Forced Data Decryption: Does It Violate the Fifth Amendment?

BY JODY GOODMAN

Does the Fifth Amendment protect an individual from being compelled to decrypt data on his or her computer? Sophisticated encryption software can effectively shield information from what would otherwise be lawful search and seizure by the government. Until software engineers can develop equally effective ways to decrypt data, recent cases suggest that a lot of illegal data may be out of law enforcement's reach.

The only federal appeals court decision that squarely addresses this issue is a 2012 child pornography case from the Eleventh Circuit. In *In re Grand Jury Subpoena Duces Tecum (Doe)*, 670 F.3d 1335 (11th Cir. 2012), FBI agents—with a valid search warrant—seized several laptop computers and external hard drives belonging to a John Doe who was under investigation for trafficking in child pornography. A forensic expert could not decrypt the data on the computers and hard drives because it was protected by a software program that made certain data inaccessible. In fact, a forensic examiner testified that he could not even tell if there *was* data residing on the laptops.

A grand jury issued a subpoena commanding Doe to decrypt and produce data from the laptop computers and hard drives, and Doe informed the US attorney that he refused to comply because doing so would violate his Fifth Amendment privilege against self-incrimination. The US attorney sought and obtained an order from the district court (Judge Lacey A. Collier in the Northern District of Florida) granting Doe immunity for production of the data. But the immunity was limited to the act of producing the data; in other words, the government could make "derivative use" of the data in a criminal prosecution of Doe. Because he was not granted full immunity, and the government would have been able to use the decrypted material as evidence against Doe (assuming the computers did indeed contain child pornography), Doe again refused to decrypt and turn over the data. Judge Collier found him in contempt and had him jailed, but the Eleventh Circuit reversed the ruling.

The Eleventh Circuit's decision is a lot more rational than the trial court's. The appellate court held that the act of decryption and production would constitute testimony, which would implicate the Fifth Amendment. The Eleventh Circuit also held that the trial judge "erred in limiting [Doe's] immunity . . . to the Government's use of his act of decryption and production, but allowing the Government derivative use of the evidence such act disclosed." (*Doe*, 670 F.3d at 1341.)

Was compelling Doe to hand over the decrypted data forcing him to "testify" against himself? And is there something special about digital data in this context? The answers are "yes" and "no"—or maybe "not really."

Consider a different case: Ramona Fricosu was under investigation for her alleged involvement in a mortgage scam. Federal agents got a search warrant, searched Fricosu's home, and seized three laptop computers. One of the computers was encrypted and two were not. An agent who turned on the encrypted computer saw the disk encryption screen, which identified the computer as "RS.WORKGROUP. Ramona." Meanwhile, Fricosu went to visit her husband, who was in jail at the time. In a recorded jailhouse conversation, they discussed whether there was "anything on [the] computer to protect it," and Fricosu said there was. "I don't know if they can get to it," she said, adding "my lawyer said I'm not obligated by law to give them any passwords or anything they need to figure things out for themselves." (United States v. Fricosu, 841 F. Supp. 2d 1232, 1235 (D. Colo. 2012).) Based on that conversation, the government sought a writ requiring Fricosu to decrypt and produce the laptop's contents. Fricosu refused, asserting her Fifth Amendment rights. The judge (Colorado District Court Judge Robert Blackburn) granted the writ, noting that because the government knew about the existence of the files on the computer, and knew their location, the act of decrypting and producing the files was not "testimonial." Compelling production therefore didn't run afoul of the Fifth Amendment.

The difference between *Doe* and *Fricosu* is government knowledge about the encrypted data. If the government doesn't know what type of data is in the computer, an individual's act of decrypting and producing it constitutes "testimony" under Fifth Amendment jurisprudence. The *Doe* court explained:

> [A]n act of production can be testimonial when that act conveys some explicit or implicit statement of fact that certain materials exist,

JODY GOODMAN *is counsel in the White Collar and Regulatory Enforcement Group at Crowell & Moring LLP, in Washington, D.C. You may contact her at jgoodman@crowell.com.*

Published in *Criminal Justice* Volume 27, Number 4, Winter 2013.

> are in the subpoenaed individual's possession or control, or are authentic. The touchstone of whether an act of production is testimonial is whether the government compels the individual to use "the contents of his own mind" to explicitly or implicitly communicate some statement of fact.

(*Doe*, 670 F.3d at 1345 (citation omitted).)

So in *Doe*, where government agents didn't know what was on the computer, the court could not compel Doe to use "the contents of his own mind" to decrypt the data; in *Fricosu*, on the other hand, Fricosu's act of decryption would provide the government with the data on the computer, but it would not provide the information that the files existed in the first place. The government already knew that.

Although there are only a handful of cases addressing this issue in a digital context, the encrypted data cases do not break new legal ground. In fact, they follow a century-long line of Fifth Amendment cases addressing whether conduct is "testimonial." The Supreme Court ruled in 1911 that when a criminal defendant is required to surrender records deposited with a receiver, "no constitutional rights are touched. The question is not of testimony, but of surrender." (*In re* Harris, 221 U.S. 274, 279 (1911); *see also* Fisher v. United States, 425 U.S. 391, 411 (1976).) The cases (just like *Fricosu*) essentially hinge on the government's knowledge and whether discovery of the compelled information was "a foregone conclusion." (*See Harris*, 221 U.S. at 279.) So, in another child pornography case, the owner of a laptop could *not* be forced to provide the password for his encrypted data, because doing so would be "testimonial." But because a border agent had seen that there were encrypted files with suspicious names on the computer (before the files became inaccessible when the computer was turned off), a grand jury could compel the defendant to produce an unencrypted copy of the data; that was *not* testimonial. (*See In re* Boucher, No. 2:06-mj-91, 2009 WL 424718 (D. Vt. Feb. 19, 2009).)

Though this line of reasoning is well established, it can also be seen as judicial hairsplitting, especially in a digital context. Is there really a meaningful distinction between being compelled to provide a password (testimonial) with being compelled to produce encrypted files (not testimonial)? What if the case involves physical objects instead of computer data? Suppose the FBI got a search warrant to search a home, including a safe inside the home. Presumably, agents would have the right to crack the lock or blow the safe open. But if the safe was so structurally sound that it was impossible, the owner couldn't be forced to provide the combination. That would be using "the contents of his mind" to open the safe, and hence would be testimonial. But could he or she be compelled to produce the contents of the safe? Under the *Doe* reasoning, the answer is "no," as long as the government does not know and cannot tell what is in the safe. If the owner had been heard discussing the stolen cash that he or she had placed in the safe, the rulings in *Fricosu* and *Boucher* would support compelling the owner to produce the money.

Based on the courts' reasoning in *Fricosu*, *Boucher*, and *Doe*, it's clear that encryption software is valuable to anyone, not just purveyors of child pornography. Think of all the people commuting and traveling with sensitive (or illegal) data on their laptops. As long as the government doesn't have a means of knowing that potentially incriminating files exist, and it is not a foregone conclusion that the government would find that out, effective encryption software is—at least for now—the ultimate protection. ■