Overcoming encryption and password protection-legal challenges

Haim Wismonsky

בשנים האחרונות מתמודדות רשויות אכיפת החוק ברחבי העולם עם קשיים הולכים וגוברים בכל הנוגע לצורך להתגבר על הגנות סיסמה והצפנה אשר מותקנות על מחשבים, מכשירי טלפון ניידים, יישומים ספציפיים או שירותים מקוונים. קשיים אלה צפו ועלו לתודעה הציבורית בעיקר לאחר פיגוע הטרור שבוצע בעיר סן-ברנרדינו בארצות-הברית בשנת 2015 ובהתדיינות המשפטית שבין ה-FBI לחברת Apple שהתקיימה לאחר מכן. מקרה זה ורבים אחרים מעידים על התנגשות בין צרכיהן של רשויות החקירה והביטחון בארץ ובעולם בבואן לחדור, על פי סמכות כדין, למחשבים ולטלפונים סלולריים, לבין זכויותיהם של המשתמשים לפרטיות, זכות השתיקה ולחסיון מפני הפללה עצמית.

ישנן מספר טכנולוגיות מרכזיות המשמשות כיום - ובעתיד הנראה לעין - לצורך הגנה מפני חדירה או עיון בלתי-מורשים בחומרי מחשב האגורים במחשב או בטלפון סלולרי, וביניהן זיהוי פנים, טביעת אצבע, זיהוי קולי ועוד.

אומנם מקובל, היסטורית, לראות בחיסיון מפני הפללה עצמית משום חיסיון מוחלט, כאשר הוא מוחל. אולם בהרצאה אנסה להציג מודל משפטי להתמודדות עם סוגיית המתח בין רצונן של רשויות החקירה להתגבר על אמצעי האבטחה על מכשירי הטלפון הסלולריים והמחשבים של חשודים ונחקרים, לבין זכויותיהם של בעלי המכשירים לחיסיון מפני הפללה עצמית ולפרטיות. המודל המשפטי המוצע מכיר בחיסיון מפני הפללה עצמית כחיסיון יחסי, ומבקש לערוך איזון קונקרטי בין הזכויות והאינטרסים המתנגשים. זאת, בהתאם למספר קווים מנחים, אשר יורכבו הן מכללים נוקשים, שהם בבחינת תנאי סף, והן מפרמטרים שייבחנו בכל מקרה ומקרה.

Overcoming encryption and password protection-legal challenges

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, and the legal proceedings that took place after the attack between the FBI and Apple. This case and many more, indicate the collision between the needs of law enforcement and security agencies around the world to lawfully search the computers and cellular phones of suspects and witnesses, and the devices owners' rights to privacy and the privilege against self-incrimination.

There are several technologies used today – and in the foreseeable future – in order to prevent unauthorized access to computer material stored on computers and cellular phones, including face recognition, finger print, vocal identification and so on.

In my lecture I will wish to present a legal model on the matter of balancing between the need of law enforcement agencies to overcome security measures installed on phones and computers of suspects and witnesses, and the owners' rights to privacy and the privilege against self-incrimination. The presented legal model describes the privilege against self-incrimination as a relative privilege, and wishes to balance between the conflicting rights and interests. The model does so using a few guidelines, which consist both from strict rules and from parameters that will be examined on a case-by-case basis.