TechXplore

Opinion: Australia needs a robust cybersecurity overhaul, not whack-a-mole bans on apps like TikTok

April 14 2023, by Lyria Bennett Moses

Credit: Unsplash/CC0 Public Domain

Australia has joined other countries in announcing a ban on the use of TikTok on government devices, with some states and territories following suit. The rationale was based on security fears and, in particular, the risk the platform will be used for foreign interference operations by China.

TikTok is a video-sharing platform operated by ByteDance, a company headquartered in Beijing, but incorporated in the Cayman Islands. Data is allegedly stored in the US and Singapore.

Like similar sites, TikTok's privacy policy indicates an expansive approach to the collection and use of personal information. It can collect information from users and third parties (such as advertisers), and it can draw inferences about its users' interests.

All of this information can then be shared with TikTok's partners and service providers to, among other things, personalize content and advertising.

The policy also says information will be shared when there is a legal requirement to do so. China's national intelligence law obliges citizens and organizations to support, assist and cooperate with national intelligence efforts, which could include ByteDance sharing people's TikTok data.

While TikTok denies it would hand over data in such circumstances, there are reports that data from American users has been accessed by China-based employees. TikTok has also censored content that is politically sensitive in China.

The problem with focusing on only one app

While the Australian government's response can be explained through this logic, questions remain.

Given the ban only affects government devices, couldn't the same people be susceptible to foreign interference through their use of TikTok on personal devices?

What about other apps, such as Facebook, that collect significant amounts of user data—are these more secure than TikTok? Even if other digital platforms don't have connections with China, couldn't they share or sell data to other entities, such as advertisers, data brokers or business partners? And mightn't those third parties have connections with China? Or other countries with similar laws?

A final point: foreign interference can take place on a range of digital platforms. Russia has run information campaigns designed to influence US elections using platforms such as YouTube, Tumblr, Google, Instagram, PayPal, Facebook and Twitter.

In other words, the problem of digital security and foreign interference is bigger than just one app or the use of government devices.

Indeed, the Department of Home Affairs notes that foreign interference activities are not only directed towards government, but also academia, industries, the media and other communities (which is actually everyone).

Banning TikTok on government devices does eliminate one risk, but the broader pool of risks remain both in government and beyond.

A new, more effective cybersecurity strategy

The government is currently developing a new cyber security strategy to replace the one put in place by the previous government just three years ago.

A discussion paper on the new strategy was released earlier this year, with submissions due this week.

This process will hopefully result in a more holistic strategy on how to manage the cybersecurity and foreign interference concerns that led to the TikTok ban.

Rather than the whack-a-mole tactical response of banning one app at a time, the strategy could provide clarity on how the government will manage issues around weak security on mobile apps (particularly used by people in sensitive sectors), as well as the potential for this to be an entry point for foreign interference.

This could include such things as:

- educating people on digital security and foreign interference
- streamlined reporting channels for data breaches, foreign interference attempts, cybercrime, bugs and vulnerabilities
- developing or recommending the use of appropriate standards on cybersecurity, which could include references to international standards in areas such as information security and data governance
- strengthening cooperation between government and platforms and civil society
- targeted prohibitions, which may include bans on apps that could share data with countries that might then use it for foreign interference.

This kind of strategic approach, particularly on the education side, would give Australians better tools to arm themselves against foreign interference online, which as Home Affairs emphasizes, is the "best defense" available.

A stronger privacy act could help, too

Another relevant policy development is the government's review of the Privacy Act, which is the primary Australian law on data protection.

Changing the rules about how data is collected and used by platforms could provide less fodder for those running foreign interference operations. This could include banning unfair uses, such as targeted messaging based on a psychological profile. If the platforms don't facilitate these uses, it becomes more difficult for foreign governments to use these tools for manipulation.

Enhancing funding for the primary data regulator, the Office of the Australian Information Commissioner, could also strengthen enforcement across the board.

What is needed is a strategy, not tactics

These two reform initiatives exist within a maze of others, including inquiries or proposals relating to online privacy, digital platform services, the influence of international digital platforms, electronic surveillance, and digital economy regulation.

Beyond Australia, at the United Nations level, some questions about whether international law can be applied to cyberspace have been resolved, while others remain open. Australia's position on these issues could also be clarified.

Ultimately, what is needed is a strategy, rather than tactics, and better coordination of relevant policies across government. The TikTok example also highlights a truism that we shouldn't think in terms of privacy *or* security, but rather privacy *and* security.

While there is an occasional need to choose between these two values (for example, when government agencies surveil those suspected of a crime, terrorism or espionage), in the vast majority of situations security is enhanced when the privacy of personal information is protected.

For example, the more personal information a foreign agent can access about citizens working in sensitive areas, the better it can target espionage and influence operations. If social media companies are restricted in how they collect, use and share Australians' data, we can take significant steps towards protecting everyone from foreign interference and other harms.

We need all the policies and associated agencies (cyber, privacy, education, platform regulation, international relations, national security and more) working together if we are to meet the current challenges. It may make sense to ban TikTok on government devices, but we need to address this problem more than one app at a time.

Provided by The Conversation

Citation: Opinion: Australia needs a robust cybersecurity overhaul, not whack-a-mole bans on apps like TikTok (2023, April 14) retrieved 2 May 2024 from https://techxplore.com/news/2023-04-opinion-australia-robust-cybersecurity-overhaul.html