Passwords, Biometrics, and the Evolving Legal Status of Encryption

The 4th and 5th Amendments to the Constitution

The 4th and 5th Amendments are among the most important principles of the U.S. court system:

- 4th Amendment: the right against unreasonable search and seizure
- 5th Amendment: the right against self-incrimination

However, with the increasing usage of encryption and biometric passcodes, the way these doctrines are applied has shifted with the emergence of new technology. There currently exists ongoing legal controversy over their application in case-law dependent on evidence that may be obtained from encrypted laptop drives, passcode locked devices, and biometrically locked phones.

Where does the right not to reveal your password currently stand?

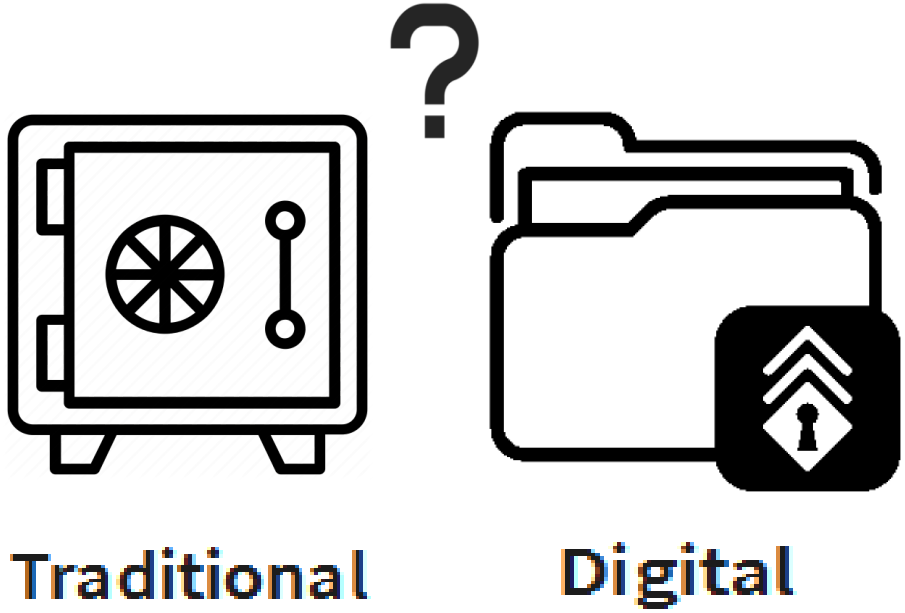
Currently, most courts recognize at least some application of the 5th amendment regarding passwords, allowing suspects the ability to refuse to unlock their phones when encrypted using a string of characters or a PIN.

However...

There is one major exception to this known as the ‘Foregone Conclusion’ doctrine. In court, this means that when the contents behind a lock are already known by investigators, then the 5th Amendment right against self-incrimination no longer applies, as the potential incriminating evidence is already known to prosecutors and therefore a ‘foregone conclusion’. In these instances, the court can force the suspect to relinquish their password.

What is the legal precedent on forcing suspects to reveal keys?

Traditional cases before the advent of digital locking tended to revolve around examples where the suspect has a safe that may contain incriminating evidence, but investigators do not know the combination lock. Whether the suspect must reveal the lock is up to the court's discretion according to the Foregone Conclusion doctrine. The current question is: Can we treat digitally encrypted files the same as traditional locked vaults?



Passcode locks vs Biometric locks – which is more legally secure?

Current case-law has also found itself muddled in the legal difference between passcode and biometric locks. Although both types can normally be used interchangeably for the same purpose, the explicit ‘key’ utilized may affect the government’s ability to compel a suspect to unlock a device.

Passcode locks are more legally secure than biometric locks

- A passcode lock, such as PIN or password, is legally considered safer as it is knowledge inherent in one's mind and not a physical fact of evidence; this gives more solid ground to be defended under the 5th Amendment right against self-incrimination, since revealing the contents of one's mind is considered legal 'testimony'.

- A biometric lock is more vulnerable to forced disclosure since 'physical features' such as one's fingerprint and face ID are not inherent to one's mind and not considered 'testimony' in the legal sense. This means courts can more easily compel suspects to unlock their devices without running afoul of their constitutional rights.

Jurisdictions offer conflicting precedent across the country

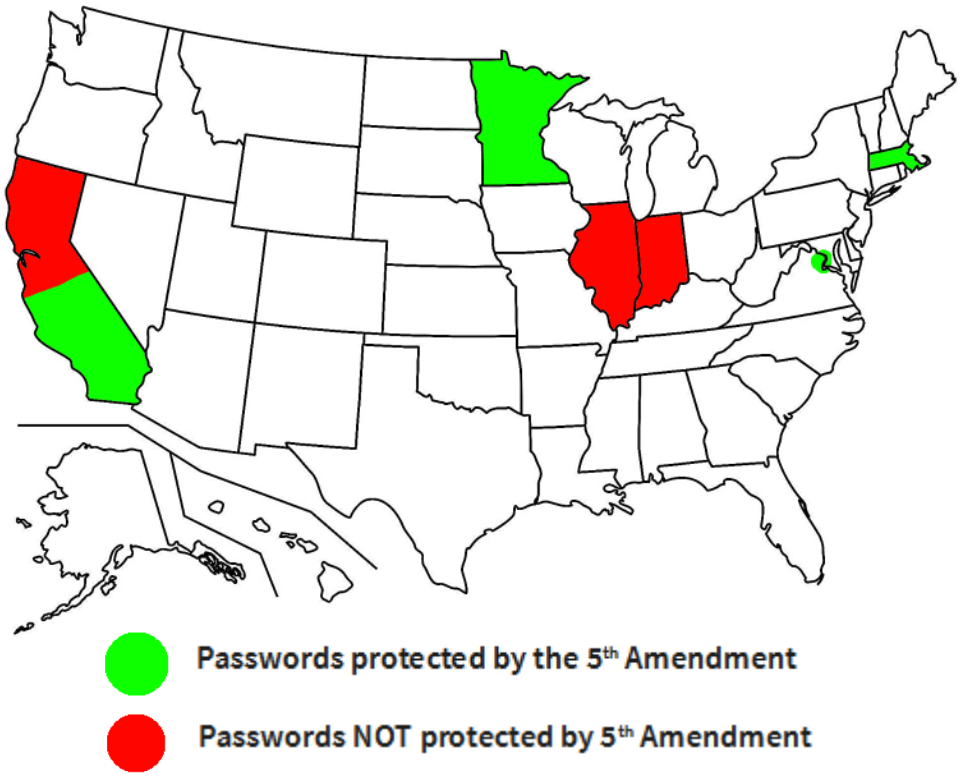
Although the general trend across the country is to see biometric locks on weaker legal ground than passcode locks, courts in various states and circuits are still in conflict over just how broad or limited the 5th and 4th Amendment rights regarding digital devices are.

Arguments have been made claiming that personal phones are more private and sensitive than even one's own home; this means that police and investigators may not even be able to turn your device on and see the lock screen without a warrant.

Jurisdictions offer conflicting precedent across the country (cont.)

In general, courts remain divided:

- D.C. – courts have stated that biometric data can be compelled out of a witness without violating the 5th Amendment
- Minnesota – courts are of the same opinion
- Los Angeles – courts have also reached a similar conclusion about compelling biometric unlocks from suspects
- Massachusetts – the state Supreme court has even ruled that neither a password or device are testimony
- Chicago – however, has upheld suspects rights to not reveal their password
- Northern California – a circuit court also disagreed with forced biometric unlocks
- Indiana – the state Supreme Court has ruled that passwords can give access to incriminating evidence and therefore fall under 5th Amendment protection



Bypassing the suspects – The Apple-FBI iPhone encryption dispute

- In 2016, in the wake of the San Bernardino terror attacks in Southern California, the FBI desired access to the deceased suspects' work iPhone for further leads on what happened. They found that the workphone was encrypted. Since the suspects could not unlock it as they were dead, the FBI went straight to Apple in an attempt to get the phone unlocked.
- Apple refused to unlock the phone or implement a backdoor. The FBI filed suit against the company in response, requesting that a judge force Apple to remove the encryption on the phone.
- The legal battle persisted for a number of months until the FBI found a private company capable of bypassing the encryption, and dropped the case against Apple.

SUMMARY: This incident demonstrates that encryption is not only an important legal consideration on the suspect's end but it's also important which company a suspect trusts to secure his or her devices.

Questions?