Travelers Beware – Compelled to Open Your Phone?

Thursday, March 21, 2019

Recent rulings conflict on whether police can force individuals to unlock their smartphones. The result depends upon where you are located, with differing rulings from Massachusetts and California. Further, there is an international dimension, illustrated by a recent decision from Israel. In short, as described below, the traveler must beware.

The United States Standard for Searching a Phone

In its 2014 decision, Riley v. California, a unanimous Supreme Court held that a warrant is “generally required” before searching a cell phone seized incident to an arrest, unless there is a need to prevent the imminent destruction of evidence, pursue a feeling suspect, or assist persons who are injured or threatened with imminent injury. The Court required this protection because cell phones contain massive troves of private personal information that in any other context would not be so accessible.

Securing a Warrant Is Only Half the Battle

With modern encryption and password technology, however, a warrant is useless unless the government can force a person to unlock their phone.

On March 6, the highest court in Massachusetts ruled in Commonwealth v. Dennis Jones that the State can compel a person to unlock their phone as long as it can prove beyond a reasonable doubt that the person knew the password. The Court, in applying the “foregone conclusion” doctrine, reasoned that it does not violate the Fifth Amendment right against self-incrimination because the question of extracting the password is “not of testimony but of surrender.”

A Tel Aviv District Court handed down an equally favorable ruling to law enforcement when it allowed Israeli police to use “reasonable force” in obtaining a drug trafficking suspect’s fingerprint to unlock his phone. The Court based its decision on the right of police to use reasonable force in taking a suspect’s fingerprint when conducting an external search.

Constraints on State Power to Compel Phone Access

In stark to contrast to both decisions, a United States District Court of Northern California recently held that forcing a person to provide a biometric feature to unlock their phone violates the Fifth Amendment. Magistrate Judge Westmore rebuked the “foregone conclusion” doctrine, as applied in Commonwealth v. Dennis Jones, on the grounds that smart phones contain so much data that the Government cannot possibly have sufficient knowledge of their contents to render it a question of mere surrender. Additionally, her analysis countered the Israeli decision by highlighting that forcibly unlocking a phone by fingerprint concedes ownership and control of the device, which provides fundamentally different information from a traditional fingerprinting, which is a mere comparison of physical evidence, i.e., one fingerprint to another.

Justice Lenk’s concurrence in the Massachusetts adopted a similar line of analysis to the Northern California decision. Justice Lenk emphasized that the Commonwealth must prove its prior knowledge of the existence and location of the files as well as that the suspect knows the passcode.
Conclusion

The unsettled situation requires the traveler to beware. Different rules apply depending on where you travel. For analysis of this problem in the context of crossing the US border, see our post on the border search of electronic devices.

© Copyright 2019 Squire Patton Boggs (US) LLP

Source URL: https://www.natlawreview.com/article/travelers-beware-compelled-to-open-your-phone