IPHONE CONTROVERSY

- The FBI wants Apple to alter what is known as a SIF - System Information File.
- In this context, the FBI is basically referring to the software that runs on the device.
- The FBI wants Apple to create a new SIF to place on Farook's iPhone that will allow it to carry out several functions normal iPhones do not allow.

The FBI wants to be able to:

1. Prevent the phone from erasing itself. If certain security settings are enabled, after 10 failed attempts at entering a passcode, an iPhone can erase the personal data on the device. The FBI doesn't want to this to happen on Farook's phone.
2. Automate the process for trying out passcode combinations. Farook used a four-digit passcode, for which there are 10,000 possible combinations. The FBI doesn't want to have to guess them all manually, and so it wants Apple to allow the passcode to be tried electronically. This means the FBI could simply instruct a computer to try every passcode, something that would take just minutes, possibly second and without unnecessary delay.
3. The iPhone prevents you from entering a passcode for longer and longer periods of time each time you get it wrong. The FBI wants this barrier removed.
4. Control the process, but not know how it's done. This is an interesting line, as it is suggests the FBI is willing to allow Apple to work on the phone at its own HQ, and in a way that doesn't risk the encryption software being released into the world.

As this row goes through the courts, expect that final element to be a key point the FBI makes - it will argue that the SIF will only work on Farook's phone, and will be known only by Apple, who could choose to destroy it.

Why is Apple refusing to comply?

- In a letter to customers, Apple boss Tim Cook said he did not want to introduce what is known in IT security as a "back door". Like a literal back door, it's simply a different way in.

- In this case, a different way to get into the phone other than by using the pass code, i.e. the front door.

- Back doors are a big deal in security. Hackers make their money from finding them - a back door into a major piece of software or popular device can be highly lucrative.

- Buyers range from criminals to governments looking to spy or obtain data they otherwise wouldn't be able to reach.

- Apple says introducing a back door into the iPhone wouldn't just make Farook's phone insecure and accessible to the US government - it would make every iPhone inherently weaker.
- "You can't have a back door that's only for the good guys," Mr. Cook said in an interview in 2015.

- "Any back door is something that bad guys can exploit."

Can it even be done?

- Most experts the BBC has spoken to think it is possible to access Farook's phone without harming the data. And significantly, Apple hasn't denied it's possible either, instead choosing to discuss the merits of why it thinks it shouldn't.

- An in-depth explanation of how it could be done was posted by security research firm Trail of Bits.

- By using the same technique that enables "jail breaking" - the practice of forcibly removing restrictions and security measures within the iPhone's software - you could force new software onto the iPhone, researcher Dan Guido wrote.

- He said that by using security signatures that only it possesses, Apple is capable of creating modified software that would work just on Farook's iPhone.

- "This customized version of iOS (*ahem* *FBiOS*) will ignore pass code entry delays, will not erase the device after any number of incorrect attempts, and will allow the FBI to hook up an external device to facilitate guessing the pass code," he wrote.

- "The FBI will send Apple the recovered iPhone so that this customized version of iOS never physically leaves the Apple campus."

Who is supporting Apple?

- On Wednesday, Apple's peers in the technology industry - also eager to keep reputations over security intact - gave their backing to the iPhone maker.
- Jan Koum, the creator of Whatsapp, which is owned by Facebook, wrote: "We must not allow this dangerous precedent to be set. Today our freedom and our liberty is at stake."

- The Information Technology Industry Council, a lobbying group that represents Google, Facebook, Microsoft, Samsung, Blackberry and a host of others, put out this statement: "Our fight against terrorism is actually strengthened by the security tools and technologies created by the technology sector, so we must tread carefully given our shared goals of improving security, instead of creating insecurity."

- Google chief executive Sundar Pichai said: "Forcing companies to enable hacking could compromise users' privacy."

- Edward Snowden, whose revelations about US government spying provoked Apple's stance on passcode-protected data, said the FBI was "creating a world where citizens rely on Apple to defend their rights, rather than the other way around".

Who is backing the FBI?

White House press secretary Josh Earnest told reporters on Wednesday that the FBI was "simply asking for something that would have an impact on this one device".

While much of the technology community has backed Apple's stance, some commentators say the company is framing the debate poorly.

"We should fight to make warrants difficult to obtain. But the real unprecedented feat is the idea that a corporation like Apple should be able to prevent our law enforcement from carrying out a lawfully obtained warrant."
In the UK, the family of murdered Fusilier Lee Rigby told the BBC Apple was "protecting a murderer's privacy at the cost of public safety".

What happens next?

- Apple has a few more days to file its formal response to the court, which can be summed up as: "No."

- After a series of briefings at this local level, if neither side is happy, the case will be passed on to the District Court.

Still no solution?

- The case would then be escalated to the Court of Appeals for the Ninth Circuit, the court which handles these sorts of issues on the US West Coast.

- If that court backs the FBI, and Apple again refuses, it could eventually reach the US Supreme Court, whose decision will ultimately be final, and in this utterly fascinating case, precedent setting.

- That could take several years.

Encryption of data

What is encryption?

In cryptography, encryption is the process of encoding messages or information in such a way that only authorized parties can read it. Encryption does not of itself prevent interception, but denies the message content to the interceptor.[:374] In an encryption scheme, the intended communication information or message, referred to as plaintext, is encrypted using an encryption algorithm, generating cipher text that can only be read if decrypted. For technical reasons, an encryption scheme usually uses a pseudo-random encryption key generated by an algorithm. It is in principle possible to decrypt the message without possessing the key, but, for a well-designed encryption scheme, large computational resources and skill are required. An authorized recipient can easily decrypt the message with the key provided by the originator to recipients, but not to unauthorized interceptors.