

Forum:[Hack Forums](#)

Thread: [FBI vs. Apple](#)

Team4o4_temp - March 29, 2016, 11:43 am

Originally, the FBI wanted access to a shooters phone, but the settings were configured to erase all data if the passcode was entered incorrectly 10(I believe?) times. FBI comes to Apple demanding access using a law that is nearly 400 years old(365 years old), and requesting a loophole be found/created to access this phone. This sparked a topic of security vs privacy. Apple's claim that the encryption used even they could not break easily, as it would take 10 techs a period of 4 weeks in order to get in. As of recent, the FBI has canceled all court hearings with Apple as they have gained access through the help of a 3rd party.

What do you guys think about this?

Should the FBI tell Apple the method used so that security can be fixed to protect privacy, or classify the method so that it cannot be fixed?

Do you believe this 3rd party was the team that was paid nearly \$2million to produce a working iOS 9.3 jailbreak for a private party? Or could it have been one of the big name companies that helped decrypt the data?

What is your opinion/view point on this issue/situation?

Baghool - March 29, 2016, 5:40 pm

If they managed to do this, then why would they brag about this?

CryptoPy - March 29, 2016, 7:45 pm

If the FBI was granted access to the phone by the courts. The case would set precedence, and the FBI would have the means to unlock every other phone in the future

Team4o4_temp - March 30, 2016, 10:30 am

(Mar 29, 2016 07:45 PM)CryptoPy Wrote: [\[CITE\]](#) If the FBI was granted access to the phone by the courts. The case would set precedence, and the FBI would have the means to unlock every other phone in the future

The thing is though that the FBI did not gain access through the courts, rather through a 3rd party that got into the phone.

-VenoM - March 30, 2016, 10:37 am

(Mar 30, 2016 10:30 AM)Team4o4_temp Wrote: [\[CITE\]](#) The thing is though that the FBI did not gain access through the courts, rather through a 3rd party that got into the phone. Therefore, they lost the opportunity at a legal precedent of having iPhones unlocked. The FBI was fighting a losing battle with Apple, so they went to the next best thing... Just to hack the phone in the first place and potentially just have a contract with the Israeli firm they hired out for this specific iPhone.

Sure, they got into the phone now, but they haven't released any statements saying that anything was actually found on the phone right? Probably because the shooter wasn't stupid enough to plan a terrorist attack through his work phone and not destroy it..

Apple is asking how the FBI got into the phone now, and I'm sure they will majorly beef up security in their next update to ensure that whatever loophole was used is patched.

Team4o4_temp - March 30, 2016, 10:47 am

(Mar 30, 2016 10:37 AM)-VenoM Wrote: [\[CITE\]](#) Therefore, they lost the opportunity at a legal precedent of having iPhones unlocked. The FBI was fighting a losing battle with Apple, so they went to the next best thing... Just to hack the phone in the first place and potentially just have a contract with the Israeli firm they hired out for this specific iPhone.

Sure, they got into the phone now, but they haven't released any statements saying that anything was actually found on the phone right? Probably because the shooter wasn't stupid enough to plan a terrorist attack through his work phone and not destroy it..

Apple is asking how the FBI got into the phone now, and I'm sure they will majorly beef up security in their next update to ensure that whatever loophole was used is patched.

For a privacy and security standpoint, I believe beefing up the security would be excellent. What you stated in your first paragraph - do you mean that after this entry method is fixed, the FBI will not have grounds to start another court case demanding an iPhone unlocked?

-VenoM - March 30, 2016, 11:42 am

(Mar 30, 2016 10:47 AM)Team4o4_temp Wrote: [\[CITE\]](#) For a privacy and security standpoint, I believe beefing up the security would be excellent. What you stated in your first paragraph - do you mean that after this entry method is fixed, the FBI will not have grounds to start another court case demanding an iPhone unlocked? One of the main problems with the FBI taking something like this to court is there aren't any previous cases like this. The whole idea of 'precedence' everyone talks about is really about how decisions work on the bench for many judges. Judges are supposed to interpret the law to solve problems in specific cases. However... since something like this hasn't been decided before, a judge cannot reference a previous case like he/she normally would for these rare cases, to make a decision. This is why this debate has been so heated from both sides of the argument.

Apple's encryption is relatively unique because the information on a new iPhone is encrypted using the user's pass code. Apple can't actually unlock it without creating some sort of dangerous tool.

There haven't been cases in which Apple or any other company(as far as I know) have been forced to open a customer's phone. Therefore, any judge or justice's decision on this case would be the legal precedent in the future for any case such as this.

Once Apple patches whichever vulnerability was used, the FBI can easily muster-up another case just like this one, but they will go through the same legal battle and face losing it. Once they patch it and the Israeli company can't open it, I expect to see the same legal shitstorm to blow up any media outlets.

Team4o4_temp - March 30, 2016, 12:45 pm

(Mar 30, 2016 11:42 AM)-VenoM Wrote: [\[CITE\]](#) One of the main problems with the FBI taking something like this to court is there aren't any previous cases like this. The whole idea of 'precedence' everyone talks about is really about how decisions work on the bench for many judges. Judges are supposed to interpret the law to solve problems in specific cases. However... since something like this hasn't been decided before, a judge cannot reference a previous case like he/she normally would for these rare cases, to make a decision. This is why this debate has been so heated from both sides of the argument.

Apple's encryption is relatively unique because the information on a new iPhone is encrypted using the user's pass code. Apple can't actually unlock it without creating some sort of dangerous tool.

There haven't been cases in which Apple or any other company(as far as I know) have been forced to open a customer's phone. Therefore, any judge or justice's decision on this case would be the

legal precedent in the future for any case such as this.

Once Apple patches whichever vulnerability was used, the FBI can easily muster-up another case just like this one, but they will go through the same legal battle and face losing it. Once they patch it and the Israeli company can't open it, I expect to see the same legal shitstorm to blow up any media outlets.

As a frequent Apple user, I really do hope this will be discovered/fixed. I want to know that my data is secured. I believe I read that NAND cloning may have been the way in. I believe they just copy the current state of the phone, RAM and all, then they enter a passcode incorrectly up until the point at which it would erase all data, then they reset back to that "back-up"/NAND copy. This allowed them to brute force the passcode.

-VenoM - March 30, 2016, 7:58 pm

(Mar 30, 2016 12:45 PM)Team4o4_temp Wrote: [\[CITE\]](#) As a frequent Apple user, I really do hope this will be discovered/fixed. I want to know that my data is secured. I believe I read that NAND cloning may have been the way in. I believe they just copy the current state of the phone, RAM and all, then they enter a passcode incorrectly up until the point at which it would erase all data, then they reset back to that "back-up"/NAND copy. This allowed them to brute force the passcode. I can see this being the most probably case... However, I do believe Apple has mentioned something about patching that so that someone can't boot into recovery unless the phone's passcode has been entered. So, a patch may already be on the way for that type of hack...

Team4o4_temp - March 30, 2016, 8:25 pm

(Mar 30, 2016 07:58 PM)-VenoM Wrote: [\[CITE\]](#) I can see this being the most probably case... However, I do believe Apple has mentioned something about patching that so that someone can't boot into recovery unless the phone's passcode has been entered. So, a patch may already be on the way for that type of hack...

I believe to prevent NAND copying they need new hardware. I read that they are adding some security chip to make NAND expire/not be usable after copying.