Forbes

Warrant Let L.A. Cops Force Open Apple iPhone With Owner's Fingerprints

Thomas Fox-Brewster

March 31, 2016

It's been a year and a half since an American judge declared it legal to use criminal suspects' fingerprints to open up smartphones. In a landmark 2014 decision, a Virginia Beach Circuit Court ruled that David Charles Baust, accused of strangling his girlfriend and later found not guilty, could not be forced into handing over the passcode for his iPhone. But he could be compelled to supply his biometric information used to unlock the device.

Since then, however, no evidence has emerged of police trying to open iPhones with users' prints. Until now. In February, as the FBI tried to force Apple to help it access the iPhone of San Bernardino shooter Syed Rizwan Farook – a contentious case that came to a close this week with the FBI hacking its own way in – cops down the road acquired a warrant letting them apply a user's fingerprints to an Apple device of interest. That warrant, uncovered by FORBES and dated 25 February 2016, allowed an LAPD detective to visit the premises of a Paytsar Bkchadzhyan in Glendale, C.A., and take the latter's fingerprints to open up their iPhone.

Signed off by a judge in the District Court in the Central District of California, the warrant's killer line, on the final page of the short document, reads: "Law enforcement personnel are authorized to depress the fingerprints and/or thumbprints of the person covered by this warrant onto the Touch ID sensor of the Apple iPhone seized… on 25 February."

What's unclear from the warrant, though court records show it was executed, is what happened once the document was signed off. Cops could have taken fingerprints directly from Bkchadzhyan. Alternatively, as hackers have proven possible in recent years, they could have obtained a fingerprint from an object, such as a glass, and used it to create a fake finger that would unlock the iPhone. The handwritten inventory of property taken in the search is ambiguous: "PAYTSAR BKCHADZHYAN – FINGERPRINT ON IPHONE DEVICE."

It's also unclear what interest Bkchadzhyan was to the LAPD. Not only are there no related files in PACER, the government's online court document repository for federal cases, or in state court databases, there's little information about Bkchadzhyan elsewhere. A Google search for the surname alone yields zero results.

The LAPD had not responded to repeated requests for comment. FORBES' attempts to contact the detective who signed the warrant were unsuccessful, though it was apparent Special Agent Raymond Martinez was part of LAPD's homicide division.

Apple declined to comment. The DoJ did not provide a statement, whilst the court for the Central District of California could not be reached at the time of publication.

A unique case

Regardless of the details of the case, the document found by FORBES is the first warrant of its kind to be published outside of the confines of PACER and state court servers.
If Bkchadzhyan's hand was used as the executed warrant suggests, it's also the first known case in which a smartphone has been unlocked by someone legally compelled to use their fingerprints. Whilst Baust's fingerprints were taken in 2014, according to his legal representation at the time, James Broccoletti, the device didn't open as a passcode was also required; after 48 hours of not using Touch ID or a reboot Apple asks for the code to be re-entered.

Apple's time and reboot limits on Touch ID use could explain why police have rarely sought to use fingerprints, at least to the public's knowledge. FORBES has trawled through hundreds of court documents, looking at cases where police have sought to gain access to iPhones and other smartphones, but could find no other examples of warrants used to apply fingerprints to devices.

In many cases, police have been forced to take forensic means to enter a smartphone, according to numerous court documents. The iPhone is often a cause of frustration (click through for warrants), whilst Google Android phones, especially those made by Samsung, are regularly cracked open with forensic techniques, as in the case of another iPhone linked to ISIS, owned by alleged terrorist supporter Aws Mohammed Younis Al-Jayab.

Often that analysis involves tools from Cellebrite, the Israeli company rumoured to have offered the FBI help in unlocking the San Bernardino phone. Where those forensic means have failed, cops have sought assistance from tech companies. In the recent fight with the Department of Justice over Farook's iPhone 5C, Apple was asked to provide a version of iOS that would allow for infinite guesses of the passcode.

\There are also some compelling legal arguments that act as a deterrence to cops in a rush to open devices with legally-acquired biometric information. Despite the ruling in Baust's case, lawyer Marina Medvin believes that whilst fingerprints from dead suspects can be used to open iPhones (as explored in a previous FORBES article), they shouldn't be allowed on living

suspects. Protections under the 5th Amendment should prevent any kind of self-incrimination, which includes handing over authentication for a smartphone, says Medvin. She believes the L.A. warrant shows Bkchadzhyan was "forced" into handing over fingerprint data, something Medvin says is legally dubious.

"He's being forced to provide everything in that iPhone, he's being compelled to do that. It's a Fifth Amendment issue, there's no question about it," Medvin added. "The government cannot force you to produce papers that are not in your interest because that is protected by the Fifth Amendment. Well if you're being forced to provide a fingerprint that is linked to every private document, photograph, search history, location history, all the private information you own, all in one place, then how can that possibly be OK? How is that not a violation of the Fifth Amendment?"

On the other side, lawyers claim there are no Fifth Amendment protections, as the judge ruled in Baust's case. Even Broccoletti, who argued for such protections for Baust in 2014, now believes that ruling was correct. "The law is clear in the U.S. that fingerprints, like blood samples or buccal swabs, do not involve Fifth Amendment protection since they are non-testimonial," said Broccoletti. "Therefore they can be compelled to be produced.

"It is beyond debate… the distinction lies in the production of something physical, a print, versus something mental, the process of producing the passcode. Think of it like having the combination to a safe in your head, you can't be compelled to produce that because of the mental process involved. The physical part, the print, is non-testimonial; the mental part, the passcode, is." Broccoletti said he had only argued for the Fifth in 2014 to "cover all bases".

There's a middle ground: that context is key. Each separate case requires a different approach, explains Marcia Hoffmann, the lawyer who predicted legal troubles with fingerprints and smartphones back in 2013, before Apple had even launched Touch ID. "The Fifth Amendment privilege against self-incrimination is extremely dependent on the facts of each case," Hoffmann said over email. "As a general matter, I think the Fifth Amendment is less likely to apply in a situation involving compelled disclosure of biometric data."

As there's no clear legal guidance for using a fingerprint to access a device, police may also avoid filing warrants as the LAPD did. "If you've got the thumbprint already, and a warrant to search the phone, there's no reason you'd need some separate warrant specifying that you can use the thumbprint to unlock the phone, or necessarily need to specify in the warrant affidavit how you're going to do the unlocking," said Julian Sanchez, senior fellow at the Cato Institute.

With just two known test cases, such sticky legal ground is yet to be thoroughly explored. Evidently, in L.A. at least, police believe they have the legal right to open smartphones with people's biological data.