Government can't force people to unlock phones using facial recognition, fingerprints: Federal judge

January 18 2019, by Ethan Baron

Credit: CC0 Public Domain

A federal judge in Oakland ruled that law enforcement agencies cannot force people to use biometric features such as facial-recognition to

unlock their phones and other devices in a case that highlights the fight between Big Tech and law enforcement over users' privacy.

The decision arose out of an extortion case in which two suspects allegedly used Facebook Messenger to threaten that if a man didn't give them money, they would distribute embarrassing video of him.

Judge Kandis Westmore took no issue with authorities' request for a warrant to search an Oakland home associated with the two men, and possibly seize cell phones and computers.

"The Government, however, also seeks the authority to compel any individual present at the time of the search to press a finger (including a thumb) or utilize other biometric features, such as facial or iris recognition, for the purposes of unlocking the digital devices found in order to permit a search of the contents as authorized by the search warrant," Westmore wrote in her ruling. But the judge said that would be unconstitutional.

Advances in mobile-device technology have pitted technology giants against law enforcement. Firms encrypt data and improve the security of unlocking features to satisfy customers' desire for privacy, while authorities argue that they need to access evidence inside devices to fight crime and keep the public safe. The issue came to a head in a high-profile battle between Apple and the FBI over access to the encrypted iPhone phone of a man who shot and killed 14 people in San Bernardino in 2015. Ultimately, the FBI didn't need Apple to get into the phone—the agency paid $900,000 to have it done, U.S. Sen. Dianne Feinstein has said.

The Oakland case puts a new spotlight on the collision between the judicial system and rapidly evolving technology, said UC Berkeley law school teaching fellow Megan Graham.

"These are issues that judges are seeing more and more and they're having to confront how we protect Constitutional rights when new technologies are involved," Graham said Tuesday.

The Oakland judge said allowing authorities to force citizens to unlock devices via biometric features in this case would violate the Constitution's Fourth Amendment protection against unreasonable search. The government's request for intrusion into seized devices was too broad because it targeted anyone at the Oakland location believed to be a user of a seized device and wasn't limited to the two suspects, Westmore said.

Permitting forced biometric unlocking in this case would also break the Fifth Amendment against self-incrimination, Westmore said, noting that courts have ruled that people can't be forced to reveal a numeric passcode to a device.

"While the Court sympathizes with the Government's interest in accessing the contents of any electronic devices it might lawfully seize, there are other ways that the Government might access the content that do not trample on the Fifth Amendment," Westmore wrote.

Authorities could seek Messenger communications from Facebook, with a warrant if need be, she suggested. "While it may he more expedient to circumvent Facebook, and attempt to gain access by infringing on the Fifth Amendment's privilege against self-incrimination, it is an abuse of power and is unconstitutional," Westmore wrote.

Law enforcement agencies routinely obtain data from seized devices by getting subpoenas, warrants and court orders compelling tech firms to divulge information. Police also use software to break into seized devices they have a warrant to search. But the government can't force citizens to use any biometric features to unlock devices, Westmore ruled.

"The Government may not compel or otherwise utilize fingers, thumbs, facial recognition, optical/iris, or any other biometric feature to unlock electronic devices," she said in her Jan. 10 decision.

Digital-privacy group Electronic Frontier Foundation applauded the ruling.

"Digital devices today typically contain far more sensitive information than would ever be found found in a person's home," said EFF staff lawyer Jamie Lee Williams. "Unlocking a phone effectively gives law enforcement access to all of the data on the phone. Given the sheer amount of data on modern day cell phones, the government simply cannot anticipate the full contents of someone's phone, and any order compelling someone to unlock their phone—whether via a numeric passcode or a fingerprint scan—violates the Fifth Amendment privilege against self-incrimination."

UC Berkeley's Graham noted that the Oakland ruling came from a lower federal court, and said she expected the issue of forced biometric unlocking of devices to end up before the U.S. Supreme Court.