An iPhone, a Terrorist and a Court Order â€“ Why Appleâ€™s Privacy Fight is Misguided

February 19, 2016 â€“ In the battle between government snooping and privacy, I donâ€™t think there has ever been a time where we have come down on the side of the government. But there is a first time for everything. For us, itâ€™s the case of the terrorists who killed 13 people in San Bernardino. One of the shooters left behind a locked iPhone. On Tuesday, a federal judge ordered Apple to help the government unlock that iPhone. Yesterday, Apple CEO Tim Cook announced the company would fight that court order over user privacy concerns. Frankly, we think the company is picking the wrong privacy fight.

As you read through this, keep in mind that the phone the government is trying to unlock didnâ€™t actually belong to one of the shooters. It was a phone supplied to him by his employer; the County of San Bernardino. Because of this, every stitch of data on the phone also belongs to the county. Thatâ€™s pretty well established law. Both the county and the federal government want access to the data. No warrant is necessary since the county is giving its permission to gain access to the phone.

Also keep in mind that the iPhone in question was configured to wipe all data contained on the phone after ten consecutive unsuccessful attempts to break into it.

The court isnâ€™t asking Apple to break into iPhone in questions. The court order tells the company to provide a means to the government to bypass the feature that wipes the phone clean. This will allow them to continue to attempt to break into the phone without damaging any data it contains.

To date, Apple has refused to cooperate with the government. Their position has been that they donâ€™t have the tools requested by the FBI and that they would have to develop them. Their public position is this would create a back door to their operating system and could allow the government to spy on anyone.

But the court order allows the company to develop a tool that would only work on the phone in question. According to an article by former IOS hacker and current CEO of Sudo Security Group, Will Strafach, â€œOn a technical level, Apple could carry out the order by creating a RAM disk signed by the companyâ€™s production certificate for the specific ECID of the suspectâ€™s iPhone. This solution would allow Apple to use existing technologies in the firmware file format to grant access to the phone ensuring that there is no possible way the same solution would work on another device.â€•

Appleâ€™s chief concern seems to be that once the proverbial genie is out of the bottle, there is no way to put it back in. But if this genie can only be implemented for one specific phone at a time, and if Apple requires a court order before implementing it for the government â€“ now or in future cases â€“ the risk to privacy is minimal at best.

It should also be noted that Apple could conceivably avoid this issue in the future for its corporate clients by allowing those clients to preconfigure the phones they supply to their employees with a master password. Had that option been available, the County of San Bernardino would have been able to hand over the password to the FBI and all parties would have been able to avoid a court battle. There is absolutely no reason that employers shouldnâ€™t be able to have access to any computing device that they supply to their employees.
byJim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.
Follow me on Twitter:

Follow ACCESS