Does 5th Amendment Protect Computer Files From Decryption?

February 10, 2012

A U.S. District Court in Colorado recently considered whether the constitutional privilege against self-incrimination extends to the compelled production of decrypted computer files. It is beyond dispute that the government may not force a suspect to provide an encryption password if the password would provide a necessary link in the chain of evidence leading to the suspect's indictment. A much more difficult question is whether the government may force a suspect to use the password to produce decrypted computer files that contain incriminating evidence.

In *United States v. Fricosu,* Judge Robert Blackburn held that the government can indeed force a suspect to use an encryption password if the testimony implicit in the use (i.e., the act of producing decrypted files) is already known to the government and/or the implicit testimony will not incriminate the suspect. The court ordered the defendant to produce decrypted files from her laptop because the government already knew (based on uncompelled testimony) that the files were on a computer that belonged to her and for which she had the password. Judge Blackburn's decision is the most recent in a growing body of case law that attempts to thread the needle as to when the Fifth Amendment protects against the court-ordered production of computer data.

In 2010, FBI agents investigating a mortgage-fraud scheme executed a search warrant at the home of Ramona Fricosu. The agents seized six computers, one of which was a laptop that apparently belonged to Fricosu. When the agents turned it on, they were able to view the disk encryption screen, which identified the computer by Fricosu's first name. But without Fricosu's password, the agents could not access the encrypted files.

The next day, Fricosu's ex-husband called her from the correctional center. FBI agents recorded the conversation. Several times during the call, Fricosu and her ex-husband referred to the laptop as hers. Fricosu also mentioned that the laptop contained encrypted documents related to the mortgage-fraud scheme. Based on that conversation, the government applied for a warrant to search Fricosu's laptop, and the

court issued a writ requiring Fricosu to produce a decrypted version of her computer files.

The Fifth Amendment guarantees that "[n]o person . . . shall be compelled in any criminal case to be a witness against himself." Generally, a person may invoke the privilege based on a showing that the government seeks to compel that person to give testimony that would incriminate him or her. If any of these three criteria are not met (compulsion, testimony, and incrimination), Fifth Amendment protections will not obtain.

The *Fricosu* court distinguished between statements that are not compelled and those that are. For example, statements in files created voluntarily before the investigation was underway were statements the court had not compelled. Thus, they were not protected. By contrast, implicit statements Fricosu would necessarily make by producing the files — statements regarding the existence, location and authenticity of the computer files, for example — were statements that would be compelled and, therefore, subject to constitutional protections.

Courts recognize a Fifth Amendment exception for implicit statements regarding the existence, location and authenticity of computer files. When the government can demonstrate that it already knows the existence and location of items to be produced, this exception precludes an individual from avoiding production based on the Fifth Amendment. In *Fricosu,* the taped conversation between Fricosu and her ex-husband included their voluntary statements about the existence, location and authenticity of mortgage-fraud documents on the laptop. Court-ordered production of the computer files would compel Fricosu to affirm statements made during the call, but the affirmation would not tell the government anything it did not already know.

Second, the court distinguished between non-testimonial and testimonial evidence. The Fifth Amendment does not protect against the production of non-testimonial evidence. Thus, a person may be required to provide blood samples or handwriting exemplars, appear in a line-up, or speak aloud for voice identification. However, the Fifth Amendment does protect against the production of evidence that discloses the contents of a defendant's mind, including his or her beliefs and knowledge. Moreover, the amendment protects against any production that would compel a defendant to restate, repeat or affirm the truth of statements contained in documents sought. That is why, for example, a court may not require a criminal defendant to provide an encryption password. The act of producing the password requires the defendant to affirm that the

password is correct. Thus, the act of production is deemed to be testimonial and subject to constitutional protections.

The *Fricosu* court avoided Fifth Amendment issues by ordering the defendant to produce decrypted versions of her laptop files instead of the encryption password. The production of decrypted files was not testimonial because it did not convey any information in the defendant's mind that the government did not already have, nor did the act of production require the defendant to restate, repeat or affirm statements contained in her files. The Supreme Court has explained that a testimonial act is akin to revealing a combination or password to a wall safe because the combination or password is in the suspect's mind. A non-testimonial act is like surrendering the key to a strongbox. The act of surrendering gives no indication of the person's thoughts or knowledge.

Finally, the privilege against self-incrimination applies only if the compelled testimony incriminates the defendant. Testimony is deemed to be incriminating if it would furnish the government with a necessary link in the chain of evidence leading to the suspect's indictment. The government can (and very often does) preclude a showing of incrimination by offering use and derivative use immunity. This ensures that that the government will not use compelled testimony to further its investigation against the source of the testimony.

In *Fricosu,* the government sought to avoid any possible Fifth Amendment issues with the writ application by offering Fricosu use immunity. As the court noted, this offer protected Fricosu against self-incrimination by guaranteeing that it would not use her act of producing decrypted computer files against her, whether directly or indirectly.

Crime in the Suites is authored by the Ifrah Law Firm, a Washington DC-based law firm specializing in the defense of government investigations and litigation. Our client base spans many regulated industries, particularly e-business, e-commerce, government contracts, gaming and healthcare.

The commentary and cases included in this blog are contributed by Jeff Ifrah and firm associates Rachel Hirsch, Jeff Hamlin, Steven Eichorn and Sarah Coffey. These posts are edited by Jeff Ifrah and Jonathan Groner, the former managing editor of the Legal Times. We look forward to hearing your thoughts and comments!