Cullen | Dykman

Court Orders Defendant to Decrypt Her Laptop's Hard Drive

February 1, 2012

U.S. v. Fricosu, 10-CR-00509 (D. Colo. January 23, 2012)

On January 23, 2012, a District Court for the District of Colorado ruled that a defendant in a mortgage fraud case had to provide the government with an unencrypted version of a hard drive despite her Fifth Amendment claim of self-incrimination.

This case surrounds an encrypted computer that the defendant refused to decrypt or provide the password to. On May 14, 2010, the FBI executed a search warrant, where federal agents seized the defendant's laptop from her home. Investigators tried to see what was on the laptop by turning it on, but were unable due to the hard drive being encrypted by using a program called PGP Desktop. When the defendant then refused to voluntarily provide the investigators with the password to the program, the Government sought a writ pursuant to the All Writs Act, 28 U.S.C. § 1651, requiring the defendant to produce the unencrypted contents of the computer. She declined, asserting her privilege against self-incrimination under the Fifth Amendment.

Generally, the Fifth Amendment provides that "[n]o person . . . shall be compelled in any criminal case to be a witness against himself." Nevertheless, "the Fifth Amendment does not independently proscribe the compelled production of every sort of incriminating evidence." Instead, "the privilege protects a person only against being incriminated by his own compelled testimonial communications." In applying the Fifth Amendment to the context of the case at hand, the court relied on precedent from the Supreme Court's *United States v. Doe*, 465 U.S. 605 (1984) decision. That is, "[a]lthough the contents of a document may not be privileged, the act of producing the document may be." *Doe*, 465 U.S. at 612. Thus, production of a document often acknowledges that the (1) document exists, (2) that it is in the possession or control of the producer, and (3) that it is authentic.

The court held that in terms of authenticity of the laptop, the Government had met its burden to prove by a preponderance of the evidence that the laptop belongs to the defendant or she was its sole or primary user. The government provided the court with a recorded conversation between the defendant and her incarcerated ex-husband, which detailed that she owned such a laptop, the contents of which were only accessible by entry of password. Moreover, the laptop was found in the defendant's bedroom, and investigators found information on the computer that demonstrated that the laptop was owned by the defendant. (Namely, the fact that the WORKGROUP was the same as other laptops in the house and contained the defendant's name was the computer's account name.)

Ultimately, the court held that because providing an unencrypted copy of the hard drive would not serve to accomplish any of those three points, her Fifth Amendment rights were not implicated. As a result, the court granted the Government's application and ordered defendant to provide an unencrypted copy of the hard drive.

A special thanks to Sean Gajewski for helping with this post. Sean is a third-year law student at Hofstra University School of Law. You can reach him by email at srgajewski [at] gmail dot com. Bio: www.sgajewski.com.