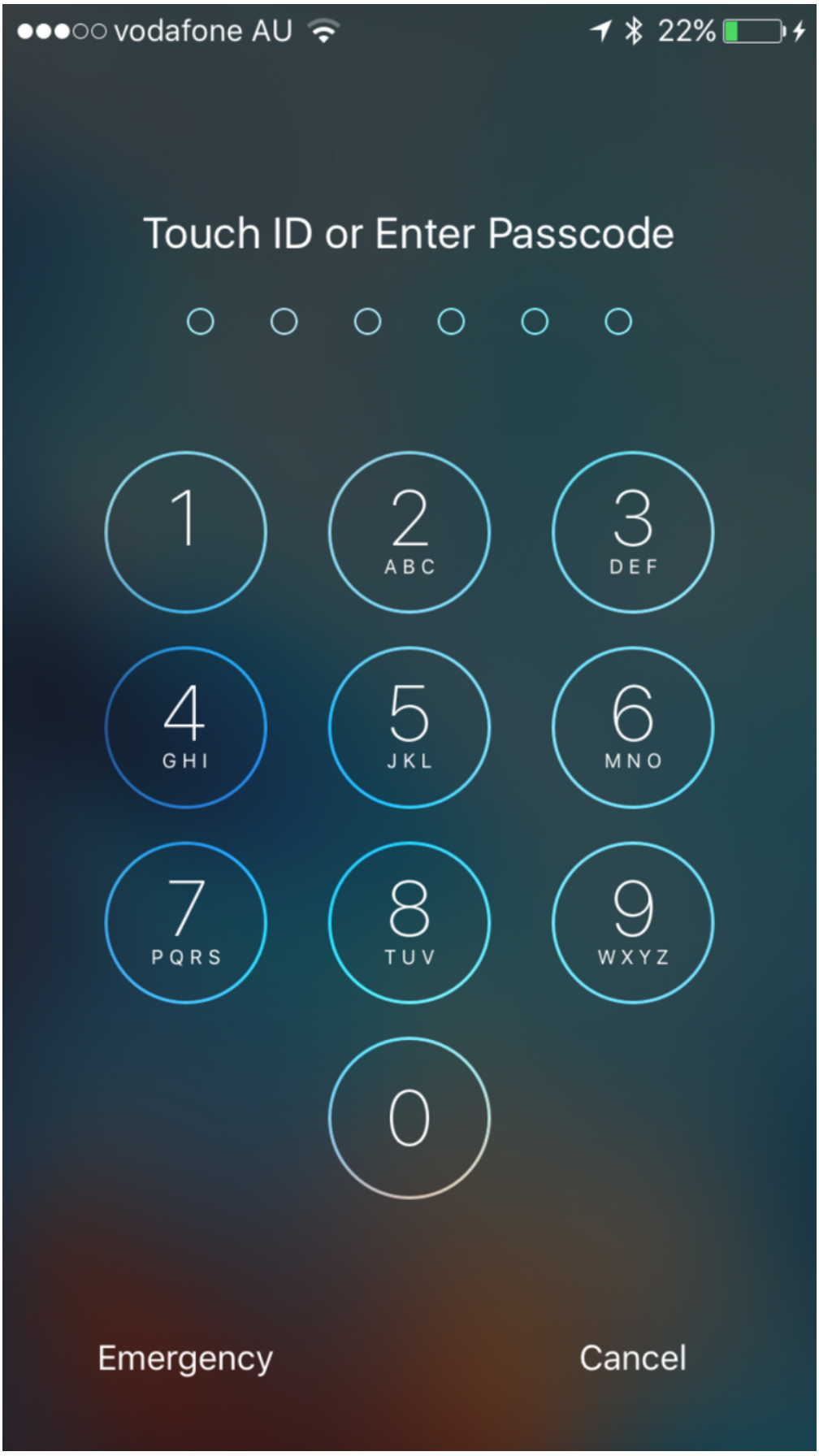
Opinion: The FBI drops its case against Apple that only made everyone's security worse

March 30 2016, by David Glance, University Of Western Australia


vodafone AU
22%
Touch ID or Enter Passcode
1
2 ABC
3 DEF
4 GHI
5 JKL
6 MNO
7 PQRS
8 TUV
9 WXYZ
0
Emergency
Cancel

Cracking the iPhone.

The FBI has succeeded in hacking into an iPhone that belonged to San Bernardino shooter Syed Farook without Apple's help. As a consequence, the FBI has dropped its legal case that was trying to force Apple to do what has been done by an unknown "third party".

Given the emotional investment by the FBI in this case and the apparent ease of giving it up, it is confusing many as to the motivation of bringing the case up in the first place. The most obvious possibility is that this case was all about the broader issue of encryption of software and the FBI's case against software companies implementing technology that makes US law enforcement's jobs more difficult in getting access to information. The second possibility is that the FBI used the publicity surrounding this case as a means of advertising to security firms and hackers that they needed help in cracking the phone. Either way, bringing the case to the courts was in the FBI's interests.

In the end, someone came forward to show the FBI how to do something that they claimed was impossible. The exact technique used is not known and it is unlikely that the FBI will disclose this information to Apple. Apple has made it abundantly clear that they would plug any particular security holes they became aware of and it is in their long-term interests to create software that can't be hacked by governments and even themselves.

Another consequence of the FBI not revealing their methods is that it is not known whether the particular exploit can be used against more modern phones with the latest version of iOS.

Apple has since released a statement that they are committed to helping law enforcement but want to increase the security of their products whilst engaging in a conversation about civil liberties, security and privacy.

For the FBI, the ability to access the phone will in all likelihood be a pyrrhic victory. It is very unlikely to reveal anything given that the San Bernardino shooters were careful about destroying other evidence before their rampage and the phone in question was a work phone and unlikely to contain any evidence related to their motives .

To a large extent, technology, and in particular encryption, is being used as a convenient excuse for law enforcement's general inability to prevent these sorts of crimes and to make meaningful progress after them. Blaming Apple or Google for the FBI's inability to answer questions about the motives and means of these sorts of crimes is extremely convenient.

It should be accepted that there will be limitations to the FBI's ability to know about, and prevent, these sorts of acts of violence. It may be that the general public has to accept that some small part of this is a consequence of all of us having security and privacy.

People will feel conflicted about this and that is to be expected. Nobody wants to see the perpetrators of such gross acts of violence getting away with their crimes or to have the possibility of people who could be apprehended still at liberty. However, the other side of the argument is equally unacceptable, that everyone cannot expect a certain level of security and privacy against all agencies, friendly or otherwise.

The questions being debated by Apple, the FBI and the general public are not ones of technology or pragmatic issues of convenient access. They are questions about whether the general public deserves a certain

level of privacy and security that is effective even against their own government. The consequences of this may be inconvenient but then we are willing to accept a wider democratic political system despite its obvious failings.

The FBI should never have brought this particular case to the courts. Whatever their motives, they have successfully avoided the central issues that should have been discussed and as a side-effect, broadcast to the world that the iPhone is vulnerable and can be hacked with relative ease. This has only succeeded in making things worse for the security of the general public, the very thing that the FBI was arguing that it was trying to protect.

This article was originally published on The Conversation. *Read the* original article.

Source: The Conversation

Citation: Opinion: The FBI drops its case against Apple that only made everyone's security worse (2016, March 30) retrieved 16 July 2024 from https://phys.org/news/2016-03-opinion-fbi-case-apple-worse.html