RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University

RSIS COMMENTARY

www.rsis.edu.sg No. 119 – 19 May 2016

Rebalancing Encrypted Messaging Apps

By Tan Teck Boon

Synopsis

End-to-end encryption has made instant messages more secure. But the technology has also made it more difficult for authorities to fight terrorism and crime. Reverting to the previous encryption technology rebalances security requirements with privacy concerns.

Commentary

THE RECENT decision by Brazilian authorities to ban WhatsApp – an instant messaging app used by millions of people worldwide – is emblematic of the kind of push around the world to rein in commercial messaging apps featuring state-of-the-art encryption.

In the case of WhatsApp, every message sent is encrypted with a unique "key" — typically, a very large number — ensuring that only the person(s) holding the specific key can unscramble the message. Even if a message were intercepted during transmission, it would be unreadable without the key. Besides WhatsApp, iMessage, Line, Signal and Telegram are some examples of commercial messaging apps featuring this technology.

To be precise, this form of encryption is called end-to-end encryption (or E2EE, for short). In earlier versions of the technology, the app developer retained the keys, thus making it possible for the developer to unscramble users' encrypted messages under court orders. But with E2EE, the keys are kept in the users' computer or mobile device and as a result, app developers are no longer able to hand over users' encrypted messages even if ordered to. The only way authorities can gain access to users' unscrambled messages in this case is to get physical access to their devices.

Upsetting Balance between Privacy and Security

History-wise, developers began seeing the need for more secure communications after a series of embarrassing photo leaks in 2014 involving quite a few female celebrities. But to be sure, monetary reward was also a big driver behind the development of encrypted messaging apps since the company that develops the app with the strongest encryption will invariably corner the lion's share of this incredibly lucrative market. The advent of encrypted messaging apps would not have been a problem except that as instant messages became more secure, criminals and militants have also caught on to their usefulness — paradoxically exploiting for their own benefit the very justification that underpinned these apps in the first place.

Indeed, Islamic State (IS) militants are known to take advantage of these apps for secure communication as well as to reach out to potential recruits around the world. As a case in point, Malaysian authorities arrested three of its own citizens earlier this year who were thought to have been recruited by IS through Telegram. IS operatives also claimed responsibility for the recent Jakarta attack using the same messaging app.

But terrorists are not the only ones exploiting encrypted messaging apps; cyber-criminals, organised crime, drug dealers and even child predators use them to mask their illegal activities. Besides making it more difficult to monitor suspects, encrypted messaging apps have also made it harder for law-enforcement agencies to collect evidence against them. If anything, the situation now is akin to the police not being able to enter a house to collect evidence even with court authorisation.

Because encrypted messaging apps have made it significantly more challenging for authorities to disrupt terrorist plots and fight crime, the vital balance between privacy and security has arguably shifted in favour of the former.

Old Way Still the Best Way

One way to restore the current imbalance is to introduce so-called backdoors or hidden flaws into the apps so that authorities might gain access to the plaintext (unencrypted) messages of suspects. The backdoors could be introduced into either the hardware or software granting the authorities unlimited access. But even this strategy is imperfect. Apart from potential abuses, this approach can be downright dangerous since cyber-criminals and hostile foreign governments can exploit these built-in flaws just as well. Once a flaw is intentionally introduced into the system, it is only fair to assume that someone out there would find a way to exploit it for malicious reasons.

Technological advancement occurs at such a brisk pace that it sometimes blinds us to the fact that earlier inventions already held the solution to an existing problem. Indeed, by reverting to the previous encryption technology (in which the keys are retained by the app developer), the authorities can again monitor encrypted instant messages if needed. As in the past, app developer will act as a check against illegal government surveillance by scrutinising requests from the authorities for plaintext

messages. The most obvious advantage is that authorities will right away regain the ability to monitor suspected militants' encrypted messages.

But what is less obvious is that reverting to the previous encryption technology will also serve to push them offline. In the same way Osama bin Laden promptly stopped using his Inmarsat satellite phone when the Al Qaeda leader learnt that it was being monitored by US intelligence, the idea here will likewise push militants offline once they realise that the digital realm is no longer a safe haven from which to promote violence.

Unlike backdoors, reverting to the previous encryption technology will not lead to a spike in cyber-attacks because the previous encryption technology is sufficiently robust against the majority of cyber criminals. We know this because the authorities had to turn to the app developers for help and if they could not break into the previous encryption technology, then chances are run-of-the-mill hackers would not be able to either. Not all developers are expected to cooperate even though their apps now arguably threaten public safety and interest. But even if some were to, it will reduce the multitude of encrypted messaging apps at the moment and allow authorities to then concentrate their cryptanalytic effort on those that remain unbreakable.

Trump Card: Changing Attitudes toward Privacy

Reverting to the previous encryption technology will entail some risks to privacy. But it is still far superior and more realistic compared to introducing backdoors into every mobile device, computer and encrypted instant messaging software out there.

More importantly, our readiness today to share much personal information online in exchange for greater convenience and accessibility is indicative of our changing attitude towards the notion of absolute privacy. If anything, the popularity of cloud storage and social media websites these days really speaks to this shift in mindset. And as militants and criminals of all stripes continue to exploit encrypted messaging apps, reverting to the previous encryption technology will restore the delicate balance between privacy and security.

Tan Teck Boon is a Research Fellow with the National Security Studies Programme in the Office of the Executive Deputy Chairman, S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University, Singapore. An earlier version appeared in Today.