Reexamining the Privilege against Self-incrimination in Light of Recent Technological Advancement

Amos Eytan

(Based on a paper written with Dr. Haim Wismonsky)

In recent years, law enforcement agencies around the world have been facing increasing difficulties regarding the need to search password-protected and encrypted computers, cellular phones, specific apps or online services. These difficulties received the public's attention mostly after the terror attack in San-Bernardino on 2015. After the attack, the FBI approached Apple and asked for Apple's assistance in overriding the encryption on one of the terrorists' phone, because the FBI had no technical ability to override the encryption on its own in a reasonable timeframe.

This case and many others indicate the collision between the needs of law enforcement agencies around the world to lawfully search the computers and cellular phones of suspects and witnesses, and the devices owners' privilege against self-incrimination.

I will address the main challenges that law enforcement agencies are facing due to recent technological advancement in this aspect, and will offer a theoretical and practical course of action, focusing on the privilege against self-incrimination. The privilege is usually considered as an absolute privilege, while the privilege's justifications may equally lead to an interpretation of the privilege as a relative privilege, meaning that it may be balanced with other interests on a case-by-case manner.

I will offer a legal model meant to balance between the need of law enforcement agencies to overcome security measures installed on phones and computers of suspects and witnesses, and the owners' privilege against self-incrimination. The legal model describes the privilege against self-incrimination as a relative privilege, and consists of a few guidelines that will be examined on a case-by-case basis.