

**From:** Richard Kahn <[REDACTED]>  
**To:** "jeffrey E." <jeevacation@gmail.com>  
**Subject:**  
**Date:** Tue, 29 Mar 2016 21:56:06 +0000

---

james commentary on apple / fbi situation

Richard Kahn  
HBRK Associates Inc.  
575 Lexington Avenue 4th Floor  
New York, NY 10022  
tel [REDACTED]  
fax [REDACTED]  
cell [REDACTED]

Begin forwarded message:

**From:** james | personal genius <[REDACTED]>  
**Subject:** Re:  
**Date:** March 29, 2016 at 5:32:36 PM EDT  
**To:** Richard Kahn <[REDACTED]>

One more thing of note, had the FBI / DOJ prevailed in court, they'd have wide reaching new powers to compel third-parties to act on their behalf, even at the expense of the third-parties' self interest.

They could, for example, have a court compel me to install tracking software on Jeffrey's systems and forbid me from disclosing it. Not that they could actually get me to do something like that, but it's within their proposed legal justification.

Also relevant is this: <https://www.washingtonpost.com/news/the-watch/wp/2016/03/10/surprise-nsa-data-will-soon-routinely-be-used-for-domestic-policing-that-has-nothing-to-do-with-terrorism/>

The surveillance state is not just for terrorism anymore.

Thank you,

 James Ce, your Personal Genius,  
<http://personalgenius.us>

On Mar 29, 2016, at 5:19 PM, Richard Kahn <[REDACTED]> wrote:

interesting,,  
thanks

Richard Kahn  
HBRK Associates Inc.  
575 Lexington Avenue 4th Floor  
New York, NY 10022  
tel [REDACTED]  
fax [REDACTED]  
cell [REDACTED]

On Mar 29, 2016, at 4:22 PM, james ce | personal genius <[REDACTED]> wrote:

There are two likely methods\* that could have been used to access the data on that phone:

1. An unpublished “zero-day” bug that allows hackers to bypass the lock screen and access encrypted data on the phone.
2. A hardware solution where the memory chip (the flash storage on the phone) was un-soldered from the logic board, and plugged into a machine that can read / write the data from the chip (this is not new, this method was actually used in the 1985 movie “Real Genius”), which then duplicated the data on the chip and simulated the phone’s hardware.

With that setup you can brute-force try all four-digit passcode options. When the device slows down/erases the data from too many failed attempts, you just copy it over and pickup where you left off. Depending on how much data / size of the flash memory chip, you can restore the original data in 5-20 minutes.

The second method is MUCH more likely to have been used. It will work on any iPhone that does NOT have a fingerprint reader. Touch ID relies on a “secure enclave” chip that manages the login attempts and would be effectively impossible to impersonate — so this method is something that Apple is aware of and has considered.

\*there’s a third method called “de-capping” which involves using microlasers to sear off the top of the CPU to read the device’s unique identifier, which is the much more complex part of the two-part encryption key that the iPhone uses.

Basically, Apple uses this hardware device ID combined with the passcode as the key to encrypt the data. With the device ID, they can try to decrypt the raw data from the flash module within 10,000 tries.

The problem is that de-capping is very risky & fragile. If you cut a micron too deep you destroy the identifier you’re looking for and there’s no possibility of recovering the data in anyway after. This makes this method practically useless for any legal inspection.

We'll never know which, if either method was used — or even if any relevant data was recovered. Since the suspects are dead, any evidence recovered from the phone and the methodology used to access it will never be entered into any court case.

If the first method was used and such a zero-day does exist — then yes, a “hacker army” could have been theoretically unleashed on Apple. In that situation, it's very likely we'll see it used in a future public jailbreak method to break into the OS — hackers are notoriously bad at keeping secrets, being that exposing secrets is the primary motivation for most hackers — at which point Apple will find out about it and fix it.

---

It's at least equally as likely that the whole “we broke in without Apple's help” story is complete fiction that the FBI / DOJ used it as an excuse to bail from a case that was going to make them look like technical incompetents, and would be lost, setting the precedent they want in the wrong direction.

The last brief Apple filed exposed some major technical inaccuracies in the DOJ briefs, and any hearing would have included Apple Engineers schooling the courts on the basics of how encryption works and embarrassed the FBI's technical resources.

Also, remember that this iPhone belonged to the terrorist's employer. Both he & his wife had personal cell phones and computers which they destroyed the day of the attack. The iCloud backup of this phone from a couple weeks previous to the attack revealed NO personal email, text messages or any other internet accounts on the device. It's very unlikely that iPhone was ever used for anything outside of work or contains anything of value to investigators.

This case was never about anything on that phone, rather it was a hot-button political case to expand the government's investigatory powers.

(Also, contrary to that article's subheading, the FBI never asked for Apple to unlock the phone before pursuing legal orders... that sounds nitpicky, but were they actually concerned with the contents of the device, you'd expect the FBI to ask nicely before trying to force-conscript private corporate resources into rewriting the device's operating system.)

I bet this will come up again as soon as the FBI's newest toys stop working, but next time it will be an Android device in hopes that Google won't raise as much of a fuss as Apple.

 James Ce, your Personal Genius,  
<http://personalgenius.us>

On Mar 29, 2016, at 3:27 PM, Richard Kahn <[REDACTED]> wrote:

<http://www.thedailybeast.com/articles/2016/03/29/did-the-fbi-just-unleash-a-hacker-army-on-apple.html>

thoughts?

Richard Kahn  
HBRK Associates Inc.

575 Lexington Avenue 4th Floor

New York, NY 10022

tel

fax

cell