Fourth Amendment Implications on the Search and Seizure of the Contents of a Smartphone

Abstract:

Fourteen people were killed in the San Bernardino shooting in December of 2015. In the process of investigating the shooting, the FBI wanted to legally compel Apple to give them access via a "master key" to the shooter's smartphone, which they were unable to unlock on their own. From this arose a question of cyber security, intellectual property and arguably most importantly, the rights of personal privacy for Americans. Apple refused to give the key and while a legal battle ensued, the FBI gained access to the shooter's phone by paying one million dollars for a private hacker to give them access. Since the point was now moot, the case did not continue. This left an important legal question unanswered: to what extent does the Fourth Amendment protect the individual from search and seizure of the contents of a smartphone? In general, a search or seizure is justified either through a warrant upon probable cause. However, there are certain exceptions to the warrant that can apply to smartphones. Most recently, the Supreme Court ruled in *Riley v. California* (2014) that the search incident to arrest exception to the warrant requirement does not justify a search of the contents of a smartphone. However, the question of whether the government can legally compel Apple to give them a "master key" remains unanswered. Many Americans today effectively have their entire lives on their smartphones, from banking information to personal messages much more. Primarily through Supreme Court decisions, this research examines the contexts in which the Fourth Amendment justifies a search of an individual's smartphone by a government agent.