Anthony Tucker-Jones reports on how Apple Inc. is refusing to cooperate with the FBI's struggle against domestic terrorism

DEFYING THE FBI

Apple, one of the most powerful tech giants in the world, finds itself at loggerheads with the Federal Bureau of Investigation. In the latest round of the struggle over privacy versus national security it seems as if Apple may have overstepped the mark. Not so says Apple, rather what the US Government is asking will put US citizens "personal safety at risk".

Last year on 2 December, Syed Rizwan Farook and his wife, Tashfeen Malik killed 14 people and wounded 22 during a party at the Inland Regional Center in San Bernardino, California. What made this particular attack despicable was that the local social services centre helps people with learning difficulties. Both killers subsequently died during a shootout with police. America was left stunned by yet another mass shooting.

The culprits' motives were initially vague. Neither attacker had a criminal record or was on the FBI's Terrorist Screening Database. At first it looked like a killing spree by a disgruntled employee. However, after conducting 550 interviews and sifting through some 500 pieces of evidence the FBI believes that the couple may have been motivated by Islamic extremism.

Malik, who entered the US on a fiancée visa in July 2014, sent two Facebook messages to Pakistani friends pledging support for Islamic jihad. She and Farook had met on the internet the year before. On the day of their attack according to the *Los Angeles Times*, the couple declared their allegiance to Islamic State but the post was subsequently taken down.

Frustratingly for the FBI, although they pieced together a four-hour timeline for that tragic day, there is an 18-minute gap in the couple's movements. It has been speculated during that time they visited a storage unit or someone's house. FBI spokesman David Bowdich says: "They did a lot of zig-zagging around, back and forth, there is no rhyme or reason to it that we've be able to determine". The only other lead was Enrique Marquez Jr who was arrested for supplying the assault rifles used in the killings.

Intriguingly for some unexplained purpose the couple visited a local lake after the attack before returning home. Police divers have since checked to see if any weapons or evidence were thrown into the waters – they drew a blank. The FBI has since spent two months trying to access Mr Farook's iPhone 5C. The challenge they faced is that the iPhone only permits 10 pass code attempts before it is permanently disabled. The FBI hoped that the encrypted data would clarify the couple's movements and show if they had discussed their plans with anyone else. It is important to determine whether the couple were self-radicalised, part of a larger cell or had a handler either in America or abroad.

When the FBI approached Apple for assistance with the phone, the company refused to cooperate. Although Apple made engineers available to advise the FBI, they would not or could not over ride the security features of the iPhone. Understandably the FBI needed to bypass these so they could electronically run millions of combinations until they cracked the password.

In response the FBI sought a court order and the Central California District Court upheld this request. Once again Apple refused to comply. Apple's Chief Executive Officer Tim Cook was unequivocal, saying "The US Government has demanded that Apple take an unprecedented step, which threatens the security of our customers".

The FBI disputes this. "We simply want a chance,

with a search warrant," says FBI Director James Comey "to try to guess the terrorist's passcode without the phone essentially self-destructing and without it taking a decade to guess correctly. That's it".

While the FBI say they only want access to Farook's phone, Apple argues that much bigger issues are at stake. Apple claims that the FBI wants an iPhone operating system that does not exist (which seems highly surprising) that could bypass its security features. The company claims that encrypted data on its products is out of even its reach – the cynic might find this rather hard to believe. Apple also claims creating such a "backdoor" would endanger the security of all iPhone users.

Tim Cook's position is that if Apple complied then this would compromise every one of its customers and leave them open to cyber criminals and hackers. "The Government suggests this tool could only be used once, on one phone," says Cook "But that's simply not true. Once created, the technique could be used over and over again on any number of devices". Is this scaremongering or can the FBI not be trusted?

Microsoft founder Bill Gates backs the FBI saying Apple has misrepresented what is being asked of it. "The San Bernardino litigation isn't about trying to set a precedent or send a message of any kind" clarifies Director Comey, "It is about the victims and justice." To try and placate Apple the FBI has reportedly offered to hand over the phone, which once unlocked could be accessed remotely without being privy to the so-called "pass key".

Apple is either grandstanding over the sanctity of data protection, or has little faith that the FBI would not let such a "backdoor" escape its grasp, or honour any agreement to use it just once. This is not be the first time that the FBI has experienced such problems with the iPhone so it is perhaps easy to understand Apple's objections.

Over the past year the FBI has been publicly critical of Apple's encryption. Director Comey and Michael Rogers, the National Security Agency's Director met with senior representatives of all the major tech companies in Silicon Valley, California in January 2016. This get together signalled the US Government realises that it cannot defeat terrorism online without help. During the meeting Tim Cook urged the Government to support its encryption work.

Distraught family members who lost loved ones during the San Bernardino shooting have said scathingly the 'i' in 'iPhone' stands for Isis or Islamic State. Apple's holier-than-thou stance is also hard to understand in light of its own business practices having got it into trouble. Recently the company was ordered to pay out $625m in damages for patent fraud. In addition iPhone users have been alarmed by reports that changing the date to 1 January 1970 could cause a shut down and result in the phone rebooting. This, Apple says, can be fixed but in the meantime do not try it.

Presidential hopeful Donald Trump has also poured scorn on Apple's stance saying: "It's ridiculous that the Government has to be put in a position where if they have information about a possible attack, we waste a second because that could be the second that kills somebody".

The FBI and other law enforcement bodies remain exasperated that increasingly sophisticated encryption is thwarting their efforts. The San Bernardino case has now further highlighted to terrorists and organised crime the merits of using iPhones. The FBI warned the US Senate Intelligence Committee that mass communication going "dark" was "overwhelmingly affecting" its ability to counter crime and terrorism.

Certainly Apple has made it clear it will not build a "backdoor" access into its products nor allow law enforcement to open phones using brute force. "We have no sympathy for terrorists,' says Tim Cook – terrorists may see the situation a little differently. Terrorist

DEFYING THE FBI

groups and organised crime are always seeking to stay one step ahead of law enforcement – Apple seems to be offering just such a service.

There is a convoluted chicken and the egg argument that says the state and indeed private companies should not have wholesale access to personal data. However, the counter argument reasons if you are law abiding then you have nothing to hide. Statistically such data is already used for trend spotting, be it health, spending forecasting or consumer buying trends. Ultimately it boils down to whether private companies can protect their customers from cyber crime while cooperating with law enforcement – without compromising their customers' data.

Apple is likely to end up in the US Supreme Court, but it has very deep pockets to fight such a legal battle. In addition Google, that other tech behemoth, along with Facebook and Twitter have stepped into the fray and backed Apple. Sundar Pichai Google's Chief Executive issued a statement saying: "We build secure products to keep information safe, and we give law enforcement access to data based on valid legal orders. But that is wholly different than requiring companies to enable hacking of customer devices and data". Both Apple and Google are likely to enjoy the support of the American Civil Liberties Union, which has been suing the US Government over the NSA's access to private phone records.

The Apple row has raked up all the Edward Snowden controversy over Washington's covert domestic internet surveillance operation known as Prism. James Clapper, the US Director of National Intelligence, claimed the NSA had not "wittingly" collected data on US citizens. Few were convinced by such platitudes.

In the UK, the Government was given a hard time over the failed Communications Data Bill better known as the snoopers' charter. This was despite the UK already having extensive surveillance regulations overseen by the Interception of Communications and Intelligence Services Commissioners.

Perhaps the reality is that the threat now posed by cyber criminals and hackers is so great that it is this – not safeguarding civil liberties – which ensures that terrorist and criminals can enjoy unbroken encryption along with everyone else.

"Although this case is about the innocents attacked at San Bernardino," concludes Director Comey "it does highlight that we have awesome new technology that creates a serious tension between two values we all treasure – privacy and safety. That tension should not be resolved by corporations that sell stuff for a living". Apple and its like will inevitably see this as a warning shot.

Anthony Tucker-Jones is *intersec's* Terrorism and Security Correspondent. He is a former defence intelligence officer and is now a widely published defence commentator specialising in regional conflicts and counter terrorism.