Centre for Air Power Studies (CAPS)
Forum for National Security Studies (FNSS)
25/17

NATIONAL SECURITY VS. PERSONAL PRIVACY: THE ENCRYPTION CONUNDRUM

Gp Capt Ashish Gupta
Associate Fellow, CAPS

Given the ubiquity of digital connectivity permeating all aspects of our social, economic and professional lives, encryption is the last line of defence against cyber-crimes, cyber terrorism and against theft of valuable information. Encryption is also being used to thwart the acts of nefarious designs of foreign state governments, criminal enterprises and normal hackers. The newspaper headlines are filled with news of cyber-attacks, security breaches, data leaking, hacking etc. affecting individuals, governments, organizations, financial institutions across the world. From preventing relatively minor cyber transgressions, to averting attempts of identity thefts, to foiling attempts of breaching critical information infrastructure, to ensure economic and military security, encryption plays an inexorably critical role. In a never-ending game of cat and mouse between the encryption developers and hackers, a lot rides on the stringency and complexity of encryption. Nevertheless, encryption is also at the centre of debate between the national security and individual privacy.

The law enforcement and security agencies - mandated and entrusted with the responsibility to combat scourge of terrorism and to protect innocent people from heinous terrorist attacks– want to use tap subtle indicators of motives, means and methods of terrorists. To strengthen their ability to undertake result oriented measures and devise new strategies to deal with modern terrorism, these agencies want override mechanisms and/or keys for encryptions to access the encrypted information in possession of a potential or proven terrorist. On the other hand, intentionally compromising the encryption or providing an access mechanism, even for arguably legitimate purposes, weakens everyone's online security and leaves everyone much more vulnerable for exploitation from hackers, cybercriminals and possibly from terrorists.

Following the terrorist attack in San Bernardino, California on December 15, 2015, which killed 14 and seriously injured 22 people, in February, 2016, the FBI requested Apple Company to assist them in hacking the iPhone, which belonged to Syed Farook, the main perpetrator of the terrorist attack. [1] FBI investigators, in possession of Farook's iPhone believed that the device contained data which could help them in unravelling the motives of Farook. But the data could only be accessed after unlocking the iPhone by using four-digit passcode. A four-digit passcode has only about 10,000 possible combinations and unlocking a phone by using these might not prove be that difficult. But modern iPhones have an optional feature that would erase all data on the phone after ten incorrect passcode entries and FBI agents were not willing to take that risk. The request was turned down by Apple.[2]The FBI, armed with an order from a federal magistrate for reasonable technical assistance from Apple to access the data on the device, again approached Apple. Apple challenged the court order, arguing that its encryption technology was necessary to protect its customers' communications, security, and privacy and raised both constitutional and statutory objections to the Magistrate's order. A magistrate judge in the Eastern District of New York ruled in favour of Apple denying the FBI request for information on Farook's iPhone by unlocking it. [3]

The debate once again has taken centre stage, this time in Britain. On March 22, 2017,London was rocked by a deadly 'terrorist' attack outside British Parliament, carried out by a 52-year-old Briton Khalid Masood, who drove a car into pedestrians killing three of them, and then fatally stabbed a police officer.[4] The Islamic State claimed responsibility for the attack, but the precise nature of his connection with the Islamic State is not yet fully clear at this time. The London police, as part of investigation, are focusing on Masood's communications and it has been widely speculated that Masood was in contact with someone through WhatsApp immediately prior to the attack.[5] In an effort to bolster their fight against terrorism, British government officials scheduled a meeting with representatives of American technology companies seeking help to access to encrypted messages sent through WhatsApp, an instant-messaging service owned by Facebook.[6] Britain is not the only country in Europe seeking a viable and workable solution from Silicon Valley companies to the 'encryption conundrum' which severely contain and retard efforts to identify and prosecute real perpetrators of terrorist attacks. For many lawmakers and regulators, that includes access to encryption keys of WhatsApp and Telegram, a rival messaging tool, to intelligence agencies involved in investigation of terrorist activities.

The tussle has been simmering in the open for months between the Washington and Silicon

Valley over the privacy of online data and new security technologies. After the San Bernardino shooting, on December 09, 2015 the FBI Director James B. Comey, while making a statement before Senate Judiciary Committee brought out that ISIS is increasingly using encrypted private messaging platforms. He said that, " This real and growing gap, which the FBI refers to as "Going Dark"; we believe it must be addressed, since the resulting risks are grave both in both traditional criminal matters as well as in national security matters." He further commented that the US government was trying to ensure that the private players who own and operate these platforms - with end-to-end encryption - understand the national security risks emanating from the use of their encrypted products and services by malicious actors.[7]On the other hand, the top tech companies of silicon valley including Apple, have again and again reiterated their commitment to respect privacy and protection of their customers and refused to dilute their position despite clear national security risks to the US and elsewhere. In one of his speech, Tim Cook, the CEO of Apple made his stand very clear by saying that, "we at Apple reject the idea that our customers should have to make tradeoffs between privacy and security. We can, and we must provide both in equal measure. We believe that people have a fundamental right to privacy. The American people demand it, the constitution demands it, morality demands it."[8]

Melvin Kranzberg once famously commented: "Technology is neither good nor bad; nor is it neutral."[9]An easy resolution of this raging debate is not in sight at the time, as it looks like both the parties have valid and compelling points in support of their respective arguments. Nevertheless, there is no denying of the fact that the global scourge of terrorism can only be exterminated through the collaborative and integrated efforts - of global political leadership, military law-enforcement, intelligence and security agencies, financial institutes and public and private companies- even if it requires transcending parochial partisan interests and objectively balancing the degree of risk that might be warranted by potential benefit.

(Disclaimer: The views and opinions expressed in this article are those of the author and do not necessarily reflect the position of the Centre for Air Power Studies [CAPS])

Notes

[1] Danny Yadron, Spencer Ackerman and Sam Thielman, "Inside the FBI's encryption battle with Apple, " *TheGuardian*, February 18, 2016 , at http://www.theguardian.com/technology/2016/feb/17/inside-the-fbis-encryption-battle-with-apple, accessed on February 22, 2016 accessed on March 22, 2017.

[2] Ibid.

[3] Spencer Ackerman, Sam Thielman and Danny Yadron, "Apple case: judge rejects FBI request for access to drug dealer's iPhone", *TheGuardian*, February 29, 2016, https://www.theguardian.com/technology/2016/feb/29/apple-fbi-case-drug-dealer-iphone-jun-feng-san-bernardino accessed on March 22, 2017.

[4]Vikram Dodd et al., "Westminster attack: police hunt for clues after four dead in 'sick and depraved' incident", *TheGuardian*, March 23, 2017, https://www.theguardian.com/uk-

news/2017/mar/22/parliament-attack-police-officer-four-dead-westminster accessed on March 22, 2017.

[5] Mark Scott, "In Wake of Attack, U.K. Officials to Push Against Encryption Technology", *The New York Times,* March 27, 2017, https://www.nytimes.com/2017/03/27/technology/whatsapp-rudd-terrorists-uk-attack.html?_r=0, accessed on March 22, 2017.

[6] Ibid.

[7] The US Federal Bureau of Investigation, Oversight of the Federal Bureau of Investigation, James B. Comey, Director, Federal Bureau of Investigation, Statement Before the Senate Judiciary Committee, Washington, D.C December 09, 2015, https://www.fbi.gov/news/testimony/oversight-of-the-federal-bureau-of-investigation-8, accessed on March 22, 2017.

[8] Matthew Panzarino , "Apple's Tim Cook Delivers Blistering Speech On Encryption, Privacy" , The Techcrunch , June 2, 2015, http://techcrunch.com/2015/06/02/apples-tim-cook-delivers-blistering-speech-on-encryption-privacy/#.oero2hn:kVGu, accessed on March 22, 2017.

[9] James W. Fraser, Reading, Writing, and Justice: School Reform as if Democracy Matters, (Albany: State University of New York Press, 1997), p.142.