gilbert, 'Here's how China is silencing coronavirus critics in the US', *VICE News*, 13 February 2020, online.
99 Zoe Schiffer, 'WeChat keeps banning Chinese Americans for talking about Hong Kong', *The Verge*, 25 November 2019, online.
100 'Fighting for free speech: starting from WeChat', Citizen Power Initiatives for China, 19 February 2020, online.
101 Cyberspace Administration of China (CAC) [网信中国], 'The Cyber Space Administration of China guides relevant local network information offices to investigate and deal with illegal websites and accounts according to the law' [国家网信办指导有关地方网信办 依法查处违法违规网站平台及账号], *Weixin*, 5 February 2020, online.
102 '微信再现大规模封号' [WeChat Reproduces a Large-Scale Ban], *China Digital Times*, 5 February 2020, online.
103 '"A healthy society should not have just one voice"—China must end crackdown on online speech in response to COVID-10', *Chinese Human Rights Defenders*, 1 April 2020, online.
104 'Fighting for free speech: starting from WeChat'.

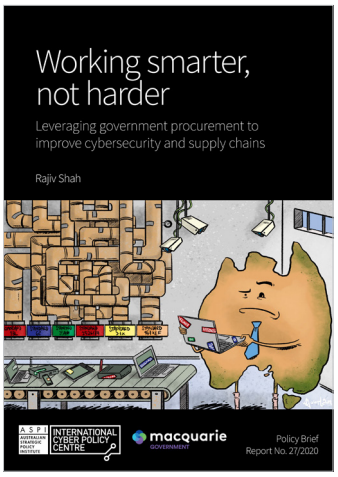
105 Greg Fay, 'Repression across borders: the CCP's illegal harassment and coercion of Uyghur Americans', *Uyghur Human Rights Project*, August 2019, online.
106 Fay, 'Repression across borders: the CCP's illegal harassment and coercion of Uyghur Americans'.
107 Joshua Lipes, 'Xinjiang authorities detain Uyghur aspiring professional footballer in "political re-education camp"', *Radio Free Asia*, 15 January 2019, online.
108 Mozur, 'Forget TikTok. China's powerhouse app is WeChat, and its power is sweeping'.
109 'China Media Bulletin 135', *Freedom House*, April 2019, online.
110 Mozur, 'Forget TikTok. China's powerhouse app is WeChat, and its power is sweeping'.
111 Yaqiu Wang, 'WeChat is a trap for China's Diaspora', *Foreign Policy*, 14 August 2020, online.
112 Isabelle Niu, 'Is WeChat a problem for democracies?', *Quartz*, 14 May 2020, online.
113 Niu, 'Is WeChat a problem for democracies?'.
114 Tom Sear, Michael Jensen, Titus C Chen, 'How digital media blur the border between Australia and China', *The Conversation*, 16 November 2018, online.
115 Alia Wong, 'The app at the heart of the movement to end affirmative action', *The Atlantic*, 20 November 2018, online.
116 Julie Makinen, 'Chinese social media platform plays a role in US rallies for NYPD officer', *Los Angeles Times*, 24 February 2016, online.
117 Rosie Lewis, Joe Kelly, 'Tampa moment looms as latest poll tightens', *The Australian*, 17 February 2019, online.
118 Steve Cannane. 'Australian politicians risk being kicked of Chinese social media', *ABC News*, 24 April 2019, online.
119 Steve Cannane, Echo Hui, 'Bill Shorten and Scott Morrison risk losing access to Chinese voters on WeChat', *ABC News*, 24 April 2019, online.
120 Marcus Wang, Stella Fan. 'Censored on WeChat: A year of content removals on China's most powerful social media platform', *Global Voices*, 11 February 2019, online.
121 'Li Wenliang: Coronavirus death of Wuhan doctor sparks anger', *BBC News*, 7 February 2020, online.
122 Ben Blanchard, 'US, China trade jibes as military tensions worsen', *Reuters*, 27 August 2020, online.
123 This is the URL of the article: online. When visited it presents an error banner stating 'Unable to view this content because it violates regulations'.
124 British Embassy Beijing, 'Hong Kong response is censored', *gov.uk*, 29 June 2020, online.
125 British Embassy Beijing, 'Hong Kong response is censored'.
126 Sutirtho Patranobis, 'India posts PM Modi's remarks on Ladakh face-off, China's WeChat app deletes it', *Hindustan Times*, 20 June 2020, online.
127 Patranobis, 'India posts PM Modi's remarks on Ladakh face-off, China's WeChat app deletes it'.
128 David Carroll, 'Is TikTok a Chinese Cambridge Analytica data bomb waiting to explode?', *Quartz*, 7 May 2019, online.
129 Katie Paul, 'Tiktok accused in California lawsuit of sending user data to China', *Reuters*, 3 December 2019, online.
130 Carroll, 'Is TikTok a Chinese Cambridge Analytica data bomb waiting to explode?'.
131 Drew Harwell, Tony Romm. 'Inside TikTok: A culture clash where US views about censorship often were overridden by the Chinese bosses', *Washington Post*, 5 November 2019, online.
132 Nicas et al., 'TikTok said to be under national security review'.
133 Roland Cloutier, 'Our approach to security', *TikTok Newsroom*, 28 April 2020, online. Full quote: 'Our goal is to minimize data access across regions so that, for example, employees in the APAC region, including China, would have very minimal access to user data from the EU and US.'
134 'TikTok Inc and Bytedance Inc vs President of the United States, Secretary of Commerce and US Department of Commerce', case2:20-cv-07672, filed 24 August 2020, online.
135 '中华人民共和国国家情报法' [The National Intelligence Law of the People's Republic of China], National People's Congress of the People's Republic of China, 27 June 2017, online.
136 Georgia Wells, Yang Jie, Yoko Kubota, 'TikTok's videos are goofy. Its strategy to dominate social media is serious', *Wall Street Journal*, 29 June 2019, online.
137 Yingzhi Yang, Echo Wang, Alexandra Alper, 'Exclusive: TikTok owner ByteDance moves to shift power out of China—sources', *Reuters*, 28 May 2020, online.
138 Osawa et al., 'Breaking off TikTok will be hard to do'.
139 Osawa et al., 'Breaking off TikTok will be hard to do'.
140 Yang et al., Exclusive: TikTok owner ByteDance moves to shift power out of China—sources'.
141 'Tiktok Content Operation manager—East EU', *ByteDance Referral*, online; 'TikTok运营实习生 — 中东', (Operations Intern—Middle East), *ByteDance*, online; '高级运营策略经理—TikTok拉美地区', (Senior Operations Strategy Manager—TikTok Latin America), *ByteDance*, online.
142 Appendix 4, 'Examples of PRC-based TikTok jobs advertised by ByteDance.
143 Harwell & Romm, 'Inside TikTok: A culture clash where US views about censorship often were overridden by the Chinese bosses'.
144 Osawa et al., 'Breaking off TikTok will be hard to do'.
145 'LinkedIn interviews ByteDance: How ByteDance builds its global employer brand', YouTube, 16 May 2019, online.
146 Osawa et al., 'Breaking off TikTok will be hard to do'.
147 '字节跳动海外解忧 TikTok与抖音加速切割' [ByteDance accelerates the process of cutting ties between TikTok and Douyin in order to tackle concerns overseas], *The Time Weekly*, 30 March 2020, online.
148 '算法工程师-TnS' [Algorithm engineer—TnS), *ByteDance*, online.
149 Appendix 4 'Examples of PRC-based TikTok jobs advertised by ByteDance.
150 TikTok has two packages on the Google Play store - com.ss.ugc.android.trill published by TikTok Pte Ltd (Singapore) and com.zhiliaoapp.musically published by TikTok Inc (US). The likely reason for this is the transition to integrate Bytedance's original TikTok with the acquisition of Musical.ly. A user's location will determine which Google Store they are presented with and thus which TikTok package they will download. Based on the text strings within the different packages, TikTok Inc is designed for an English speaking audience and the TikTok Pte Ltd app, the rest of the world.
151 Laurence Dodds. 'How popular apps can read your phone's clipboard without permission', The Telegraph, 30 March 2020, online.
152 Dan Goodin, 'Tiktok and 32 other iOS apps still snoop your sensitive clipboard data', *Ars Technica*, 28 June 2020 online; Zak Doffman, 'Apple suddenly confirms hidden problem impacting all iPhone, iPad users', *Forbes*, 23 June 2020, online; Zak Doffman, 'Warning—Apple suddenly catches TikTok secretly spying on millions of iphone users', *Forbes*, 26 June 2020, online.
153 Tommy Mysk, 'Popular iPhone and iPad apps snooping on the pasteboard', *Mysk*, 16 August 2020, online.

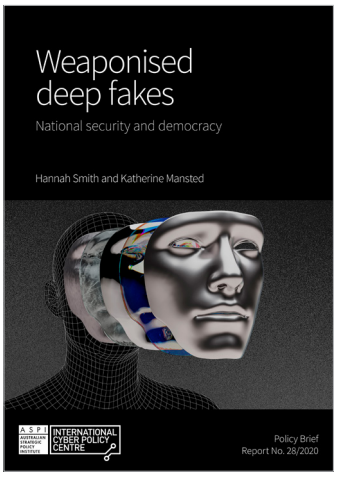
154 Roland Cloutier, 'Updates on our security roadmap', *TikTok Newsroom*, 30 June 2020, online.
155 Matthias Erbel, 'Privacy analysis of TikTok's app and website', *Rufposten*, 5 December 2019, online.
156 Kevin McMillan, 'Tiktok tracked user data using tactic banned by Google', *Wall Street Journal*, 11 August 2020, online.
157 'Misty Hong vs Bytedance Inc, TikTok Inc, Beijing Bytedance Technology Co. Ltd, Musical.ly', *Courthouse News*, 27 November 2019, online.
158 Elliot Alderson, 'TikTok: logs, logs, logs', *Medium*, 3 August 2020, online.
159 Bytedance manages AS396986 & AS138699 'Bytedance Peering Policy', Bytedance, online.
160 'Privacy policy: How we share your information', *TikTok Legal*, online.
161 Appendix 1, 'Comparison between v15 and v17'.
162 Mara Hvistendahl, 'Blueleaks reveals what TikTok shares with US authorities', *The Intercept*, 11 August 2020, online.
163 See Appendix 3
164 The .apk file was downloaded from Weixin, online, and doesn't appear to be a fully functional stand-alone apk.
165 China Media Bulletin 136: The survival of dissent, WeChat monitoring, smuggled videos (May 2019), *Freedom House*, online.
166 'WeChat denies "storing" chat histories', *BBC News*, 2 January 2018, online.
167 'WeChat privacy policy', *WeChat*, online.
168 'WeChat Help Centre: How secure are my chat messages and conversations on WeChat? Can third-parties snoop or read my messages?', *WeChat*, online.
169 How Private Are Your Favourite Messaging Apps?". 2016. Amnesty.Org, online.
170 'How secure are my chat messages and conversations on WeChat? Can third-parties snoop or read my messages?', WeChat Help Center, online.
171 See Appendi1 for Tencent and ByteDance CCP connections
172 Lotus Ruan, 'Internet censorship: how China does it', *The Strategist*, 9 October 2017, online.
173 This recommendation is derived from ideas expressed by Lindsay Gorman here: https://securingdemocracy.gmfus.org/qa-with-lindsay-gorman-how-does-tiktok-pose-a-national-security-risk-to-the-united-states/ and by Kara Frederick, Chris Estep and Megan Lamberth here: https://warontherocks.com/2020/08/beyond-tiktok-preparing-for-future-digital-threats/
174 '不忘初心 重温入党志愿书' [Never forget the original intention, reflect upon the application for party membership], *People's Daily*, 15 June 2020, online.
175 Yi-Zheng Lian, 'China, the party–corporate complex', *New York Times*, 12 February 2017, online.
176 'Full text of Constitution of Communist Party of China', *News of the Communist Party of China*, 29 March 2013, online.
177 Zhang Lin, 'Chinese Communist Party needs to curtail its presence in private businesses', *South China Morning Post*, 25 November 2018, online.
178 '字节跳动 (ByteDance) 党委 : 认真学习讲话精神 · 努力承担社会责任' [ByteDance Party Committee: Earnestly study the spirit of the speech and work hard to assume social responsibility], *VITO*, 27 December 2018, online.
179 '字节跳动党委举办专题党课学习贯彻全国宣传思想工作会议精神' [The ByteDance Party Committee held a special party class to study and implement the spirit of the national propaganda and ideology work conference], China Federation of Internet Societies, 31 August 2018, online.
180 '省领导到福建字节跳动公司调研' [Provincial leaders visited Fujian ByteDance Company for investigation], *Southeast Net*, 11 March 2020, online.
181 '日照市首届政务头条大会暨政务号集体入驻仪式举行' [Rizhao City held its first Toutiao conference for government services and a ceremony for the launch of Toutiao accounts for government services], *Shouji Rizhao Wang*, online.
182 Wells et al., 'TikTok's videos are goofy. Its strategy to dominate social media is serious'.
183 '积极构建互联网党建工作新格局' [Actively build a new pattern of internet party building work], Cyberspace Administration of China, 16 April 2020, online.
184 '腾讯、ofo、知乎……互联网企业掀"党建潮"背后意义何在？' [Tencent, ofo, Zhihu … what is the meaning behind the 'party building wave' launched by internet companies?], *Xinhua*, 30 March 2018, online.
185 'Tencent, ofo, Zhihu… what is the meaning behind the "party building wave" launched by internet companies?'.
186 Charles Clover, 'China to tighten grip over country's internet users', *Financial Times*, 5 August 2015, online.
187 Liza Lin, Josh Chin. 'China's tech giants have a second job: helping Beijing spy on its people', *Wall Street Journal*, 30 November 2017, online.
188 Lin & Chin, 'China's tech giants have a second job: helping Beijing spy on its people'.
189 Lin & Chin, 'China's tech giants have a second job: helping Beijing spy on its people'.
190 '腾讯政务全新战略升级 发布新一代WeCity技术平台' [New strategic update of Tencent's government affairs work. A next-generation WeCity technology platform], *ZhongGuoXinWenWang*, 15 July 2020, online.
191 Sijia Jiang, 'China communist party mouthpiece slams Tencent game; shares slide', *Reuters*, 4 July 2017, online.
192 Louise Lucas, Wang Xueqiao. 'Patriotic Tencent city-building game tops China download charts', *Financial Times*, 30 September 2019, online.
193 Josh Ye, 'Chinese propaganda game Homeland Dream is disturbingly addictive', *South China Morning Post*, 2 October 2019, online.

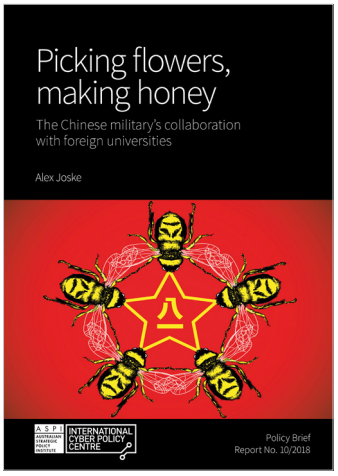
Acronyms and abbreviations

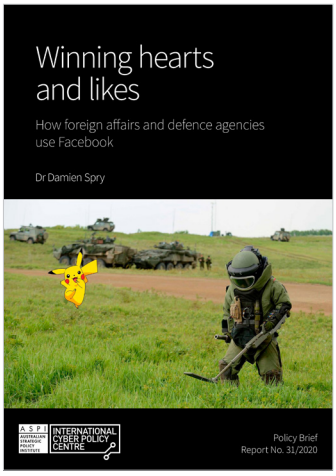
AI	artificial intelligence
C2S	client-to-server
CCP	Chinese Communist Party
CEO	chief executive officer
DFRLab	Digital Forensic Research Lab
DNS	domain name system
E2E	end-to-end
EU	European Union
GPS	Global Positioning System
ICPC	International Cyber Policy Centre
IMEI	international mobile equipment identity
IMSI	international mobile subscriber identity
IP	internet protocol
PRC	People's Republic of China
R&D	research and development
SDK	software development kit
TnS	trust and safety
VPN	virtual private network

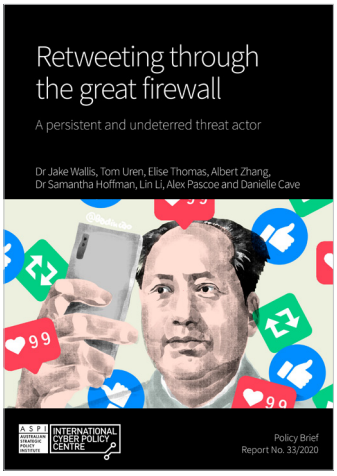
Some previous ICPC publications

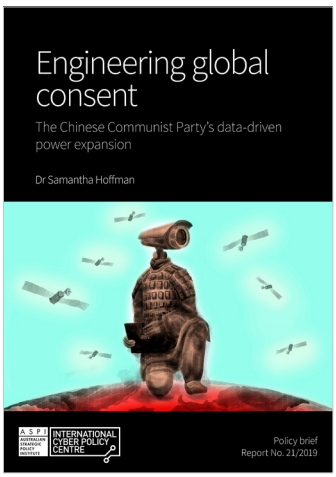












ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

INTERNATIONAL CYBER POLICY CENTRE