December 2022

POLICY BRIEF

The Mysterious TikTok-ing Noise

Noah Diekemper
Senior Research Analyst

WISCONSIN INSTITUTE
FOR LAW & LIBERTY

Introduction

In July of 2020, Joe Biden's presidential campaign instructed their staff to delete the app "TikTok" from their phones.[i] This month, Wisconsin's Republican congressional delegation sent an open letter to Governor Tony Evers urging him, in essence, to follow suit—to ban TikTok from Wisconsin government devices and to delete his own accounts.[ii] The federal government and several other states have also sought to curb the risk posed by the app by banning TikTok from devices on public employees' phones—just last week, the US Senate unanimously passed a bill that would ban the app on government phones.[iii] While banning the app beyond government-owned devices would implicate a different set of principles, the government is on firm footing protecting their own devices from the threats posed by this software. We wanted to explore in a little more detail the technology that the app contains, what that power could look like in the wrong hands, and why this proposal makes sense.

The Rise of TikTok

TikTok only launched five years ago, but in that time it has skyrocketed to dominance. It was assessed by one web-performance company to be the most popular website of 2021—even beating out Google.[iv] The app is estimated to have more than 138 million active users here in the United States, with about 62% of them under the age of 40.[v] You could correctly call it the app of choice among young people, and it has alarming ubiquity among older Americans as well.

TikTok's parent company, ByteDance, is headquartered in Beijing.[vi] Although TikTok is not a part of the Chinese government or owned by them, it is important to acknowledge the inherent risk of that situation. China is a communist-run "people's republic" with a powerful central government.[vii] TikTok's own professed safeguards to firewall U.S. data from the Chinese government, such as the idea that TikTok houses U.S. data on servers outside of Chinese soil, have been repeatedly challenged—leaked and confirmed audio revealed that ByteDance employees in China routinely accessed nonpublic data on U.S. users after all.[viii] And to cap it all off, the Chinese government recently acquired a 1% stake in the company[ix] and placed a Chinese government official on the Board of Directors.[x] All told, there is ample reason to distrust that the Chinese government will refrain from controlling TikTok, either as a source of data or as a tool to be used offensively.

China

The West was alerted to the Chinese government's violent character with the Tiananmen Square protests of June 4, 1989, which saw the government open fire and massacre a still-unknown number of civilians that is at least in the multiple hundreds.[xi] China has increasingly caught international flack for concentration camps in which they've interned perhaps a million individuals of the country's Muslim minority (the Uyghurs).[xii] They have earned scrutiny for the circumstances that led to them suppressing information about the novel coronavirus—from silencing the would-be whistle-blower who was initially concerned,[xiii] to suppressing case numbers and information about the disease,[xiv] among many other nefarious actions.[xv] There is widespread concern that China's president-for-life is considering a Putin-style invasion of the island of Taiwan.[xvi]

One of China's weapons of choice for pursuing their interests is technology. "The Chinese government—officially known as the People's Republic of China (PRC)—engages in malicious cyber activities to pursue its national interests," writes the Department of Homeland Security's Cybersecurity & Infrastructure Security Agency.[xvii] They detail: "Malicious cyber activities attributed to the Chinese government targeted, and continue to target, a variety of industries and organizations in the United States, including healthcare, financial services, defense industrial base, energy, government facilities, chemical, critical manufacturing (including automotive and aerospace), communications, IT (including managed service providers), international trade, education, video gaming, faith-based organizations, and law firms."

In all, the PRC is a coordinated and powerful force that aspires to power on the world stage and is willing to use inhumane, violent, and unjust means in pursuit of that power. TikTok's software has the potential to give them personally identifying and compromising information on other people—this is a public concern when those people are in positions of governmental power.

What TikTok Can Do

TikTok collects information on its users. Its privacy policy states point-blank:

"We collect certain information about the device you use to access the Platform, such as your IP address, user agent, mobile carrier, time zone settings, identifiers for advertising purposes, model of your device, the device system, network type, device IDs, your screen resolution and operating system, **app and file names and types, keystroke patterns or rhythms**, battery state, audio settings and connected audio devices. Where you log-in from multiple devices, we will be able to use your profile information to identify your activity across devices . . . **We may collect information about the images and audio that are a part of your User Content, such as identifying the objects and scenery that appear, the existence and location within an image**

of face and body features and attributes, the nature of the audio, and the text of the words spoken in your User Content."[xviii] (Emphases added.)

It doesn't end there. TikTok also acknowledges that "We may collect **biometric identifiers and biometric information as defined under US laws, such as faceprints and voiceprints, from your User Content."** (Emphases added.)

All of that is just the information that TikTok is public and up-front about collecting. A 2020 analysis by an Australian cybersecurity firm found that TikTok helps itself to more data on a phone than what it is clear about accessing—that it also explores a phone's calendar, contact list, and photos.[xix]

There is, ultimately, concern that TikTok knows people's usernames and passwords for anything accessed on mobile—including email accounts, banking information, and credit card numbers. TikTok's source code was analyzed by a former Google and Twitter developer who went public with his findings: "TikTok injects JavaScript through their in app browser that has code in place to track keystroke happening on third party websites."[xx] Tracking users' individual keystrokes gives TikTok the chance to record things like credit card numbers and passwords. Though other social media services are known to have data collection whose scope makes people uncomfortable when they're described, this is transgressive even by those standards. As the *New York Times* reported, "But while Facebook and Instagram can use in-app browsers to track data like what sites a person visited, what they highlighted and which buttons they pressed on a website, TikTok goes further by using code that can track each character entered by users, [the analyst] said."[xxi]

This developer is careful to hedge that what he's conclusively detected is merely the capability to do so, and not evidence of TikTok doing this—but it's hard to explain why they'd build out this capability to begin with,[1] or why a known bad-faith actor like the PRC wouldn't make use of it. After all, U.S. government agencies routinely publish reports on nefarious exploits used by the PRC. "PRC state-sponsored cyber actors continue to exploit known vulnerabilities to actively target U.S. and allied networks as well as software and hardware companies to steal intellectual property and develop access into sensitive networks," reads one report published two months ago.[xxii]

[1] As reported in the *Times*, the company's official response was that the capability was (somehow) for "debugging, troubleshooting and performance monitoring." Again, this is capability that is unusual for comparable social media apps, and the material discussed later in this report provides (if any was needed) more reason to doubt the goals that TikTok's operating company's self-proclaimed end goals aren't trustworthy enough to be accepted at face value.

The Threat to State Employees

For all of the chatter about data aggregation and learning algorithms, it's important to recognize that TikTok has capabilities that let it profile and surveille specific individuals. Materials reported on by Forbes just two months ago found exactly that—namely, that TikTok's parent company had, on at least two separate occasions, planned to collect data on U.S. citizens.[2,] [xxiii]

If TikTok can target and surveille individuals, it's important to ask what leverage they could wield over government employees. Even Uber came under criticism for reportedly offering an altered version of their app at government actors and regulations in an attempt to escape scrutiny.[xxiv] So much less should the personal accounts and profiles of public servants be in the hands of a hostile foreign power.

It's hard to know where to begin enumerating the possible disastrous outcomes if they should choose to exercise this kind of leverage. One real-life example from recent history is instructive: in May of 2019, the city of Baltimore, Maryland, was hit by a cyberattack.[xxv] City employees were locked out of their email accounts. Impound lots couldn't process and return vehicles. The Department of Public Works couldn't process billing. All official city card payment systems were offline—parking ticket and property tax payments and other such transactions became conducted by pen and paper.[xxvi] Hackers (who have never been identified) demanded about $75,000 in ransom to return functionality (which the City refused to pay). All told, numerous public services ground to a halt and then to a grinding manual pace for months. The City expended upwards of $18 million recovering their systems and capabilities.

For all that went wrong, the city's emergency response services (911 and 311) were not affected. But they *had* been shut down by a brief, separate hacking attack in 2018.[xxvii]

This is the sort of attack that would be facilitated by having access to individual security information. The PRC is already known to work on remote code execution attacks even without the advantage of things like direct passwords.[xxviii] But even if this is an extreme example, that doesn't absolve us of responsibility for safeguarding against it, nor of safeguarding against all the lesser types of potential attacks.

There are many other, more creative examples of possible threats. An enemy having a comprehensive understanding of networks, built up through contact lists and scheduled meetings (see above), could allow it to influence decision-making in subtler and more sustainable ways. Having lots of information of people's habits and identities could facilitate the crafting of cover stories for actual, on-the-ground espionage.[xxix] The congressional delegation's letter raises the fact that a significant number of people consume the news through TikTok—giving an adversary the power to influence that public perspective, whether among an entire population or among

[2] This was partly significant because of TikTok's official repeated insistence that U.S. users' data is inaccessible to its Chinese owners. There's ample reason to doubt that, e.g. at the source cited in the endnote.

targeted groups (like just political leaders' circles) is a recipe for disaster. Having access to state actors' personal photos on their phones (see above) opens the door to the kind of compromising material and blackmail that has been such a concern in recent years.[xxx] These are short- as well as medium- and long-term threats: nefarious actors could blackmail employees and hold embarrassing or incriminating information over their heads. Alternatively, Wisconsin state employees who become candidates for higher office disfavored by the Chinese regime might find compromising material about themselves widespread online prior to an election or appointment. That kind of selective targeting of candidates isn't a power to which we should even put ourselves at risk.

These concerns have been echoed by the FBI, which testified before a House committee last month about "a number of concerns," including "the possibility that the Chinese government could use it to control data collection on millions of users or control the recommendation algorithm, which could be used for influence operations if they so chose, or to control software on millions of devices, which gives it an opportunity to potentially technically compromise personal devices."[xxxi]

This is why the American government has already begun normalizing bans of this software. Back in 2019, U.S. Senators Chuck Schumer (D-NY) and Tom Cotton (R-AR) co-signed a letter to the then-Acting Director of National Intelligence "to express our concerns about TikTok."[xxxii] The Pentagon issued a warning later that year about TikTok's presence on devices, which resulted in some subsequent bans throughout the Defense Department and the branches of the military.[xxxiii] Nebraska forbade it from state devices two and a half years ago.[xxxiv] More recently, South Carolina,[xxxv] South Dakota,[xxxvi] and Texas[xxxvii] have followed suit. Most recently, the cyber and governmental hub of Maryland (home of the Baltimore ransomware attack) announced a ban on TikTok, as well as some Russian-based platforms, within the state's executive branch on Wednesday, December 7. Governor Larry Hogan explained, "There may be no greater threat to our personal safety and our national security than the cyber vulnerabilities that support our daily lives."[xxxviii]

Bans within Government

Wisconsin's Republican Congressional delegation is right, TikTok should be banned on state devices. This is a fundamentally different question from banning the device from individuals' personal phones or even doing an end-run around that question by pressuring companies to do so. The government has well-known discretion when it comes to regulating its own operations and when it comes to policy concerning foreign actors—this issue implicates both.

Foremost, then, a ban on TikTok within government means that action should be taken within Wisconsin's executive branch to ban the app on any and all government-owned technology. Employees should be strongly discouraged from having accounts on their personal devices, and should be prevented from having the technology in use on state property or during official hours. Governor Evers should follow the example of now-President Biden's campaign team and delete his own accounts as well.[xxxix] This is the sort of administrative decision that the head of the

executive branch is empowered to make on his own, separate from any consultation with the legislature.

Lawmakers in the legislature, for their part, would be well advised to follow suit with any personal accounts and devices of theirs. They should also encourage staffers to divest themselves from the app, though that specifically isn't a matter for coercion.

Conclusion

China is a hostile foreign power that controls an app that can access individuals' most personal and private information—from contacts and calendar appointments to credit card numbers, passwords, and photos. All of this valuable, personal information is effectively in the hands of the same state actor that already leverages technology in nefarious ways to undermine and best America. Wisconsin is opening itself up to enormous vulnerability at the hands of a merciless enemy by allowing government employees to let this nefarious software live on their phones. We should follow the collective guidance of Senators Schumer and Cotton, of Texas and Maryland, of Wisconsin's Republican congressional delegation and now-President Biden. TikTok should be banned.

Endnotes

[i] https://www.cnn.com/2020/07/28/politics/biden-campaign-tiktok/index.html
[ii] https://www.ronjohnson.senate.gov/services/files/7B5A48E1-AD49-4E18-9C2C-455BF1660F68
[iii] https://thehill.com/policy/technology/3775845-senate-votes-to-ban-tiktok-use-on-government-devices/
[iv] https://www.nbcnews.com/tech/tech-news/tiktok-surpasses-google-popular-website-year-new-data-suggests-rcna9648
[v] https://wallaroomedia.com/blog/social-media/tiktok-statistics/
[vi] ByteDance Corporate Headquarters, Office Locations and Addresses | Craft.co
[vii] https://www.britannica.com/summary/China
[viii] https://www.forbes.com/sites/emilybaker-white/2022/09/14/tiktok-china-ties-senate-hearing/?sh=2a880cc23ff5
[ix] https://www.washingtonpost.com/technology/2021/08/17/chinese-government-bytedance-tiktok/#:~:text=China%E2%80%99s%20government%20has%20acquired%20a%201%20percent%20stake,the%20condition%20of%20anonymity%20to%20discuss%20sensitive%20matters.
[x] Chinese government appoints director to board of ByteDance Beijing: Report (medianama.com)
[xi] https://content.time.com/time/subscriber/article/0,33009,970278,00.html
[xii] https://www.bbc.com/news/world-asia-china-22278037
[xiii] https://www.bbc.com/news/world-asia-china-51403795
[xiv] https://apnews.com/article/virus-outbreak-health-ap-top-news-international-news-china-clamps-down-68a9e1b91de4ffc166acd6012d82c2f9
[xv] https://www.youtube.com/watch?v=G5VGPYtbTk8
[xvi] https://www.theatlantic.com/international/archive/2022/12/taiwan-xi-jinping-china-invasion-us-support/672336/
[xvii] https://www.cisa.gov/uscert/china#chinese
[xviii] https://www.tiktok.com/legal/page/us/privacy-policy/en#privacy-us
[xix] https://www.gizmodo.com.au/2022/07/tiktok-app-phone-access/
[xx] https://www.vice.com/en/article/5d3dmd/tiktok-says-no-it-isnt-stealing-your-passwords
[xxi] https://www.nytimes.com/2022/08/19/technology/tiktok-browser-tracking.html
[xxii] https://media.defense.gov/2022/Oct/06/2003092365/-1/-1/0/Joint_CSA_Top_CVEs_Exploited_by_PRC_cyber_actors_.PDF
[xxiii] https://www.forbes.com/sites/emilybaker-white/2022/10/20/tiktok-bytedance-surveillance-american-user-data/?sh=2fd2d7dd6c2d
[xxiv] https://www.nytimes.com/2022/08/19/technology/tiktok-browser-tracking.html
[xxv] https://heimdalsecurity.com/blog/baltimore-ransomware/
[xxvi] https://www.vox.com/recode/2019/5/21/18634505/baltimore-ransom-robbinhood-mayor-jack-young-hackers
[xxvii] https://www.nbcnews.com/news/us-news/baltimore-s-911-emergency-system-hit-cyberattack-n860876
[xxviii] https://www.cisa.gov/uscert/ncas/alerts/aa22-279a
[xxix] This was a tactic of the Soviet Union's. See e.g, Zink, Lubor J., *What Price Freedom?* pp. 144-46.
[xxx] https://www.cnn.com/2017/01/11/politics/what-is-kompromat/index.html
[xxxi] https://www.npr.org/2022/11/17/1137155540/fbi-tiktok-national-security-concerns-china
[xxxii] https://www.democrats.senate.gov/imo/media/doc/10232019%20TikTok%20Letter%20-%20FINAL%20PDF.pdf
[xxxiii] https://www.nytimes.com/2020/01/04/us/tiktok-pentagon-military-ban.html
[xxxiv] https://governor.nebraska.gov/press/gov-ricketts-announces-tiktok-app-ban-state-devices
[xxxv] https://www.wistv.com/2022/12/05/tiktok-blocked-mcmaster-bans-app-government-devices/
[xxxvi] https://www.wsj.com/articles/south-dakota-bans-tiktok-surveillance-beijing-ccp-government-devices-data-farm-food-security-app-noem-11670277776
[xxxvii] https://www.axios.com/2022/12/07/tiktok-national-security-republican-governors
[xxxviii] https://www.npr.org/2022/12/07/1141338246/tiktok-maryland-ban-cybersecurity-china
[xxxix] https://www.cnn.com/2020/07/28/politics/biden-campaign-tiktok/index.html