Court: Cops Can’t Force You to Unlock a Phone With Biometrics

A California federal judge rules that police cannot compel users to unlock their devices with facial recognition, fingerprints, or other forms of biometrics.

January 15, 2019 2 min read

This story originally appeared on PCMag

If a police officer or federal investigator wants to get into your smartphone, they can no longer use your eyes, face, or fingerprint to force you to unlock it.

A federal judge in Northern California has ruled that compelling a device unlock using biometric data is a violation of Fifth Amendment rights against self-incrimination. Cops are already barred from asking suspects to unlock their devices with a passcode, thanks to a Florida appeals court decision this past October. With this decision, biometric login mechanisms are afforded the same protection.

In her decision, Judge Kandis Westmore said that fingerprints and face scans such as Face ID on iOS devices are not the same as physical evidence, and that even with a warrant, the government has no right to force suspects to incriminate themselves.

“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,” she wrote.

The case hinged on Judge Westmore denying a warrant to police officers investigating an alleged extortion crime in Oakland, California, where the suspects used Facebook Messenger to threaten the release of a compromising video. She said officers had probable cause to search the suspects' property, but not to unlock any devices or compel suspects to do so.

Apple and other device makers have pushed back against forced device unlocks in many forms for years. The warrant denial, and the precedent it sets for protected biometric data, is a significant decision for digital privacy as well as search and seizure law in the connected devices era.

https://www.entrepreneur.com/article/326359