TikTok bans: What the evidence says about security and privacy concerns

March 15 2023, by Benjamin Dowling

Some concerns centre around the ability to construct profiles of individual users. Credit: Shutterstock

The U.K. prime minister, Rishi Sunak, recently hinted that he may ban the social media application TikTok from devices used by government

employees.

His comments follow similar bans by the European Commission and U.S. federal government. In the EU and U.S. cases, security concerns were used as the justification for a ban. Unlike Facebook or Instagram (both owned by US-based Meta), TikTok is owned by ByteDance, which is based in China.

Such concerns are not new. In October 2022, the former U.S. secretary of state Mike Pompeo described his fear that China could compel TikTok to act as a "Trojan horse," accessing and exploiting sensitive data on users' devices.

TikTok, like many social media applications, collects significant amounts of user data including dates of birth, email addresses and telephone numbers.

Discussions around privacy in social media applications usually concern excessive collection of data that users consent to handing over. TikTok's privacy policy says the app collects user location data, up to a granularity of three square km. This is quite coarse—Instagram, for example, allows for more precise location tracking.

Instagram says this is for personalizing advertisements. But the risk is that, if exposed, location data could be used by malicious parties to track users, enabling behavior such as intimate partner stalking. This kind of location data was involved in an alleged effort by TikTok employees (who were subsequently reported to have been sacked) to determine the location of US-based journalists—in a bid to catch leaks from inside the company.

In an email published by Forbes magazine, ByteDance chief executive Rubo Liang wrote that he was "deeply disappointed" by the episode.

Access to user data enables businesses to build profiles for specific users. The increasing availability to the public of software tools using machine learning—a type of AI that improves at a task with experience—has caused some cybersecurity analysts alarm.

These experts are concerned about the potential use of this technology for "targeted phishing attacks." In these attacks, victims receive communication, such as an email, that impersonates a trusted source, prompting the victim to engage with a scam.

Social media applications have significant knowledge of their users. So it's entirely plausible that building a profile from user data could enable targeted phishing attacks on sensitive government accounts. However, there is no evidence TikTok has been used for this purpose.

Industry standards

ByteDance has responded to recent bans by saying it has not provided user data to the Chinese government. It also claims that its data collection practices align with those of other social media companies. A cursory comparison with the privacy policy of Instagram supports this view: the identifying information collected by Meta from Facebook and Instagram generally matches the information TikTok collects in terms of device information, social media graphs and location information.

Some criticisms of applications such as TikTok have centered on a claim that they function as spyware. The goal of spyware, in comparison to data collection, is to extract confidential or sensitive information that users did not consent to providing. For instance, spyware may target information that the user has copied into the clipboard of their device.

Common advice is to use complex and unique passwords for every online account. So people who are concerned about privacy will often

use password managers such as LastPass or 1password.

However, these users are likely to copy and paste the complex password from their password manager into an account's log-in mechanisms. Extracting clipboard information allows those with malicious intent to recover passwords and access sensitive accounts.

Evaluating the risk

TikTok is a "closed-source application," which means the source code—the underlying instructions—used to build the application is not available. However, there have been efforts to reverse-engineer TikTok's source code. These efforts have been used to determine whether the app behaves as spyware, or otherwise collects user data in ways that are excessive.

A report by Citizen Lab Research described the reverse-engineering of an Android-distributed version of TikTok. It concluded: "TikTok… (does) not appear to exhibit overtly malicious behavior" such as that displayed by spyware. Furthermore, the report says that while TikTok collects a large variety of device information and usage pattern information, "(these) characteristics are not exceptional when compared to industry norms."

It is reasonable to conclude that Tiktok itself does not necessarily present a much greater risk in this regard than other US-based social media applications, a conclusion shared by the Electronic Frontier Foundation.

The recent bans prompted ByteDance to strengthen privacy protections for users. Specifically, ByteDance announced Project Clover, which outlines strategies for improving European data security.

Project Clover proposes a so-called European Enclave, which aims to

guarantee that ByteDance employees cannot access or transfer European user data externally without complying with data protection laws such as GDPR. It would also be overseen by a third-party European security company—discussions between ByteDance and this third-party are currently ongoing.

User protections

ByteDance has also proposed two mechanisms for anonymizing user data, the goal of which is to ensure that any malicious parties that wanted to access TikTok user data could not exploit it for phishing or other types of attack. The first approach is to "pseudonymize" personal data collected from users to align with Article 4(5) of GDPR. This would require personal data to be processed in such a way that it cannot be linked to specific users without the use of additional, external information.

ByteDance will also aggregate information from users in large data-sets, achieving anonymity by separating the details from a particular user's profile. Thus, the recent TikTok ban from the European Commission highlights a growing perception from governing bodies that TikTok and other applications could potentially harm user security and privacy through targeted and excessive data collection.

While this has caused ByteDance to propose strengthened privacy protections, users must wait for these to materialize, and for experts to verify them. In the meantime, the onus remains on users to manage their own privacy and decide for themselves whether the risks presented by social media applications like TikTok are worth the value they provide.

Provided by The Conversation