United States V. Phone Companies - FICTIONAL CASE #5

On January 22, 2018, the suspects, two brothers, entered a New York City, New York County building where public government meeting were taking place. The two brothers, as suicide bombers, then ignited the bomb vests and killed twenty people, and seriously injured fifty others. Both suspected bombers were killed at the scene.

The officers recovered the brother's smart phone at their home with a warrant. Subsequent FBI investigations revealed that the suspects had recently pledged their joint allegiance to the Islamic State on a **social media site**. The FBI is investigating the attack as an act of terrorism. The suspects moved to the New York City area six months before the attack. One brother had been employed by the County for the eight months before the incident. The FBI obtained valid warrants to search both phones.

The Albany Sherriff's Office is also investigating the brothers in conjunction with a series of murders in where they resided before moving to New York City. The Sheriff obtained a warrant to search the suspects' home and is also seeking access to their smart phones.

The companies have cooperated with the government and complied with search warrants, sharing all of the data that had been uploaded from the phones onto the suspect's servers.

The law enforcement authorities now seek additional assistance, demanding that the companies create software to override e-Phone security features to access password-protected information stored on them that may be relevant to its investigation. They argue time is of the essence for obtaining additional information that may help them apprehend other possible suspects and prevent future terrorist attacks.
After repeated efforts, the FBI, the Sheriff or **third-parties** *(even those that were successful in the past)* have NOT been able to unlock the security codes on the e-Phones.

The companies emphasize here and in customer literature the protections that exist for the security and privacy of users, and the high priority placed on secure operating systems, with no bypasses or back doors – and with end-to-end encryption. The companies affirm their opposition to any government ordered backdoor that would weaken security and put customers' privacy and safety at risk.

A federal district court granted the FBI's request (and that of the Sheriff); the court issued an order under the All Writs Act, 28 U.S.C. § 1651(a), compelling the companies to help the FBI

access the locked e-Phones. The order requires the companies to create a security bypass to allow the FBI and the Sheriff access for National Security. The companies contend that they lack an existing method to bypass the security on e-Phones, and would need to "invent" such a process.

The companies appealed to the Circuit Federal Appeals Court and that, insofar as it was authorized, it violated the companies' First Amendment rights to free speech and Fourteenth Amendment Rights, including privacy. The Appeals Court ruled in favor of the companies.

The FBI was granted writ of certiorari by the Supreme Court (the court agreed to hear the case).

May use (FBI v. Apple) to help prepare your case.
Coding is considered free speech at this time.