LOS ANGELES
Daily Journal
www.dailyjournal.com
TUESDAY, FEBRUARY 23, 2016

PERSPECTIVE

Are your encryption keys safe?

By Bruce J. Heiman

The latest salvo in the current Crypto Wars is a federal judge's order last week that Apple provide the FBI with a way to disable the feature on an iPhone that erases the memory after 10 unsuccessful attempts to input a password. The FBI argues this is necessary in order for it to be able to "brute force" attack the iPhone's encrypted information (i.e., by randomly trying decryption codes until it finds the right one).

This case involves the phone used by accused terrorist Syed Rizwan Farook, who with his wife allegedly killed 14 people in San Bernardino last December. The facts are certainly sympathetic for the government: The suspect is dead (killed in a police shootout); the phone is owned by the county (which has consented); and it is an older model (potentially limiting collateral impact).

The FBI argues that it is not asking for a backdoor or even a private encryption key (that Apple does not have), but only for the opportunity to use its own tools and techniques to try to decrypt the information on the iPhone.

Apple correctly argues that the government is asking it to specifically design and provide software to weaken the security of its product — if not creating a backdoor then at least taking off the hinges on the front door! Apple reasons that such an order would set a dangerous precedent and weakening the security of all its phones. Apple will argue that the government is extending an ancient statute regarding assistance to law enforcement beyond the breaking point.

Beyond the current controversy, there also is another way that the government could threaten encryption in many cases — by asking a court to directly force a suspect to reveal his or her private encryption key. Would the government succeed?

The Fifth Amendment to the Constitution provides that "no person … shall be compelled in any criminal case to be a witness against himself." The Supreme Court has said that the Fifth Amendment "protects a person … against being incriminated by his own compelled testimonial communications." The amendment's lineage goes back centuries to the revolt against the use of torture forced confessions in the ecclesiastical courts and Star Chamber in England.

However, the Supreme Court has been clear that the Fifth Amendment only protects "testimonial" communications — those indicating a person's thoughts or knowledge. For that reason the Fifth Amendment does not protect a person's fingerprints, blood sample, handwriting or voice.

The court also has been clear that such a testimonial communication must be "compelled." The Fifth Amendment does not protect information a suspect had previously voluntarily written down and hidden that the government finds on its own.

The Supreme Court has not ruled on whether the Fifth Amendment would prevent the government from compelling someone to reveal his private encryption key because it would be testimonial communication. In three other cases, the Supreme Court distinguished between forcing a suspect to turn over a key to a strong box (permitted) versus compelling the suspect to reveal the combination to a wall safe (not) because doing so would convey the contents of the suspect's mind. Thus a private encryption key would seem to be protected.

Beyond the current controversy, there also is another way that the government could threaten encryption in many cases — by asking a court to directly force a suspect to reveal his or her private encryption key.

But two other Supreme Court decisions involving the forced disclosure of documents appear to circumvent this rationale and narrow the circumstances in which requiring a suspect to reveal unencrypted documents (rather than the actual private key) would be considered compelled to testimonial communication. In these cases, the court ruled that forcing a suspect to disclose plaintext documents is not prohibited if the government with "reasonable particularity" already knows the location, existence and authenticity of the material, because then any testimonial value derived from the suspect's act of production adds nothing to the government's case.

Indeed, in three cases since 2009, lower courts have directly applied these precedents to child pornography cases involving encrypted files on a computer. Rather than attempting to force the suspect to reveal the private encryption key, instead the government sought the production of plaintext files. The court decisions turn not on principle but on the facts of each case. In the two where the government could independently show that it knew of the location, existence and authenticity of the encrypted files, the suspect was compelled to produce unencrypted files. In the third, where the government only could suggest or speculate as to what encrypted information a hard drive might contain, the suspect's Fifth Amendment rights were upheld.

Judges often say that "hard cases make bad law." Terrorism and child pornography are certainly hard cases. But constitutional protections do not exist just for easy situations. Encryption will not protect information if companies can be forced to develop solutions to defeat security in their products or if those using encryption can be compelled to reveal their private key (or the functional equivalent by producing unencrypted information).

Bruce Heiman *is a partner in the global law firm K&L Gates where he is co-head of the Policy & Regulatory Practice Area. He helped lead the effort in the 1990s to ensure that Americans can use and export strong encryption.*

BRUCE HEIMAN
K&L Gates