Feds Can't Force You To Unlock Your iPhone With Finger Or Face, Judge Rules

Thomas Brewster Forbes Staff
Cybersecurity
I cover crime, privacy and security in digital and physical forms.

Social Media Data Security NURPHOTO VIA GETTY IMAGES

A California judge has ruled that American cops can’t force people to unlock a mobile phone with their face or finger. The ruling goes further to protect people’s private lives from government searches than any before and is being hailed as a potentially landmark decision.

Previously, U.S. judges had ruled that police were allowed to force unlock devices like Apple's iPhone with biometrics, such as fingerprints, faces or irises. That was despite the fact feds weren't permitted to force a suspect to divulge a passcode. But according to a ruling uncovered by *Forbes*, all logins are equal.

The order came from the U.S. District Court for the Northern District of California in the denial of a search warrant for an unspecified property in Oakland. The warrant was filed as part of an investigation into a Facebook extortion crime, in which a victim was asked to pay up or have an "embarassing" video of them publicly released. The cops had some suspects in mind and wanted to raid their property. In doing so, the feds also wanted to open up any phone on the premises via facial recognition, a fingerprint or an iris.

While the judge agreed that investigators had shown probable cause to search the property, they didn't have the right to open all devices inside by forcing unlocks with biometric features.

On the one hand, magistrate judge Kandis Westmore ruled the request was "overbroad" as it was "neither limited to a particular person nor a particular device."

But in a more significant part of the ruling, Judge Westmore declared that the government did not have the right, even with a warrant, to force suspects to incriminate themselves by unlocking their devices with their biological features. Previously, courts had decided biometric features, unlike passcodes, were not "testimonial." That was because a suspect would have to willingly and verbally give up a passcode, which is not the case with biometrics. A password was therefore deemed testimony, but body parts were not, and so not granted Fifth Amendment protections against self-incrimination.

That created a paradox: How could a passcode be treated differently to a finger or face, when any of the three could be used to unlock a device and expose a user's private life?

And that's just what Westmore focused on in her ruling. Declaring that "technology is outpacing the law," the judge wrote that fingerprints and face scans were not the same as "physical evidence" when considered in a context where those body features would be used to unlock a phone.

"If a person cannot be compelled to provide a passcode because it is a testimonial communication, a person cannot be compelled to provide one's finger, thumb, iris, face, or other biometric feature to unlock that same device," the judge wrote.

"The undersigned finds that a biometric feature is analogous to the 20 nonverbal, physiological responses elicited during a polygraph test, which are used to determine guilt or innocence, and are considered testimonial."

There were other ways the government could get access to relevant data in the Facebook extortion case "that do not trample on the Fifth Amendment," Westmore added. They could, for instance, ask Facebook to provide Messenger communications, she suggested. Facebook has been willing to hand over such messages in a significant number of previous cases *Forbes* has reviewed.

Law finally catching up with tech?

Over recent years, the government has drawn criticism for its smartphone searches. In 2016, *Forbes* uncovered a search warrant not dissimilar to the one in California. Again in the Golden State, the feds wanted to go onto a premises and

force unlock devices with fingerprints, regardless of what phones or who was inside.

Andrew Crocker, senior staff attorney at the digital rights nonprofit Electronic Frontier Foundation, said the latest California ruling went a step further than he'd seen other courts go. In particular, Westmore observed alphanumeric passcodes and biometrics served the same purpose in unlocking phones.

"While that's a fairly novel conclusion, it's important that courts are beginning to look at these issues on their own terms," Crocker told *Forbes*. "In its recent decisions, the Supreme Court has made clear that digital searches raise serious privacy concerns that did not exist in the age of physical searches—a full forensic search of a cellphone reveals far more than a patdown of a suspect's pockets during an arrest for example."

The magistrate judge decision could, of course, be overturned by a district court judge, as happened in Illinois in 2017 with a similar ruling. The best advice for anyone concerned about government overreach into their smartphones: Stick to a strong alphanumeric passcode that you won't be compelled to disclose.

I cover security and privacy for Forbes. I've been breaking news and writing features on these topics for major publications since 2010. As a freelancer, I worked for The Guardian, Vice Motherboard, Wired and BBC.com, amongst many others. I was named BT Security Journalist o... MORE

Got a tip? Get me on Signal on +447837496820 or use SecureDrop to tip anyone at Forbes. Email at TBrewster@forbes.com or tbthomasbrewster@gmail.com for PGP mail.

Retail Experiences: Here's How To Avoid A Bad One