Read the Wikipedia page on the FBI - Apple encryption dispute (<https://en.wikipedia.org/wiki/FBI%E2%80%93Apple_encryption_dispute>).  Then, discuss whether Congress pass a law that specifically addresses compelling equipment makers to assist in accessing encrypted data? If so, what should that law require?  You may use any other references you need to make your argument.

The FBI-Apple encryption dispute arises from an application that the FBI filed with the federal judge in California, seeking assistance with the search of an iPhone that was seized during an investigation of the December 2015 attacks in San Bernardino, CA. The court order required Apple to provide “reasonable technical assistance” in decrypting the phone since the agency was unable to access data on the locked iPhone. That is, the court issued an order requiring a custom hacking tool to be created and installed by Apple without unlocking or changing the data on the phone. However, Apple declined to help the FBI. Tim Cook, Apple’s chief executive at the time, argued that if the FBI could access this iPhone, nothing would stop them from doing it to many others. Apple also opposed the order request on the grounds that it is unlawful and unconstitutional. The company believed that if the order is granted, it will undermine the security of all Apple devices and set a dangerous precedent for future cases. However, the fact that law enforcement authorities insisted that the case was a onetime request resulted in them bringing the case to court. The case marked one of the highest clashes in the debate over encryption and data privacy between the government and a technology company.

For many years law enforcement agents have relied on their ability to intercept and exploit subject communications in furtherance of investigations. However, this scenario has been changing. Law enforcement authorities have begun saying that the encryption methods used by companies such as Apple make it harder for them to solve cases and stop terrorist attacks. On the other hand, Technology firms have kicked back, saying that encryption is key to protecting user data from hackers. Additionally, following the former National Security Agency contractor Edward Snowden’s leaks about the extent of the government’s surveillance activities, technology companies have begun to enhance encryption to safeguard their intellectual property and customer privacy. As a result, when served with proper legal process, companies such as Apple and Google claim that they cannot comply with court orders and provide law enforcement with the requested information or assistance. The companies claim that they are just unable to bypass the encryption designed by their own engineers.

Furthermore, a significant gap exists between what law enforcement believes is reasonable access to information, and what privacy experts and technology companies perceive as continued government overreach. Such companies and privacy experts assert that providing access to electronic devices by introducing vulnerabilities to assist law enforcement would unduly increase the risk of exposed information about individuals and businesses. Due to all of these reasons, Congress should step back from passing a law that specifically addresses equipment makers to assist in accessing encrypted data. Instead, law enforcement agencies should recognize that their requests for continued access to communications may present a risk to individuals and corporations, depending on the method(s) used.

References

<https://epic.org/amicus/crypto/apple/>

<https://www.hsdl.org/?abstract&did=811374>

<https://www.cnbc.com/2016/03/29/apple-vs-fbi-all-you-need-to-know.html>