LJN LAW JOURNAL NEWSLETTERS

Business Crimes Bulletin ®

An ALM Publication

Volume 19, Number 10 • June 2012

The Fragile Fifth Amendment

Compelling 'Decryption'

By Abraham J. Rein

Equipped with a search warrant or subpoena, and sometimes without either, the government may seize or compel an individual to turn over the contents of a computer or smartphone. But when those contents are encrypted (meaning they cannot be accessed without a password), as most are today, must the owner affirmatively facilitate the government's review by decrypting the data or supplying the password to do so? Few courts have weighed in, but two recent opinions demonstrate the fine factual distinctions that drive the analysis.

Background

Computers and related devices, like smartphones, can store massive amounts of private data. For many people, virtually all of their private information is stored and accessible digitally. Moreover, these devices serve as portals to an even greater accumulation of password-protected information housed in "the cloud." Due to this increased volume of digital storage, as well as reliance on such storage for increasingly sensitive information and increasing sophistication of those determined to get at that information, data privacy has become a paramount concern. The use of passwords (encryption) has correspondingly mushroomed.

When the government seeks to compel a target or criminal defendant to produce or enter a password in order to decrypt a device, the Fifth Amendment is implicated to the extent that: 1) the act is "testimonial"; and 2) the facts about which the act is testimonial might tend to incriminate the witness. An act is testimonial if it requires the witness to reveal the contents of her mind, and in so doing to communicate something — in this case the existence, possession, and authenticity of the data behind the encryption curtain. *See United States v. Hubbell*, 530 U.S. 27, 36 (2000) (testimonial nature of "act of production" in a non-digital context).

Two federal courts recently addressed the Fifth Amendment implications of compelled decryption of digital media, coming to different conclusions. In arriving at those outcomes, the opinions illustrate the delicate analytical line that can stand between an individual's password-protected data and a government investigator.

United States v. Fricosu

Fricosu concerned a formerly married couple, Scott Whatcott and Ramona Fricosu, who were indicted for bank fraud, wire fraud, money laundering and related offenses. *United States v. Fricosu*, 2012 U.S. Dist. LEXIS 11083 (D.Colo. Jan. 23, 2012). Pre-indictment, the FBI executed a search warrant at the defendants' home, and seized a number of computers. Later, they discovered that one of the seized computers was encrypted, meaning its contents could not be accessed without a password. At the time of the indictment, Whatcott was in prison for a separate offense. The prison telephone system recorded a conversation between Whatcott and Fricosu discussing an encrypted laptop and ostensibly making reference to data that the defendants apparently wanted to keep from the government.

The prosecution demanded that Fricosu provide them with the password to the computer. Her attorney refused, relying on two of a handful of cases that have addressed the question. In both, the courts ruled that the compelled production of a password violates the Fifth Amendment. *United States v. Kirschner*, 2010 U.S. Dist. LEXIS 30603 (E.D.Mich. Mar. 30, 2010) (subpoena requiring the target to verbally tell investigators the password to his encrypted computer violates the Fifth Amendment and is unenforceable); *United States v. Rogozin*, 2010 U.S. Dist. LEXIS 121162 (W.D.N.Y. Nov. 16, 2010) (un-*Mirandized* custodial questioning as to a computer's password is impermissible).

In response, the government sought a court order requiring the defendant simply to type her password into the computer, *unobserved*. The prosecution argued that: 1) this would not require any "testimony" from Fricosu, as she would not be divulging the password to a human being; 2) requiring her to "unlock" her computer without revealing the password was equivalent to requiring her to take the non-testimonial act of turning over the key to a strongbox; and therefore 3) the Fifth Amendment was not implicated. *Accord In re Grand Jury Subpoena* (*Boucher*), 2009 U.S. Dist. LEXIS 13006 (D.Vt. Feb. 19, 2009) (issuing such an order to a defendant who had already revealed to investigators that his computer contained child pornography).

Abraham Rein (arein@postschell.com) is an attorney in the Philadelphia office of Post & Schell, P.C., and a member of the firm's white collar defense and data integrity groups. He previously co-founded and managed a Web-development and consulting firm.

The government's motion generated a strong reaction from the digital rights community, not to mention Fricosu's defense lawyers. The San Francisco-based Electronic Frontier Foundation filed an *amicus curiae* brief in support of Fricosu, and technology publications followed the story. Fricosu's fundamental legal argument was that the very act of decrypting the laptop would be "testimonial" in nature — she would be required to disclose the "contents of her mind" and consequently reveal information, like the fact that she knew the password, implying that she owned or controlled the computer and its contents. As a result, she argued, the Fifth Amendment was implicated.

The district court granted the government's motion. The decision turned on its finding that, to the extent that Fricosu's decryption of the machine would be testimonial, it would go to facts that had already been established independently, adding nothing to the government's knowledge and thus not implicating the Fifth Amendment. *See Fisher v. United States*, 425 U.S. 391, 411 (1976) ("no constitutional rights are touched" when the act of production is testimonial only as to information that is a "foregone conclusion" and "adds little or nothing to the sum total of the Government's information"). The key "testimonial" fact — that Fricosu owned and controlled the laptop — was demonstrated to a preponderance of the evidence by her recorded statements on a prison telephone line, and the fact that the computer was found in her room, outside of its case, and apparently identified on a computer network as "RS. WORKGROUP.Ramona" (Fricosu's first name being Ramona). The Tenth Circuit declined to hear the issue, holding that Fricosu sought an improper interlocutory appeal. 2012 U.S. App. LEXIS 3561 (10th Cir. filed Feb. 21, 2012).

United States v. Doe

Just days after the Tenth Circuit turned away Ramona Fricosu's appeal, the Eleventh Circuit found that the Fifth Amendment barred the government from requiring an individual suspected of sharing explicit materials involving minors to decrypt certain seized hard drives. *United States v. Doe* (*In Re Grand Jury Subpoena Duces Tecum*), 2012 U.S. App. LEXIS 3894 (11th Cir. Feb. 23, 2012). In *Doe*, pursuant to a search warrant, the government seized a number of encrypted hard drives from Doe's hotel room. Unable to crack the encryption, the government served Doe with a grand jury subpoena that required him to decrypt the devices himself. Doe refused to comply and, appearing *pro se*, he — like Fricosu — argued that the subpoena sought to compel a testimonial act that might incriminate him in violation of the Fifth Amendment. The district court held Doe in civil contempt, and ordered him incarcerated.

The Eleventh Circuit reversed. Its decision turned on two holdings. First, the court found that forced decryption of the hard drives would constitute "testimony" for Fifth Amendment purposes, a question that the *Fricosu* court did not reach. Second, the *Doe* court rejected the government's argument that Doe's control of the data on the hard drives was a foregone conclusion and therefore the "testimony" required by the subpoena would add nothing to the government's knowledge. The court reached this crucial conclusion despite the fact that Doe's ownership of the hard drives was not in dispute. "Nothing in the record before us reveals that the Government knew whether any files exist or the location of those files on the hard drives," the court explained. "[W]hat's more, nothing in the record illustrates that the Government knew with reasonable particularity that Doe was even capable of accessing the encrypted portions of the drives."

Practice Pointer: The Crucial Factual Distinction

These cases appear to turn on whether pre-existing, independent evidence mooted the testimonial nature of compelled decryption. Remember that in *Fricosu*, other facts, and the inferences drawn from them, established the defendant's knowledge and control over the encrypted machine and its data; without those facts and inferences the decryption might have been found to be potentially incriminating and therefore protected by the Fifth Amendment. More specifically, the *Fricosu* court found that prison call tapes and the location and network identity of the encrypted machine established that the machine both: 1) contained data about which Fricosu was aware; and 2) was in her control. In *Doe*, by contrast, while it was not disputed that the hard drives at issue actually belonged to the witness-suspect, there was no evidence from which the court could determine that he controlled them or that they in fact contained any data. Thus, for Doe, decryption would be testimonial on these points.

Age-old Fifth Amendment jurisprudence developed in the context of ink-on-paper disputes now must be applied in the digital age. The line between *Fricosu* and *Doe* illustrates the kind of minute factual analysis that likely will drive outcomes. As a corollary, our ability to preserve the privacy of our most personal information becomes less certain than ever.

Epilogue

Two weeks after the district court decision in *Fricosu*, Ms. Fricosu's defense attorney suggested to the press that she may have forgotten her password. Then, just three days after the Tenth Circuit declined to hear her appeal, the entire issue — including whether she remembered the password — was mooted when federal authorities finally succeeded in decrypting the laptop without her help. With that, the possibility of a second circuit court opinion on this crucial issue ended — for now.

—❖—

Reprinted with permission from the June 2012 edition of the LAW JOURNAL NEWSLETTERS. © 2012 ALM Media Properties, LLC. All rights reserved. Further duplication without permission is prohibited. For information, contact 877.257.3382 or reprints@alm.com. #055081-06-12-09