Can Government Compel Your Client to Decrypt a Hard Drive?

By Christopher B. Hopkins

The May 2013 article regarding the limited Fourth Amendment protection afforded to travelers' phone and computer devices upon crossing the U.S. border lead local criminal defense counsel, Larry Buck, to pose this Fifth Amendment question: can the government compel a person to hand over the password to an encrypted hard drive?

Once again, novel technology and limited legal precedent suggest that this will be a case-by-case, court-by-court question likely destined for the U.S. Supreme Court. Recent case law, however, provides some guidance.

The Fifth Amendment holds that a natural person cannot be "compelled in any criminal case to be a witness against himself." To fall within the ambit of the Fifth Amendment, a person must show (1) compulsion, (2) testimonial communication or act, and (3) incrimination. This protection is extended to both incriminating evidence and content which would lead to incriminating evidence. Your client's decryption and production of content triggers constitutional protection because such acts are "testimonial" because they require a *mental* process (recalling the password) as opposed to a simple physical act, like producing a key, fingerprints, blood samples, or donning gloves.

Of course, there are exceptions to this "testimonial"-based protection. First, the government could extend both "use" and "derivative use" immunity, which likely dissolves constitutional protection. Second, if the "location, existence, and authenticity" of the purported evidence is already known by the government, then the content of the individual's mind (the password) is not used against him and there is no constitutional protection. This is known as the "foregone conclusion doctrine" – of note, four federal circuits require a "reasonable particularity" standard which has not been adopted by the Supreme Court. Third, albeit untested in the encryption context, there is a Required Records Exception to the Fifth Amendment when the requested documents are required to be kept by regulation. http://1.usa.gov/18Ec8s1

Problems arise when clients are chatty or careless in "jealously protecting" their constitutional rights. In *Boucher II*, border patrol searched the defendant's laptop for images/videos. Incriminating file names were found and the defendant made inculpatory statements about owning the laptop and downloading child pornography. When the laptop was shut down and later accessed, the Z: drive became password-protected via PGP software. The district court held that the "location" and "existence" of the subpoenaed files were known to the government. Moreover, Boucher's production of the password would not "authenticate" the Z: drive since he previously admitted possession of and had given access to the drive; finally, the government extended immunity for the act of production. Thus, Boucher had no Fifth Amendment rights.

In a similar 2012 case, defendant Fricosu's PGP-encrypted computer was seized. In a recorded phone call between Fricou and her incarcerated husband, she admitted being the owner / sole or primary user of the machine and that she could access the encrypted contents – thus, she had no Fifth Amendment protection (the government's lack of knowledge of the content of specific files was not a barrier). While a motion to reconsider was pending, defendant Fricosu's ex-husband handed over the password. http://bit.ly/ZHbt8R In short, evidence of the client's sole / primary control or ownership of the machine coupled with admitted knowledge of the password may overcome any constitutional rights.

In the case of *In Re: Grand Jury Subpoena* Dated March 25, 2011, Florida defendant John Doe declined to decrypted seven hard drives which were suspected of containing child pornography but were protected with TrueCrypt. The prosecution's forensic expert admitted that, although encrypted, it was possible that the drives contained no information. The Eleventh Circuit held that Doe's decryption and production would be testimonial because it was tantamount to Doe testifying about (1) his knowledge of the location and existence of potentially incriminating files; (2) his possession, control, and access; and (3) his ability to decrypt. Unlike *Boucher and Fricosu*, the government had no independent knowledge of existing files located on the drives and thus there was no "foregone conclusion" exception.

In April 2013, a District Court in Wisconsin denied a writ for decryption of nine previously seized computers. Defendant Feldman was the sole occupant of the residence and he had a degree in computer science, a job working as a software engineer, and even a software patent. The computer login screen showed one user: his first name. FBI examiners found eMule P2P software and log histories reflecting the distribution and storage of over 1,000 files with names indicative of child pornography. Unlike the Florida case, the prosecution was able to establish, as a "foregone conclusion," that the drives actually contained data, the probable existence of specific files, and even file names. But, even though Feldman was presumably able to decrypt the drives because of his computer expertise, he never admitted personal access and control. In what the court described as a "close call," the writ was denied. http://bit.ly/18Em4Sm but see http://1.usa.gov/18Erk8u

The mere presence of encrypted files should not imply illegal behavior any more than owning a locked safe. It appears that PGP and TrueCrypt provide reliable security. The weakness is on the human-side: admissions, disclosures, or poor password safekeeping. Looking ahead, if a defendant uses cloud storage, how will the government prove "location" much less possession, control, and access? Likewise, if a device is accessed via fingerprint, retina or facial scan, will future courts hold that to be "testimonial"?

Christopher B. Hopkins is a shareholder at Akerman Senterfitt. Send your cryptography or constitutional communiqués to Christopher.Hopkins@Akerman.com.