Centre for Air Power Studies (CAPS)
Forum for National Security Studies (FNSS)
21/16

FBI-APPLE STAND OFF: CAN A TRADEOFF BETWEEN NATIONAL SECURITY AND PERSONAL PRIVACY POSSIBLE?

Gp Capt Ashish Gupta
Senior Fellow, CAPS

The vociferous and ongoing debate between privacy and security and its consequences has led to an increasing tension between the principle of "security" and that of 'privacy and democracy'. The threats of internal extremism, global terrorism, radical insurgency, threats from rogue nations and asymmetric threats from non-state actors – has resulted in deepening and intensification of security measures across the whole spectrum of political, economic and social, constitutional and legal, and security strategies, tactics and approaches. A pressing question recurrently posed, not only by the citizenry but by experts as well, is whether it is possible to strike a balance between security and privacy. In the midst of security imperatives, will it be even plausible to not tread upon fundamental rights and civil liberties. In the present security environment - underpinned by the rationality of a "war on terror" and buttressed by all the possible means, methods and materials – the privacy concerns seem trivial compared to overarching security necessities. Security concerns are readily discernable and understandable since national security, human security and economic security stakes are far too high than the abstract and vague conception of privacy rights.

The FBI-Apple standoff has reignited the debate between the national security and privacy. On February04, 2016, the Apple headquarter in Cupertino, California received a request from FBI to assist them in hacking the iPhone, which belonged to Syed Farook, who along with his wife carried out a terrorist attack in San Bernardino, California on December 2, 2015 killing 14 people and seriously injuring 22. The request was turned down by Apple.[1]FBI investigators, in possession of Farook's iPhone believe that the device contains data which could help them in unravelling the motives of the couple. But the data can 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 may not be that difficult. But the Modern iPhones have an optional feature that will erase all data on the phone with ten incorrect passcode entries and FBI agents are not willing to take that risk. On February 16, the FBI armed with an order from a federal magistrate sought help from Apple to unlock a single iPhone of one of the killers and again it was refused. Prior to these developments, when the FBI approached Apple for providing them with backup data of weekly backups, which Farook made with Apple's iCloud service, the Apple complied with the request. The backup were available till October 19, 2015 as after that backups were made by Farook.[2]

The tussle has been simmering in the open for months between the Obama administration 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 is trying to ensure that the private players who own and operate these platforms - with end-to-end encryption - understand the national security risks that results from the use of their encrypted products and services by malicious actors. Though there is no legislating obligation upon these companies, the companies are being asked to cooperate constructively with the US government.[3] France, the country that rates value of privacy much higher than other countries is now considering outlawing the 'encryption' in the wake of the Paris massacre. The British Prime Minister, David Cameron has made similar demands. Some of the top US top brass and intelligence officials including FBI Director Comey met with the executives from Apple, Facebook, Twitter and Google in Silicon Valley on January 8, 2016.[4] The CEOs of top tech companies including Apple CEO Tim Cook were extremely firm on their stand of doing nothing which could dilute the privileges and protection of their customers. In one of his speech, Tim Cook 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."[5] The law enforcement officials, on the other hand insisted that surveillance on suspected terrorists would help them to prevent horrific acts of violence, like those in Paris and San Bernardino, California.

The standoff has reached a critical level attracting vociferous supporters as well as opponents, criticizing or siding with the law enforcement agencies or tech companies. Apple has come under vitriolic attack from many quarters questioning its patriotic values vis-à-vis loyalty towards its customers. Senator Tom Cotton of Arkansas wrote in a statement that," Apple chose to protect a dead ISIS terrorist's privacy over the security of the American people." [6] Donald Trump, the republican candidate in this year presidential elections has called for a boycott of Apple until it complies with a court order to unlock an iPhone 5c used by Syed Farook. Apple CEO, Tim Cook on the other hand remarked that. "In the wrong hands, this software - which does not exist today - would have the potential to unlock any iPhone in someone's physical possession'.[7] In an open letter, Cook wrote, "We believe it would be in the best interest of everyone to step back and consider the implications."Twitter CEO Jack Dorsey and Google CEO Sundar Pichai have spoken in the defense of Apple and Tim Cook.

Melvin Kranzberg once famously commented: "Technology is neither good nor bad; nor is it neutral."[8]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 and unimaginable atrocities – want to use even subtle indicators of motives, means and methods of terrorists to strengthen its ability to undertake result oriented measures and device new strategies to deal with scourge of terrorism. On the other hand, intentionally compromising the encryption or providing an access mechanism, even for arguably legitimate purposes, weakens everyone's online security and leave everyone much more vulnerable for exploitation from hackers cybercriminals and possibly from terrorists. 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 and the outcome of legal battle between FBI and U.S. Justice Department against Apple in federal courtroom will have far reaching consequences on national security and personal privacy. 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 require giving up of parochial concerns, financial considerations and sense of misplaced morality.

(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, " *The*

Guardia, February 18, 2016 , at http://www.theguardian.com/technology/2016/feb/17/inside-the-fbis-encryption-battle-with-apple, accessed on February22, 2016

[2] Ibid.

[3]The US Federal Bureu 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 February 22, 2016.

[4]Haley Sweetland Edwards, "Why we can't unscramble the fight over encryption," *Time*, January 25 , 2016, p.25.

[5]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 February 22, 2016.

[6]Pamela Engel, "GOP senator unloads: 'Apple chose to protect a dead ISIS terrorist's privacy over the security of the American people", The Business Insider, February 17, 2016, http://www.businessinsider.in/GOP-senator-unloads-Apple-chose-to-protect-a-dead-ISIS-terrorists-privacy-over-the-security-of-the-American-people/articleshow/51031844.cms, accessed on 22 February, 2016.

[7]Ibid.

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