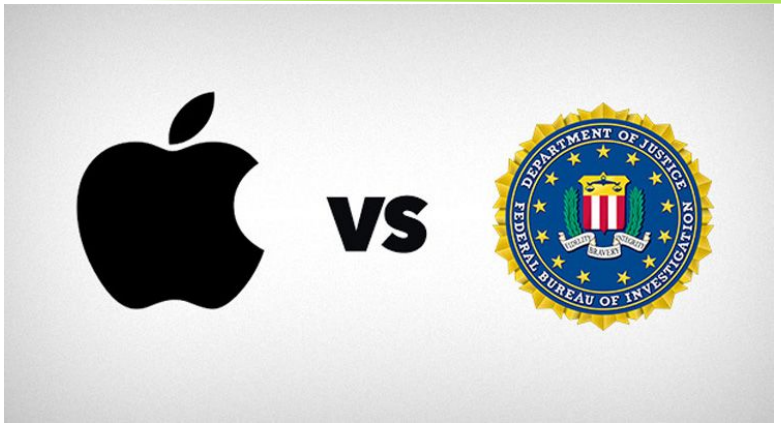
Why can or cannot apple withhold information from the federal government?

By Stephannia and Jovani

Apple v FBI 2016

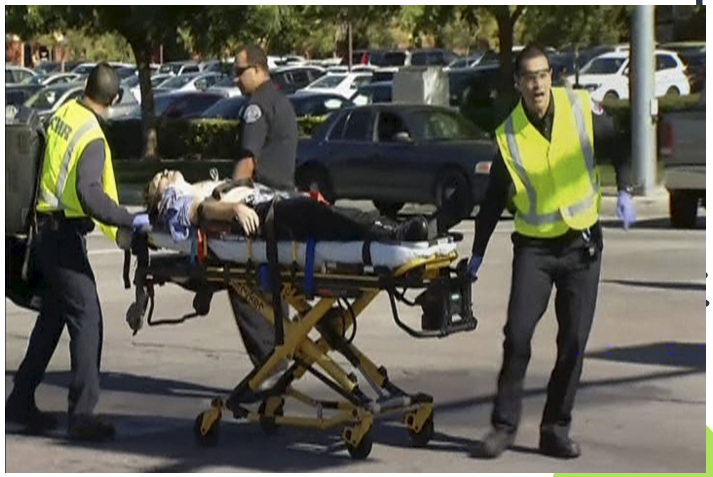


- FBI via court order asked Apple to unlock an iPhone.
- Apple refuses to assist.

Context for this case

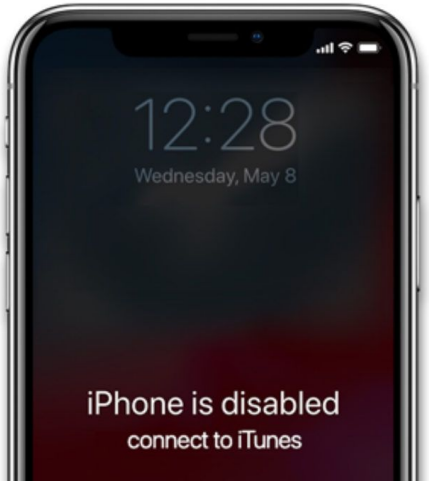
December 2nd 2015- San Bernardino

- ✗ The deadliest mass shooting since 2012's Sandy Hook
- ✗ Culprits failed to destroy their phones and several hard drives.



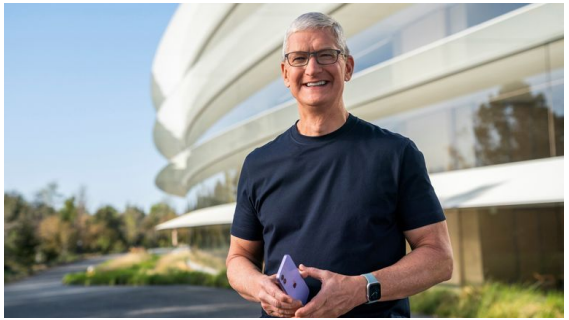
Why does the FBI need to unlock personal phones?

- ✗ Once an iPhone is disabled, it is near impossible to retrieve data from it.
- ✗ FBI believed a possible third shooter may have been involved.



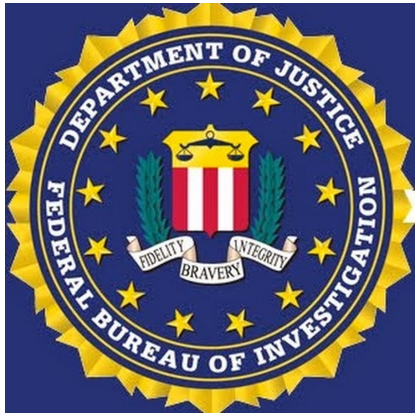
Why is Apple refusing to help the FBI?

- ✗ FBI asked to make a custom iOS for the purpose of unlocking disabled iPhones.
- ✗ Backdoor access would undermine Apple policy of maintaining product integrity
- ✗ Could be used without Apple's control



"It's not an issue of privacy versus security ... it's privacy and security or privacy and safety versus security." -Tim Cook

Should the FBI have the ability to extract data from any encrypted device?



Pro's

- Potentially increase security against terrorist attacks
- Eliminates criminals ability to communicate/ privacy
- Obtain evidence that would be lost due to encryption

Con's

- ✗ Weaken device safety and encryption
- ✗ Special tool to unlock iPhones will be released to the FBI and can be potentially be stolen allowing unwanted parties access to iPhone encryption keys
- ✗ Violates privacy of personnel that require encryption
  - ✗ Finances
  - ✗ Sex life
  - ✗ Journalist
  - ✗ Whistle blowers
  - ✗ Medical Professionals

Bigger questions implicated in this case:

- ✗ Can Apple be considered an accessory to the crime by refusing to provide the FBI aid?
- ✗ Should laws be implemented to protect device encryption or should government overreach be expanded?
- ✗ Is it ethical for the government to force companies to alter their privacy and safety features for information that could potentially be useful?
- ✗ Should you sacrifice privacy for physical safety?
- ✗ Should companies be allowed to make devices that are completely “unsearchable”?

Resources:

https://www.hrw.org/news/2020/01/16/us-government-challenges-apple-encryption-again

https://www.inquirer.com/opinion/commentary/fbi-apple-iphone-search-privacy-data-security-20200302.html

https://www.nytimes.com/interactive/2016/03/03/technology/apple-iphone-fbi-fight-explained.html

https://www.businessinsider.com/apple-reignites-privacy-battle-with-trump-administration-over-shooting-2020-1

https://ethicsunwrapped.utexas.edu/case-study/fbi-apple-security-vs-privacy

Random

In October 2019, Attorney General Barr demanded that Facebook halt plans to implement encrypted messaging on its platforms, citing the need for law enforcement to access that data in investigations.

Resolving this issue is not simple. Experts tell us that creating “back doors” to encryption systems means that they can be broken more easily. Apple’s encryption system does not protect one device; it protects all of Apple’s phones. If Apple creates an encryption key, it could be used against every iPhone. Even if Apple keeps the key, there is the danger that the key could leak out, endangering the privacy of all iPhones. Although Coca-Cola, for example, has managed to keep its formula secret, in August 2016, the National Security Agency lost control of some major cyber tools, resulting in major internet attacks. This could happen again.