WhatsApp—a great idea for mates but a terrible one for ministers

October 13 2016, by Vidyasagar Potdar

Credit: AI-generated image (disclaimer)

Cyber security experts have raised concerns about Prime Minister Malcom Turnbull and senior government ministers sending private and confidential information via the messaging service WhatsApp.

WhatsApp and similar messaging apps are great for normal day-to-day

communication between friends, but using it to discuss matters of national security is certainly a choice that will raise eyebrows.

As with any technology, particularly those that allow for speedy communication, the benefits have to be weighed carefully against the associated security risks.

Not on the list

One of the main points of criticism over the decision to use WhatsApp is that it doesn't feature on the Evaluated Products List – the list of accepted tools for ministerial communications compiled by the Australian Signals Directorate.

This list features products that are tested and certified for specific purposes against internationally recognised standards. Vendors can apply for this certification for their products and once evaluated it can be used for the specific purpose.

Many different types of products are on this list, including biometrics, data protection, smart cards, mobile products, network devices, operating systems, and so on. Within the mobile products space, the list features Apple's iOS and Blackberry's operating system, both of which are platforms from which text messages can be sent – but messaging apps such as WhatsApp are not featured.

What's wrong with WhatsApp?

Besides text-based messages, WhatsApp also allows files to be shared and transferred between users. This has implications for government, especially if used by ministers or staff with access to classified information. If such information were disseminated via WhatsApp, this

would constitute a serious security breach.

Although WhatsApp now offers end-to-end encryption, meaning in theory that no one can intercept the communication, the sharing of sensitive documents through this service would still be grounds for serious concern. What would happen in a situation in which a device was lost or stolen? Anyone with access to that device can access the shared files, including any media (images, documents, videos) shared via WhatsApp, which are automatically transferred to and stored in a WhatsApp folder on both devices.

Furthermore, it is possible to hack into the WhatsApp folder via tools such as WiFi File Transfer, which is used to copy files from a mobile to a desktop computer. Sharing web links via WhatsApp also potentially leaves users vulnerable to phishing or other attacks via malware or ransomware.

As WhatsApp now also works via the web, it is prone to all of the web's security threats.

Besides malware posing as genuine WhatsApp links, it is also reportedly possible to crash the app by sending large (over 7 megabytes) messages, or messages containing special characters – a particular fear given that these messages can be typed and sent very quickly by someone who gains access to a device for a short period.

Privacy concerns are also raised by the existence of apps such as WhatSpy, which allows others to monitor a user's messages and photos or even alter their security and privacy settings. Another app called mSpy monitors and reports on a mobile user's activities, such as text messages, WhatsApp messages and phone calls. This app can be installed very quickly and once installed it can report to a designated number or email.

Perhaps worst of all is WhatsApp's vulnerability to MAC spoofing attacks, which involve changing the media access control (MAC) address that acts as a unique identifier for every phone. By changing it, the messages can be routed to an unauthorised device.

Freedom vs responsibility

The truth is that as soon as any sensitive information is placed on the WhatsApp network, it can potentially be shared or forwarded to anyone, meaning that both the sender and the receiver of the information is at greater security risk.

Once confidential information is out in the open network, it is effectively beyond the government's control.

Another concern relates to Freedom of Information. As an encrypted third-party network, it is not clear whether it will be possible to retrieve this information if requested. Recently, US presidential candidate Hillary Clinton has faced severe criticism, media scrutiny and investigation by the FBI for using private email services rather than official communication channels.

WhatsApp or Instant Messaging via mobile devices represents a new wave of communication adopted by the community at large. But the question of whether high-ranking members of the government should be using secured messaging apps is one that requires further investigation.

WhatsApp and other messaging services are promising, useful, and great fun. But they should not be used in a government setting without prior certification.

This article was originally published on The Conversation. *Read the* original article.

Source: The Conversation