RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University

RSIS COMMENTARY

www.rsis.edu.sg No. 053 – 4 March 2016

Beyond Apple vs FBI: Implications for Singapore's Smart Nation Project

By Benjamin Ang

Synopsis

The ongoing legal dispute between Apple Inc and the FBI, over accessing data on the iPhone of a deceased terror suspect, has been characterised as a conflict between security and privacy in the US. But it has also highlighted cybersecurity issues that have serious implications for Singapore's Smart Nation initiative.

Commentary

APPLE INC is refusing to comply with a court order demanding that the company disable a key security feature on the iPhone of a deceased terror suspect, so that the FBI can gain access to its data as part of investigations into the San Bernardino mass shooting. The legal battle, including appeals and congressional hearings, could take months to conclude. But regardless of the outcome, it has raised awareness of serious cybersecurity issues.

Opinions are divided between those who believe that Apple should comply, to protect national security, and those who believe that Apple should resist, to protect civil liberties like the right to privacy. Opinions are also divided between those who believe that the technology that would be created as a result could be discovered and used by criminals, and those who believe that Apple could help the FBI without creating such a risk.

Implications for cybersecurity

While these are serious debates, the case has other implications for the relationship between public and private sectors around the world.

If Apple loses, a legal precedent could be set that compels technology companies to help governments and law enforcement agencies gain access to customer data. Alternatively, if Apple wins, legislators (in many countries) might want to overcome this by passing laws that require technology companies to grant that access from the stage of creation, called ‘back doors’ – this has already been proposed in some countries. Such tight control over the technology sector could stifle innovation and even expose the public to greater cyber security risks.

Besides, Apple already operates in many countries where specific laws leave no room for debate. For example, Singapore’s Criminal Procedure Code makes it compulsory to help the police gain access to data stored on a suspect’s computer, or face imprisonment, while the Computer Misuse and Cyber Security Act grant wide powers of access if national security is at risk.

Furthermore, the majority of smart phone users do not use Apple iPhones. Among the other mobile phone manufacturers, some would not (and already do not) refuse to help governments or law enforcement agencies gain access to customer data.

In any of the scenarios above, if this technology is discovered (by accident, deception, corruption, or neglect) by hackers, they could use it as a back door to gain access for criminal purposes like identity theft or credit card fraud. Then the public would be well advised not to rely on manufacturers for security, but to use other means of protection instead, like installing additional security (or encryption) software on their phones and computers, like an additional lock on their ‘back door’.

On the other hand, criminals and terrorists are known to use encryption to hide their nefarious deeds, such as ISIS using the Telegram secure messaging app. Law enforcement agencies need to develop tools to break through (decrypt) this security, creating a competitive race of encryption and decryption.

Implications for Singapore’s Smart Nation Project

If security continues to be a lower priority for manufacturers, this has serious implications for Singapore as we become a Smart Nation. Internet of Things (IoT) devices like smart refrigerators, pacemakers or cars, depend on manufacturers to secure them, because unlike smartphones and computers, these IoT devices are usually not designed for users to install additional security.

It has already been demonstrated that a hacker who gains access to a smart refrigerator, could use it to enter other computers or smart phones in the same household or office network. And if hackers gain access and take over pacemakers or cars, tests have shown that the results could be deadly.

On the other hand, law enforcement could make good use of evidence stored in a smart device, such as where a suspected terrorist’s smart car has travelled, or if a suspected drug dealer had stored illegal drugs in his smart refrigerator.

Options Going Forward

In light of these issues, there are two available options. The first is to legislate that manufacturers of smart devices build in tighter security. This is a highly rational option that would protect customers from hackers, but would most likely hinder police investigations as well as create unease among manufacturers and some consumers.

The second is to legislate that manufacturers install back doors to device security for law enforcement agencies to access in an emergency/national security crisis – this option would certainly help investigators, but expose customers to criminals who discover these back doors. It would similarly create unease among some manufacturers and consumers.

At this point, there are no ready answers but rather more questions that will result from the expected fallout from this and other similar cases in the future. This means that more meaningful discussions need to take place between the private and public sector.

Governments may need to incentivise and perhaps nudge manufacturers to adopt a security-by-design approach to future offerings. In the meantime, smart citizens should lock their phones and computers, but also pay attention to securing their other smart devices.

Benjamin Ang is a Senior Fellow at the Centre of Excellence for National Security, S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University, Singapore.
