

From: **Wert, David (CAO)** dwert@cao.sbcounty.gov
Subject: Re: Media inquiry: Ars Technica
Date: February 20, 2016 at 8:26 PM
To: Cyrus Farivar cyrus.farivar@arstechnica.com

WD

Statement from the FBI:

STATEMENT TO ADDRESS MISLEADING REPORTS THAT THE COUNTY OF SAN BERNARDINO RESET TERROR SUSPECT'S IPHONE WITHOUT CONSENT OF THE FBI

Recent media reports have suggested that technicians in the county of San Bernardino independently conducted analysis and took steps to reset an iPhone 5C that was recovered during a federal search following the attack in San Bernardino that killed 14 people and wounded 22 others on [December 2, 2015](#). This is not true. FBI investigators worked cooperatively with the county of San Bernardino in order to exploit crucial data contained on a county-issued iPhone that was assigned to the suspected terror suspect, Syed Rizwan Farook.

Since the iPhone 5C was locked when investigators seized it during the lawful search [on December 3rd](#), a logical next step was to obtain access to iCloud backups for the phone in order to obtain evidence related to the investigation in the days following the attack. The FBI worked with San Bernardino County to reset the iCloud password [on December 6th](#), as the county owned the account and was able to reset the password in order to provide immediate access to the iCloud backup data. The reset of the iCloud account password does not impact Apple's ability to assist with the the court order under the All Writs Act.

The last iCloud data backup to the iPhone 5C was [10/19](#) and, based on other evidence, investigators know that Syed Rizwan Farook had been using the phone [after 10/19](#). It is unknown whether an additional iCloud backup to the phone after that date -- if one had been technically possible -- would have yielded any data.

Through previous testing, we know that direct data extraction from an iOS device often provides more data than an iCloud backup contains. Even if the password had not been changed and Apple could have turned on the auto-backup and loaded it to the cloud, there might be information on the phone that would not be accessible without Apple's assistance as required by the All Writs Act order, since the iCloud backup does not contain everything on an iPhone. As the government's pleadings state, the government's objective was, and still is, to extract as much evidence as possible from the phone.

Laura Eimiller
FBI Press Relations
Los Angeles Field Office

Sent from my iPhone

On Feb 20, 2016, at 11:16 AM, Cyrus Farivar <cyrus.farivar@arstechnica.com> wrote:

Hello,

Cyrus Farivar here, a journalist with Ars Technica.

I'd like confirmation that this is indeed the case, that a county employee reset the iCloud account at the request of the FBI. Is there any way that you or someone else from the county can help us piece together a timeline as to what was attempted when?

<http://mobile.reuters.com/article/idUSKCN0VS2GC>

Best,

-C

Sent from my iPhone

Cyrus Farivar

<http://arstechnica.com/author/cyrus-farivar/>