Australia Needs to Think Beyond China About Data Security

by **Yun Jiang**

Australian Outlook, 15 February 2023

Link: https://www.internationalaffairs.org.au/australianoutlook/australia-needs-to-think-beyond-china-about-data-security/

The discussion on TikTok and Hikvision infiltration in Australian government departments has centred inarticulately and dogmatically on the country of origin. But there are other more realistic and probable security threats lurking in plain sight

The possibility of the Chinese government accessing Australia's sensitive and national security information has been in the headlines again in the past few weeks. Federal government departments have banned their employees from installing the Chinese social media app TikTok on their work devices. They have also committed to remove security cameras that were made by Chinese companies Hikvision and Dahua from their premises.

However, these steps show that the Australian government is concerned mostly about mitigating potential threats from China rather than the broader issue of data security. This is a whack-a-mole approach to security rather than a holistic or systemic approach, and it is detrimental to Australia's overall security.

Federal departments should ban TikTok on work devices because the app collects sensitive and personal data. But other social media apps such as Facebook or Twitter also collect a huge amount of data from mobile devices. Moreover, it was revealed in 2018 that Strava, an American exercise tracking app, could show the location and activities of soldiers at military bases.

Most of these companies then sell personal data to third parties. Data can be purchased on the open market by anyone, including the Chinese government. Thus, there is no guarantee that American social media apps are safe when it comes to data security.

Although country of ownership is an additional risk factor, it is not the only one. To ensure the privacy of Australians and the information of the government are appropriately protected, the departments should take a broader look at how apps collect and use data, and not just focus on WeChat or TikTok.

Apart from their profit motive of selling data, the accounts can also be hacked. Recent research suggests that federal government employees are using departmental emails as login for services such as Netflix and Twitter. When these services experience a data breach, their emails and passwords are then sold. The recent high-profile Optus and Medibank breaches show that a large amount of personal data can be traded.

Instead of banning apps, departments should consider allowing only apps from a pre-set list and train their employees better on data security. After all, these devices are used only for work purposes, so they do not need social media apps installed on them in most instances. Employees at these departments could install these apps, including TikTok, on their personal devices where there is no sensitive national security information, should they wish to do so.

Similarly, when it comes to security cameras, companies or governments do not need to manufacture particular pieces of hardware to access information held or transmitted by that equipment. Spyware can be installed on equipment made anywhere. For example, Pegasus, a spyware developed by Israeli company NSO Group, could access data from mobile phones, even though neither the company nor Israel makes these phones.

While manufacturing the equipment may make it easier to access information from that equipment, it is not necessary. If a government is motivated enough, it can find other means of accessing that information.

The key differentiating factor should be the sensitivity of the information being protected. For example, Australian intelligence agencies probably would not use Hikvision or Dahua equipment because their risk tolerance for security breaches is extremely low, meaning that equipment from these companies is less reliable from a national security perspective. At the other end of the spectrum, security cameras in public spaces should pose few problems. Museum exhibits, for instance, are open to the general public and a Hikvision security camera there is unlikely to collect or transmit any more information than someone wandering through the exhibits and taking photos.

How these security cameras are installed is more important. In Australia, one can buy the fanciest, top-of-the-range security cameras and still be exposed to significant security risks if they are not installed and networked properly. The information held or transmitted by those cameras can then easily accessed by others. This can happen whether the cameras were made in China or elsewhere.

The Australian government and the people should not think that their data is safe just because a Chinese app or a camera made in China has been removed. Australia's approach to data security should be more than a focus on where the equipment is made or who owns the app. Having better security awareness among the staff, including in dealing with phishing and scams, is also important when it comes to data security.

Unfortunately, the focus on China as the only threat, rather than on the broader issues at stake, has been a common theme in Australia over the last few years. This leads to over-securitisation when the government deals with China-related issues yet leaves Australia vulnerable to risks that are unrelated to China. It is an approach that we should move away from under the new government. Instead, we should think about security issues such as data and privacy more broadly.

Yun Jiang is the AIIA China Matters Fellow.