Testimony

Cognitive Hacking as the New Disinformation Frontier

TikTok's links with an Artificial Intelligence Algorithm designed to repress the Chinese Population.

Paul Dabrowa

Testimony presented before the Commonwealth of Australia Senate Select Committee on Foreign Interference through Social Media on September 22, 2020.

This is a submission by Paul Dabrowa, an artificial intelligence and social media expert specialising in the operational underpinnings of persuasion and related psychology. He argues that data breaches are not the real danger posed by TikTok, but rather how that data is already being exploited by the Chinese government to influence young minds with persuasive algorithmic techniques. Reports show the same source code that powers Douyin, a tool used by the Chinese Communist Party to facilitate the brutal crackdown on their own population, may also power TikTok a smartphone application used by children.

After studying at the University of Melbourne and Harvard Kennedy School between 1998 - 2002, Paul Dabrowa worked in fixed income in London for Morgan Stanley, Merryl Lynch and Goldman Sachs from 2003 - 2009. In 2010, he co-founded the company Astrosleep, commercialising technology originally developed for NASA to manage astronaut circadian health and using it to maximise performance for elite athletes, racehorses and Formula One teams.

Presently, Dabrowa is the co-founder of biome.ai, a company which uses artificial intelligence to develop treatments for disease using the human microbiome. Dabrowa gained a specialisation in propaganda and persuasion during his studies, interviewing former Nazis and KGB operatives to develop a neuroscience model of how totalitarian propaganda works. He is now leading a global campaign to persuade those governments currently being targeted by aggressive Chinese and Russian propaganda to launch formal domestic counter-propaganda efforts to defend their populations.

Cognitive Hacking as the New Disinformation Frontier

Interim Submission:

TikTok's links with an Artificial Intelligence Algorithm designed to repress the Chinese Population.

Testimony of Paul Dabrowa

Select Committee on Foreign Interference through Social Media

Commonwealth of Australia Senate

September 22, 2020.

The risk in the new propaganda war

The science and practice of persuasion has gotten drastically more sophisticated in recent years, thanks in large part to technology. Today, digitally-crafted propaganda can trigger wars, economic collapse, riots, and protests of all kinds. It can also destroy the credibility of government institutions and turn a population against itself.

But while 2016 gave the world a quick-fire lesson in how hostile foreign nations can abuse social media to achieve their political agendas, or how personal data can be exploited for persuasive political campaigns, it did little to educate people on the role being played in the propaganda arts by sophisticated state actors and personalized Artificial Intelligence Algorithms.

In 2020, the biggest risk when it comes to the hacking of collective minds is AI-driven persuasion hiding behind "secret" algorithms on social media platforms. The targets of such persuasion ops are often children who would not be aware of anything being amiss in the usual barrage of social media content they consume. In this new frontier, persuasion is invisible, or at least can be designed to look very benign.

So how does it work?

The first thing to remember is that persuasion (or propaganda, a term popularised by Edward Bernays in the 1920s) need not persuade the majority of the public to be effective. It's enough to persuade just one per cent of the population to destabilise a democracy effectively with protests, rioting and a collapse in institutional trust. So the question that really needs asking is how hard is it to radicalise one per cent of the public with modern, weaponized forms of persuasion?

The answer is dangerously easy.

How hard is it to programme children without their knowledge? Even easier.

Remove from the equation for a moment whether the social movements erupting across America and other western democracies in 2020 are justified or not. The intention of this testimony is not to analyse the tenets of these movements, but rather to consider if it is possible thanks to propaganda, social conditioning or amplified feedback loops to radicalise well-intentioned people to the point their own primary beliefs begin to work against them. Consider for a moment if it is possible that a good cause can be sabotaged and intentionally weaponized against a population without their knowledge?

What we know is that the potential gain for a foreign adversary to purposefully radicalise elements of any social movement is large and potentially incalculable. The risk on their end, meanwhile, is trivial not least because every part of the technology already exists. It represents a simple evolution from computer hacking to cognitive hacking.

Such cognitive attacks, if they were indeed happening, for the most part would be invisible to us if they were delivered via private company social media platforms.

A ticking time bomb?

TikTok is a private Chinese company with 800 million users that is most popular with adolescents and young kids. Until the recent controversies about its ownership prompted interventions, its leadership was vulnerable like many other Chinese platforms to direct influence by the Chinese Communist Party.[1] This comes about because Chinese parent companies are obliged to follow CCP directives even if their foreign entities are in theory separated, since such directives apply globally. China's 2017 national intelligence law directs that "any organisation and citizen" shall support and co-operate " in national intelligence work".[2] Thus, if the Chinese government decided to boost the signal of any particular message on TikTok, it would be trivially easy for it to do so by exploiting security vulnerabilities, as was recently highlighted in the recent executive order put out by the White House.[3]

One way the CCP could destabilise a foreign presidential campaign using TikTok, for example, could be to boost the signal of an otherwise small user calling for a prank involving fake registrations for a campaign rally. All we would know is that the prank went viral. We wouldn't know why. Or how. What's certain, is that once the message went viral on TikTok it would be further amplified across all media because once content becomes popular on TikTok (which has a younger audience), it soon spreads to SnapChat where it enters a mixed audience, and from there on to other platforms of all ages.

But this is not actually a hypothetical.[4] State sponsored actors are already using social media to influence politics. In one case in 2013, a group hijacked the Associated Press' Twitter account and sent the following tweet: "Two explosions in the White House and Barack Obama

[1] https://medium.com/@pandaily/open-apology-from-ceo-of-toutiao-following-the-ban-of-neihan-duanzi-6381000939d0
[2] http://www.npc.gov.cn/npc/c30834/201806/483221713dac4f31bda7f9d951108912.shtml
[3] https://www.whitehouse.gov/presidential-actions/executive-order-addressing-threat-posed-tiktok
[4] https://www.scmp.com/comment/opinion/article/3095575/us-election-tiktok-firing-line-over-trump-campaign-fears-china

is injured." This message, with the weight of the Associated Press behind it, caused a drop and recovery of roughly $136bn in equity market value over a period of about five minutes.[5]

On the other side of the world in 2013, unverified news spread about a young Hindu girl who complained to her family that she had been verbally abused by a Muslim boy.[6] In response, her brother and cousin reportedly went to pay the boy a visit and killed him. This story spurred real clashes between Hindu and Muslim communities. A political actor was reportedly behind the story.[7] His intent was simply to incite a race riot by posting a gruesome video of two men being beaten to death, accompanied by a caption that identified the two men as Hindu and the mob as Muslim. The news was spread by social media "bot" accounts recounting the rumour that the mob had murdered the young girl's brother and cousin in retaliation. 13,000 Indian troops were called upon to put down the resulting violence[8]. In the end, the video showing two men being beaten to death was exposed as recording an entirely different incident. Not only was the video not of the men claimed in the caption, the incident had not even taken place in India.

To gain traction the operatives behind this attack required no technical skill whatsoever; just a psychosocial understanding of the place and time to post to achieve the desired effect.

Speed was the key to success. In both cases, weaponized disinformation attacks were distributed widely to and by the intended victims -- the people. State actors used manipulative language and images to evoke a desired, emotional response. The content was designed specifically to appeal to and inflame typical human fears and anxieties. In today's world, social media companies, and the state actors that leverage their data, know more personal information about individuals than the individuals themselves. With this arsenal of data -- attacks are developed to stoke fear and inflame emotions to produce a desired outcome. The more personal the information we unwittingly shed online the easier it is to groom a target - especially children. The pervasiveness of artificial intelligence in this domain means that mass manipulation is not just easier in 2020, it can also be personally targeted.

Active measures are back in play

In February 2017, Russian Defence Minister Sergey Shoigu openly acknowledged the formation of an Information Army within the Russian military, noting:

"Information operations forces have been established that are expected to be a far more effective tool than all we used before for counter-propaganda purposes."[9]

Dwarfing Russia's effort in personnel and budget, however, are China's propaganda operations.[10] Unlike Russia's efforts these are highly secret and hidden from diagrams of the Chinese bureaucratic system. Those who have studied the system say the central propaganda department extends its tentacles throughout every bureaucratic establishment, into virtually

[5] https://www.washingtonpost.com/gdpr-consent/?next_url=https%3a%2f%2fwww.washingtonpost.com%2fnews%2fworldviews%2fwp%2f2013%2f04%2f23%2fsyrian-hackers-claim-ap-hack-that-tipped-stock-market-by-136-billion-is-it-terrorism%2f
[6] https://www.latimes.com/world/la-xpm-2013-sep-09-la-fg-india-communal-20130910-story.html
[7] https://www.ndtv.com/india-news/the-mystery-of-kawwal-were-muzaffarnagar-riots-based-on-distortion-of-facts-534608
[8] https://www.latimes.com/world/la-xpm-2013-sep-09-la-fg-india-communal-20130910-story.html
[9] https://www.bbc.com/news/world-europe-39062663
[10] https://www.westminsterpapers.org/articles/abstract/10.16997/wpcc.15/

every medium concerned with the dissemination of information with the goal of "ideological remodelling" and "thought reform".[11]

The department is headed by Wang Huning,[12] a key figure behind the rise of Xi Jingping (who many have noted appears to model himself on Mao[13]) and recently became China's dictator for life.[14] Wang ruthlessly rooted out internal opposition[15], and created a leadership cult under the principles of "Xi Jinping Thought"[16] - where citizens are even encouraged to replace images of Jesus with the party leader.[17] His department remains a top economic and political priority for the regime as an indoctrinated population is the key to the totalitarian regime remaining in power.[18]

The Office of Foreign Propaganda more commonly known as 'Information Office of the State Council of the People's Republic of China'[19], coordinates with a coalition of front groups including the "50 Cent Party"[20] and "United Front"[21] to conduct information warfare operations globally.

Cambridge Analytica simply harnessed social media and personal data to influence elections in the same way PR agencies target advertising. State-based propaganda, however, ruthlessly reaches into every aspect of people's lives and utilises all the tools available to totalitarian states; from military grade artificial intelligence to millions of full-time employees posting government messaging on social media. It is even responsible for the shipment of millions of dissidents to re-education camps, where an independent commission found human organ harvesting takes place.[22]

Why TikTok is not like other platforms

TikTok's direct connection to the Chinese government means it is different from other Western social media applications. But TikTok is also a fundamentally different[23] app to other social media in the way it uses artificial intelligence to hook its users.[24]

What the public domain knows is that the Chinese military has for decades been developing powerful artificial intelligence technology[25] designed to manipulate and shape the behaviour of individuals.

[11] https://www.journals.uchicago.edu/doi/10.1086/tcj.57.20066240
[12] https://www.washingtonpost.com/news/theworldpost/wp/2017/11/06/wang-huning/
[13] https://www.cato.org/publications/commentary/xi-jinping-wants-become-new-mao
[14] https://www.theguardian.com/world/2018/feb/26/xi-jinping-china-presidential-limit-scrap-dictator-for-life
[15] https://www.rand.org/content/dam/rand/pubs/testimonies/CT500/CT503/RAND_CT503.pdf
[16] https://foreignpolicy.com/2016/03/08/the-personality-cult-of-xi-jinping-china-leader-communist-party/
[17] https://www.scmp.com/news/china/policies-politics/article/2119699/praise-xi-jinping-not-jesus-escape-poverty-christian
[18] https://www.wilsoncenter.org/article/chinas-foreign-propaganda-machine
[19] http://english.scio.gov.cn/
[20] https://www.washingtonpost.com/news/monkey-cage/wp/2016/05/19/the-chinese-government-fakes-nearly-450-million-social-media-comments-a-year-this-is-why/
[21] https://www.abc.net.au/news/2020-06-17/china-communist-party-australia-united-front-aspi-report/12334498
[22] https://www.forbes.com/sites/ewelinaochab/2019/06/17/the-china-tribunal-pronounced-its-verdict-on-organ-harvesting-in-china/#687ce7432eeb
[23] https://www.nytimes.com/2019/03/10/style/what-is-tik-tok.html
[24] https://towardsdatascience.com/why-tiktok-made-its-user-so-obsessive-the-ai-algorithm-that-got-you-hooked-7895bb1ab423
[25] https://www.theatlantic.com/magazine/archive/2020/09/china-ai-surveillance/614197/

This is a programme that develops predictive behavioural models expunged from the data exposed by users' digital footprints online. This includes their computers, their smartphones, wearables, and just about any other data tracking devices. Online communities that have attempted to reverse engineer some of TikTok's processes have also highlighted the risks.[26] Finding serious breaches of data privacy and a backdoor for hackers to manipulate the way the Artificial Intelligence curates user news feeds: *"TikTok is a data collection service that is thinly-veiled as a social network. If there is an API to get information on you, your contacts, or your device..well, they're using it… They have several different protections in place to prevent you from reversing or debugging the app as well. App behaviour changes slightly if they know you're trying to figure out what they're doing. There's also a few snippets of code on the Android version that allows for the downloading of a remote zip file, unzipping it, and executing said binary. There is zero reason a mobile app would need this functionality legitimately."*[27] US-based Penetrum Research also analysed the application and confirmed *"After extensive research, we have found that not only is TikTok a massive security flaw waiting to happen, but the ties that they have to Chinese parties and Chinese ISP's make it a very vulnerable source of data that still has more to be investigated."*[28]

Unlike Facebook which analyses your current friendship network, TikTok uses a behavioural profile powered by artificial intelligence to populate a user's feed before friends are even added. It also predicts the type of friends you should have for your personality.[29]

Once outfitted with this information, the TikTok AI has the capacity to train users using similar methods that dog trainers use, i.e. deploying positive and negative feedback loops to encourage TikTok users to behave in certain ways. In practice the user would see a feed of people they are not necessarily linked to. Initially the videos would appear funny and generate positive emotions, at which point they would be directed to a propaganda video generated by the CCP with the hope they would then share it. With repeated exposure the positive emotions will become subconsciously linked to the propaganda message in the same way a dog can be made to sit with food training.

The technology further has the capacity to create a user-specific profile[30] of individuals' fears and anxieties, learning which stimuli are likely to trigger desired responses and behaviours. It could then utilise addictive principles and implement stimuli that compel young adults to spend hours scrolling on their phone, purchase products, or join political movements. These algorithms are bespoke to the user and are powerful due to a century's worth of research into shaping human behaviour.

The Financial Times published my findings on the 17th August, 2020. Dr. Robert Lustig, author of "Hacking of the American Mind" and a paediatric endocrinologist who has looked closely at how neuromarketing can influence addictive behaviours online was asked how plausible my

[26] https://www.reddit.com/r/videos/comments/fxgi06/not_new_news_but_tbh_if_you_have_tiktiok_just_get/fmuko1m/
[27] https://www.reddit.com/r/videos/comments/fxgi06/not_new_news_but_tbh_if_you_have_tiktiok_just_get/fmuko1m/
[28] https://penetrum.com/research
[29] https://towardsdatascience.com/why-tiktok-made-its-user-so-obsessive-the-ai-algorithm-that-got-you-hooked-7895bb1ab423
[30] https://towardsdatascience.com/why-tiktok-made-its-user-so-obsessive-the-ai-algorithm-that-got-you-hooked-7895bb1ab423

finding was that users could be being groomed on apps like TikTok through addictive processes? His answer was:

"Absolutely. These apps are engineered to generate dopamine AND cortisol. If it were just dopamine, they would not be addictive. But they do both, in part due to peer pressure, which is particularly problematic in the teen age group. I can't specifically tell you how TikTok does it (I have not investigated personally), but my understanding is that kids are supposed to generate their own content — but that it gets "liked", just like Facebook. And that's where the addiction comes. And we've learned that anything that generates both dopamine and cortisol will turn the prefrontal cortex offline. In fact, a colleague in Paris and I are building a "robotic limbic system" to test this exact paradigm. So far it works! Which is not good news for kids."[31]

The psychology in question

The propaganda techniques described are based on well-established behavioural psychology discoveries from the last century which showed how human behaviour could be moulded by stimulating primordial brain pathways - i.e. with well-timed reward or punishment stimuli. In the 1950s, Harvard psychologist Burrhus Frederic "BF" Skinner created the Skinner Box[32] to study how these stimuli affect rat behaviour. It is an isolated enclosure equipped with a food dispenser, electrified floors and levers: using computers to precisely measure and control experimental conditions.

He taught birds to play "ping pong"[33] and cats to play the piano by breaking tasks into small parts and rewarding success (or punishing failure). Humans it turns out are no different. They too can be trained subconsciously through graduated steps with feedback at each stage. Sheldon Cooper even used it to train[34] Penny in the "Big Bang theory".

It is reasonable to suggest that TikTok might be able to operate like a modern-day digital Skinner Box wherein bespoke AIs are released to exploit users' behavioural profiles and guide their experiences of their service so as to stimulate specific behaviours.

Based on its data access potential it knows what a child is doing whether it is going to school, eating dinner or watching television. It knows what causes the user to experience specific emotions and how to combine stimuli to create a response.

This information conceivably allows the app to insert fake news into a news feed at the exact moment a user is experiencing an intense emotion. Like an electric shock, a video can be scheduled to exacerbate their greatest fears to make them more susceptible to persuasion. Over time, in the same way that a cat can be taught to play the piano, your child can be subconsciously taught to associate positive emotions to whatever TikTok desires, all the while shielded from parental oversight. In 1948, Skinner predicted this dystopian future.[35] He envisaged a utopian society where the government controlled all aspects of life to condition the population to conform to a predetermined set of behavioural standards. An idea eerily reminiscent of China's Social Credit system.

[31] https://ftalphaville.ft.com/2020/08/14/1597405270000/Cognitive-hacking-as-the-new-disinformation-frontier-/
[32] https://www.youtube.com/watch?v=CtoH5tlr-bI
[33] https://www.youtube.com/watch?v=vGazyH6fQQ4
[34] https://www.youtube.com/watch?v=bDZCyObMfkA
[35] https://en.wikipedia.org/wiki/Walden_Two

Are we all becoming Manchurian Candidates?

The reason why TikTok has generated a security panic in Washington is tied not just to the fact that data harvested by the platform's Chinese owner ByteDance may be being transmitted back to China, but also because the Chinese government may already be using this data to exploit user vulnerabilities.

Some of the evidence for this is in the public domain. In 2018, for example, ByteDance's founder Zhang Yiming publicly pledged to use his company to *"promote socialist core values"*, adhere to the Chinese Communist Party's ideology, political thinking and deeds, *"deepen cooperation"* with state propaganda and *"integrate the right values into technology and products."* [36]

In September 2020, the CCP propaganda ministry announced that it will send government officials into companies such as Alibaba to ensure they comply with the regime's propaganda goals.[37] They published guidelines calling on its members to "educate private business people to weaponise their minds with [Xi's] socialism ideology."[38] The directive said the private sector needs "politically sensible people," who will "firmly listen to the party and follow the party." The message from the propaganda ministry to ByteDance and TikTok is very clear; ***it doesn't matter how big you get or how many investors you have from the United States; in the end, you must follow the party - if the party doesn't approve a TikTok deal, or the Chinese Government wants access to its source code; there may be nothing ByteDance can do.***

TikTok has a remarkably similar behavioural profiling AI[39] to its Chinese version Douyin -- which is also owned by ByteDance but can only be downloaded in China. The Chinese Propaganda ministry published that; "Tic Tok and Douyin…have the same source code" in their official mouthpiece, The Global Times. The same source code that powers Douyin, a tool used by the Chinese Communist Party to facilitate the brutal crackdown on their own population, may power TikTok a smartphone application used by children.[40] [41]

Just like TikTok, Douyin too creates a profile of existing fears and anxieties to predict and influence behaviour through well-timed triggers.[42] Douyin is compelled by Chinese Law[43] to share any information the Chinese Government requests. The technology in this way has the capacity to serve the Communist regime to help feed data to China's Social Credit System, which seeks to assign citizens scores and thereby engineer social behaviour.[44] Data has already been used to ban more than seven million people deemed "untrustworthy" from boarding flights and nearly 3 million others from riding on high-speed trains.[45]

[36] https://medium.com/@pandaily/open-apology-from-ceo-of-toutiao-following-the-ban-of-neihan-duanzi-6381000939d0
[37] https://edition.cnn.com/2019/09/24/business/china-government-officials-companies/index.html
[38] https://edition.cnn.com/2019/04/08/asia/china-students-socialist-theory-app-intl/index.html
[39] https://en.wikipedia.org/wiki/TikTok
[40] https://www.globaltimes.cn/content/1201625.shtml
[41] Such a confirmation could only be published with the official knowledge and endorsement of the CCP.
[42] https://www.scmp.com/abacus/who-what/what/article/3028253/tiktok-viral-short-video-sensation-has-its-roots-china
[43] https://oxford.universitypressscholarship.com/view/10.1093/oso/9780190685515.001.0001/oso-9780190685515-chapter-11
[44] https://www.wired.co.uk/article/china-social-credit-system-explained
[45] https://www.abc.net.au/news/2018-03-31/chinas-social-credit-system-punishes-untrustworthy-citizens/9596204

Chinese authorities recently announced they would seek to freeze the assets of those deemed "dishonest people".[46] These intimate profiles are also used by the totalitarian regime to curate social media feeds to distract from undesirable political ideas such as “free speech” or the protests in Hong Kong.[47] In some cases, the data the CCP collects is used to isolate and flag enemies of the people for arrest and shipment to concentration camps.[48] Former Google CEO Eric Schmidt recently warned about Chinese AI stating: "*Trust me, these Chinese people are good. They are going to use this technology for both commercial as well as military objectives with all sorts of implications,"* and they are.[49] Hence the panic. This AI is most likely already being used by the Chinese government to attempt to exert social and political control to pre-emptively shape how people behave on a scale never seen before in human history.

Reddit CEO Steve Huffman went further. He described the app as “fundamentally parasitic” warning that it was always listening and that the fingerprinting technology used was truly terrifying. “I could not bring myself to install an app like that on my phone,” he said.[50]

What’s even more frightening is that TikTok is actively hiding how their AI system curates users’ feeds. ByteDance tells us that it is trying to separate the Chinese version of the app from TikTok.[51] Yet with every month that passes, we find growing evidence that a core aspect of China’s totalitarian control system is built into the western applications.

TikTok has also been found to suppress videos by users with an "abnormal body shape", "too many wrinkles," or "eye disorders".[52] Worse still, it had a policy of systematically suppressing videos featuring disabled people with "autism" or "Down's syndrome". A disabled German user, for example, was branded by the app a "special user".[53] It was also reported that the app censored videos mentioning Hong Kong Protests, Tibetan independence and the Tiananmen Square massacre.[54] TikTok claims that these practices have stopped. But the question remains: can we trust a company that has openly aligned itself with assisting a totalitarian regime?

Oracle purchasing TikTok and storing all user data in the United States is a step forward but may not be enough to keep users safe. Data breaches are not the real concern and never have been. The real threat is the true agenda of the artificial intelligence[55] that uses TikTok data for manipulation purposes.[56] Irrespective of whether Oracle or any other US company buys the company, these AI algorithms will remain in place along with unknown back-doors geared at manipulating users - originally created by a totalitarian regime. Considering the

[46] https://www.abc.net.au/news/2018-03-31/chinas-social-credit-system-punishes-untrustworthy-citizens/9596204
[47] https://www.cambridge.org/core/journals/american-political-science-review/article/how-the-chinese-government-fabricates-social-media-posts-for-strategic-distraction-not-engaged-argument/4662DB26E2685BAF1485F14369BD137C/core-reader
[48] https://www.nytimes.com/2019/05/22/world/asia/china-surveillance-xinjiang.html
[49] https://www.insider.com/eric-schmidt-on-artificial-intelligence-china-2017-11
[50] https://techcrunch.com/2020/02/26/reddit-ceo-tiktok-is-fundamentally-parasitic/?guccounter=1
[51] https://www.economist.com/business/2020/07/25/tiktoks-chinese-parent-is-scrambling-to-hang-on-to-its-hit-app
[52] https://theintercept.com/2020/03/16/tiktok-app-moderators-users-discrimination/
[53] https://netzpolitik.org/2019/discrimination-tiktok-curbed-reach-for-people-with-disabilities/
[54] https://www.bbc.com/news/technology-49826155
[55] https://towardsdatascience.com/why-tiktok-made-its-user-so-obsessive-the-ai-algorithm-that-got-you-hooked-7895bb1ab423
[56] https://towardsdatascience.com/why-tiktok-made-its-user-so-obsessive-the-ai-algorithm-that-got-you-hooked-7895bb1ab423

regular Microsoft Windows security updates, we could never be sure all backdoors in the source-code would be secure.

China has used US companies to facilitate technology transfer, raising moral and security concerns as to how TikTok's AI will interact with users even under US control.[57] Microsoft itself has worked with a Chinese military-run university on artificial intelligence research that could be used for surveillance and censorship.[58] Twitter, another potential purchaser, recently added former Google AI chief Fei-Fei Li to its board of directors. She is reported to have links to the "United Front", the overseas influence arm of the Chinese Communist Party. In a 2017 interview she pledged to help China develop its AI capabilities and used the CCP slogan "stay true to our founding mission" and "China has awakened."[59]

A deal that fails to protect the public

In August 2020, the United States President issued executive orders against ByteDance to divest all interests and rights in TikTok. The order classified TikTok as a national security threat referencing that TikTok's *"data collection threatens to allow the Chinese Communist Party access to Americans' personal and proprietary information"* and TikTok *"censors content that the Chinese Communist Party deems politically sensitive, such as content concerning protests in Hong Kong and China's treatment of Uyghurs and other Muslim minorities."*[60] In September 2020, it was announced that TikTok may be acquired by the US company Oracle.[61] Unfortunately, the Chinese Communist Party has circumvented the intent of the executive orders. The conditions imposed by the CCP in the planned partnership between Oracle and ByteDance make it impossible to address national security concerns.

The deal only provides for Oracle to take over TikTok's US hosting. It does not resolve any of the issues surrounding Chinese influence efforts and invalidates US Intelligence efforts to protect the public. Oracle won't have control over the AI algorithms behind the app, a protection Beijing insisted on before it would approve the deal - meaning China will still have control over the controversial AI system this application uses.

Taking over the source code and the algorithms is the *only* way to ensure ByteDance's Chinese engineers were not designing code and algorithms to affect what users saw, or did not see. The Whitehouse should insist Oracle control TikTok's data and algorithms from the day of the acquisition and move source code for the algorithms to the United States. Otherwise, there is little way to stop ByteDance or the Chinese Communist Party from smuggling in malware. In this proposed deal, Oracle won't be rewriting the TikTok algorithm or handling moderation, so it will be just as easy for ByteDance to push Chinese propaganda or censor embarrassing messages. Oracle will be a contractor rather than a subsidiary, and vulnerable to pressure from China.

The major risks TikTok poses to the Australian population have not been addressed and we should be very concerned.

---

[57] https://www.uscc.gov/sites/default/files/Research/How%20Chinese%20Companies%20Facilitate%20Tech%20Transfer%20from%20the%20US.pdf

[58] https://www.ft.com/content/9378e7ee-5ae6-11e9-9dde-7aedca0a081a

[59] https://www.rfa.org/english/news/china/concern-05202020134312.html

[60] https://www.whitehouse.gov/presidential-actions/executive-order-addressing-threat-posed-tiktok/

[61] https://edition.cnn.com/2020/09/14/tech/oracle-tiktok-us-china-intl-hnk/index.html

Conclusion

In recent times, the Australian public has started to realise that the Chinese Communist Party is systematically working to undermine Australian national security. One method is via social media applications such as TikTok; which currently remains a platform for censorship and propaganda while gathering an extraordinary amount of data on Australian users. The CCP uses similar platforms domestically to control and persecute its population. The regime understands the enormous influence social media exerts in manipulating politics and national elections. It seeks to exercise some of this same influence, and same power, more directly here in Australia, in an effort to control what Australians see, hear, and ultimately think. TikTok poses a clear national security risk to the Australian population and should be banned.

I urge the Australian Government to take all measured actions necessary to protect Australians and our national interest: insisting on an outright sale of TikTok or, if necessary, ban the application to protect Australian national security.