APPLE V FBI

Category: Commercial Law,Privacy Law, Infosec, and POPIA,Technology Law
written by Yashoda Rajoo | April 26, 2016

Background

On December 2, 2015, 14 people were killed and 22 others seriously injured in what, President of the United States, Barack Obama, has deemed a terrorist attack in California. The attack comprised of a mass shooting and an attempted bombing. The perpetrators, Syed Rizwan Farook and Tashfeen Malik attempted to flee the scene, but were killed by police in a shootout.

On January 5, 2016, the FBI began investigating the perpetrators. On February 9, 2016, the FBI announced that it was unable to unlock one of the mobile phones they recovered from the perpetrators; a county-owned iPhone 5 C which was found on Farook, due to its advanced security features. As a result, the FBI approached Apple Incorporated to create a new version of the phone's operating system (iOS) that could be installed and run in the phone's random access memory to disable certain security features. Apple declined citing its policy to never undermine the security features of its products. In 2014 Apple made the decision to remove itself from being allowed to access encrypted devices, thus increasing the security provided by these devices. The FBI responded by successfully applying to a federal judge to issue a Court Order, mandating Apple to create and provide the requested software. Apple announced their intention to oppose the Order based on the innumerable security risks that the creation of a backdoor would pose to their customers.

What does the FBI want?

In response to the opposition, on February 19, 2016, the United States Department of Justice filed a new application urging a federal judge to compel Apple to comply with the Order.

The FBI requests that Apple alter the System Information File (SIF) in a way which would allow for:

1) Apple to bypass or disable the auto-erase functions of the device. This is due to the fact that if certain security features are enabled the device can erase all personal data stored on it after 10 failed attempts at entering the correct password;

2) Apple to enable the FBI to submit passcodes to the device for testing electronically. Farook used a 4 digit passcode to secure the device, there are therefore mathematically speaking, 10 000 numerical combinations, which could possibly be the code utilised by Farook. If the FBI is permitted to

electronically attempt every possible combination, unlocking the device would prove to be a task capable of completion in mere minutes, as opposed to the numerous hours it would take to enter the various possibilities manually;

3) Apple to remove any additional delay between failed passcode attempts. This is because the device restricts you from entering a passcode for increasingly lengthy periods of time in each instance an incorrect passcode is entered. The FBI essentially wants this barrier removed.

The FBI suggests that, in order to minimise the risk of the backdoor being accessed by hackers, the SIF be installed at a government facility or an Apple facility, and after the FBI have hacked the phone via remote connection, Apple be permitted to remove and destroy the malware.

Why is Apple refusing to comply?

Encryption encodes and decodes information permitting only authorised persons to access it. A backdoor is a method of bypassing the normal method of authentication. Essentially, a backdoor would allow an intruder to access the encrypted information without having the correct credentials, in this case, a passcode. In order to grant the FBI's requests, Apple would need to create a backdoor to the encryption to allow the FBI to access the device. Creation of such backdoor would have severe security implications should it be accessed by the wrong hands. Incidentally, hackers have found lucrative business in locating these backdoors. This would make every iPhone inherently weaker. Apple would in essence be enabling hacking, and in doing so, US courts may set a precedent other manufacturers may be obliged to adhere to.

What happens now?

It is evident that competing interests are at war in these circumstances. Individuals, more especially Apple users expect that their private communications be protected, whilst law enforcement strives to ensure that public safety and national security are not jeopardised. It is clear that encryption is essential, however the question currently being debated is whether or not law enforcement should be granted access to encrypted communications and in essence invasion of an individual's privacy, when enforcing the law and pursuing the objective to keep citizens safe. Should Apple continue to refuse to allow the FBI access, this matter may eventually find itself before the US Supreme Court, whose ruling will be final and binding.