Apple vs FBI

By: Jenna Bresalier, Daniel Cunningham, Leka Lee-Maeba, Justin Orriola, Mohamed Alhaj

Meet The Team

Justin Orriola

Jenna Bresalier

Mohamed Alhaj

Daniel Cunningham

Leka Lee-Maeba

What Is More Important: Privacy or Security

Discussion Question 1

What Happened?

- In December 2015, terrorist attacks occurred in San Bernardino, California
  - The perpetrator's phone was seized during investigations
- The FBI was unable to access the data on the phone because it was locked with a passcode
- San Bernardino Health Department owned the phone but it was used by one of the perpetrators
- The court ordered Apple to assist with decrypting the phone and allowing access to the data inside
- FBI wanted Apple to bypass security features including:
  - 4-digit password
  - the feature that erases all the phone's data after ten unsuccessful password attempts

What Happened?

- Apple's CEO Tim Cook did not want to cooperate with the FBI
  - he had concerns about allowing this security bypass to occur, even though the FBI claimed it would be one time
- Tim Cook believed that the FBI was "stepping out of bounds" by using the court system to expand its own authority

Apple’s Stance

- Sole purpose is to protect the privacy of its customers
- Refused to comply with the FBI’s request
- Argued that creating such software would set a dangerous precedent
- Creating a "backdoor" to bypass encryption would put all iPhone users at risk
- “The case was about more than just one iPhone and that it was a matter of principle for the company”

Arguments in Favor of Apple

- First amendment, pointed to several court cases where code was considered a form of free speech
- Fifth amendment, the requested order would require Apple to “do the governments bidding” in a way that takes away and violates Apples core principles of privacy
- Argued the court decision endangered everyone's privacy and could set a dangerous precedent
    - Adding that such a backdoor could slip into the wrong hands, further threatening breaches and the privacy of all iPhone users

FBI’s Stance

- Purpose is to protect the country from terrorism
- Requested Apple’s assistance because it contained important evidence that could help their investigation
- Believed Apple would be able to extract data stored on iPhone
    - Information on the iPhone could help prevent future terrorist attacks.
- Argued Apple’s refusal was hindering their investigation

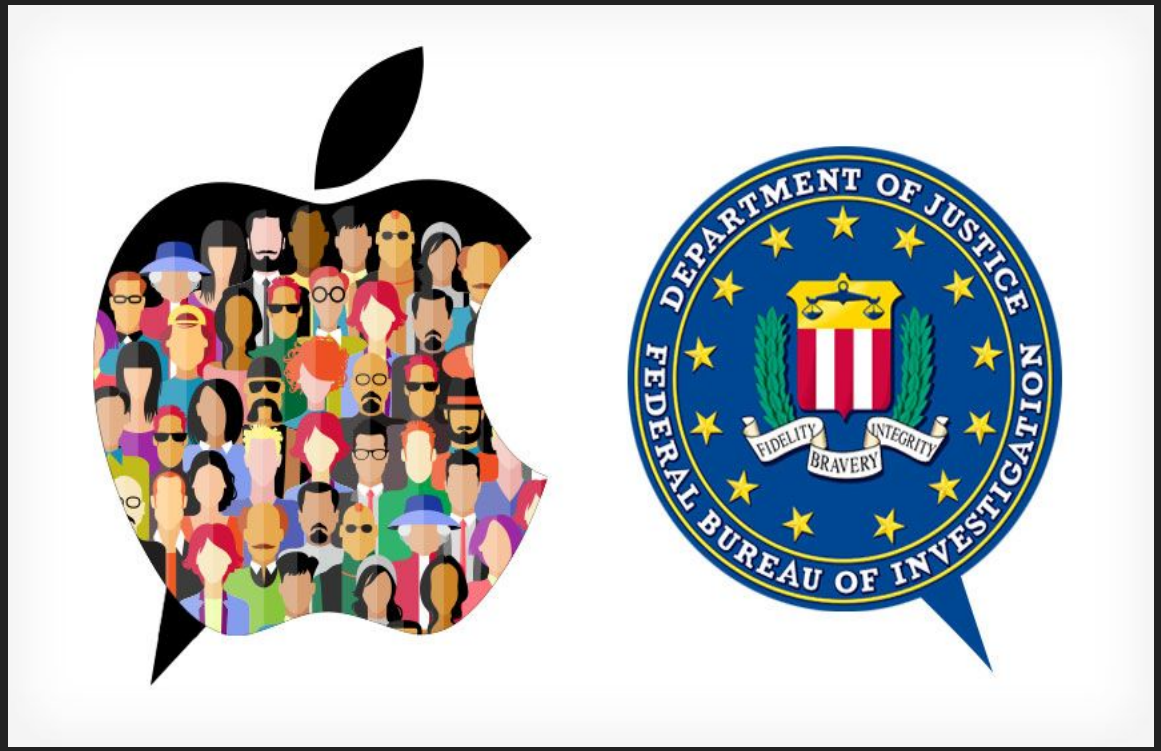
Arguments in Favor of the FBI

- Relied heavily on the All Writs Act which allows courts to “issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law"
- Further saying that Apples participation is necessary to access the phone
    - To protect the people
- The government had obtained a warrant to search the phone

Reevaluate your stance on Privacy vs Security after hearing the arguments from each side.

Discussion Question 2

Controversy: Apple and Privacy



Apple refused to comply with the request, arguing that it would set a dangerous example and undermine the security of all iPhones.

The case sparked concerns that companies like Apple could be forced to create similar backdoors for other law enforcement agencies, posing a significant risk to privacy.

Apple believed that complying with the FBI's request to create a backdoor into the iPhone of the San Bernardino shooter would set a dangerous precedent and undermine the company's commitment to privacy.

Protecting individual privacy and government overreach can be seen as more important

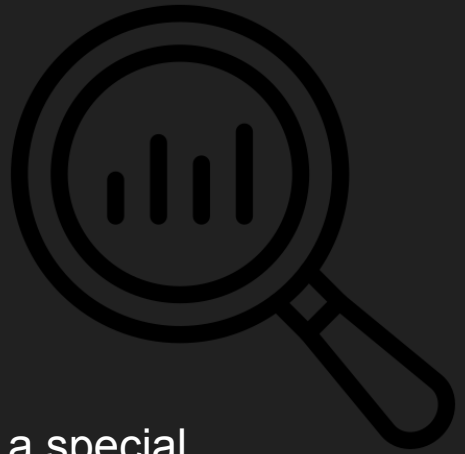
Controversy: FBI and Security

Law enforcement officials argued that encryption hinders investigations into criminal activity, particularly in cases where the evidence is stored on a device with a strong encryption system.

In the San Bernardino case, the FBI believed that accessing the shooter's iPhone could provide critical information about the attack and any potential accomplices.

Law enforcement agencies argued that they needed access to encrypted data to effectively perform their duties and protect public safety.

Outcome



- Apple declined to offer assistance
  - Apple persisted in its defense of civil liberties
- The FBI requested a court order compelling Apple to develop a special operating system that would turn off the iPhone's most important security protections
  - Apple vacated the case and rejected the FBI's request to remove the security protections
- The FBI cracks the Apple phone password
  - Apple wants to know their vulnerability

Do you think Apple was right or wrong in declining to offer assistance? Why?

Discussion Question 3

Jenna’s Lessons Learned

- The importance of encryption
  - Highlighted critical role encryption plays in protecting user privacy and security
  - Potential risks associated with creating a "backdoor" to bypass encryption
    - Creates a vulnerability that could be exploited by hackers potentially putting sensitive information at risk
  - Case underscored the need for careful consideration when it comes to privacy and national security concerns

Justin’s Lessons Learned

- Code is a form of free speech
- Gave IT companies a platform to stand on against government overreach when something similar may happen in the future
- IT services and technologies evolves significantly faster than the laws being able to adapt to the changes
- The importance of company principals

Daniel’s Lessons Learned

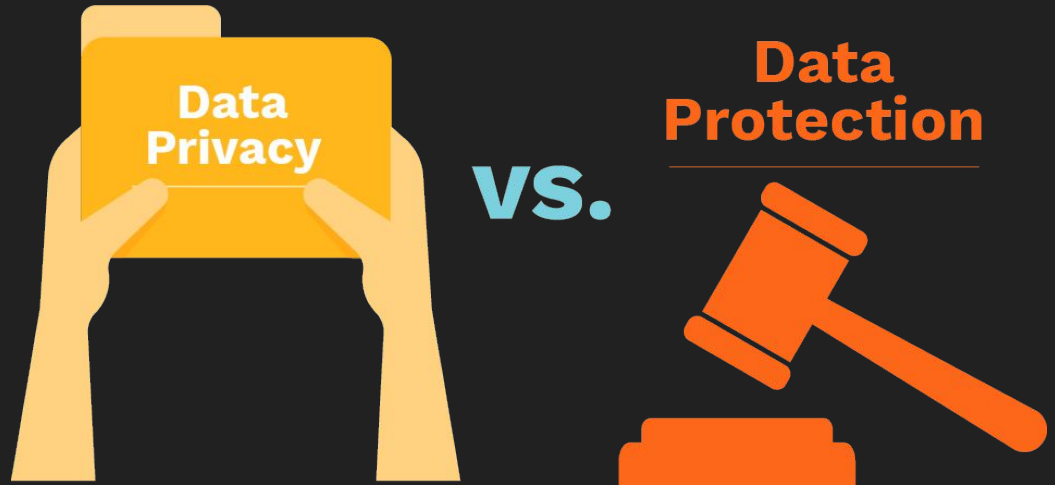
- Encryption is incredibly important to privacy
- We must find a balance between privacy and security
- The power of the public’s opinion
- There are limitation on how technology companies can help the government
- The need for clear policies regarding privacy and laws

Mohamed’s Lessons learned

- In IT companies, user privacy is important
- Software companies have to check their vulnerability
- Creating decryption software for the FBI will violate the company's First Amendment and Fifth Amendment rights

Leka’s Lessons Learned

- Although they both focus on the public, law enforcement and technology companies have different perspectives and priorities when it comes to privacy and security due to user wants and needs.
- Apple did a great job even if it might not have been moral to do so. On the other hand, once this request has been accepted, they will be more in the future. They can use any kinds of legal reason to invade people's privacy.



Thank you!
Any Questions

References

- https://www.cnbc.com/2016/03/29/apple-vs-fbi-all-you-need-to-know.html
- https://www.computerworld.com/article/3038269/apple-vs-the-fbi-the-legal-arguments-explained.html
- https://epic.org/documents/apple-v-fbi-2/
- https://blog.ipleaders.in/apple-vs-fbi/
- https://www.linkedin.com/pulse/fbi-v-apple-zachary-zynda#:~:text=The%20ethical%20issue%20in%20this,dangerous%20precedent%20for%20future%20companies.
- https://www.scu.edu/ethics/focus-areas/business-ethics/resources/apple-vs-fbi-case-study/#:~:text=Apple%20provided%20the%20FBI%20with,data%20after%20ten%20incorrect%20attempts.