Andy Greenberg, Forbes Staff
Covering the worlds of data security, privacy and hacker culture.
Follow (667)

TECH | 2/24/2012 @ 12:49PM | 6,634 views

Two Cases' Lessons: If Cops Don't Know What You Encrypted, They Can't Make You Decrypt It

The last 24 hours have produced two opposite rulings about whether suspects in legal cases have to cough up the password to potentially incriminating data that they've encrypted on a hard drive. The two cases add up to a lesson: If the cops don't know what they don't know, your secrets are safe. But if they know what they're looking for, the world's strongest cipher isn't going to stop them from getting it from a suspect.

On Thursday, the 11th circuit court of appeals ruled in the child pornography case of an unnamed man called John Doe that he wasn't legally required to give up the password to an encrypted hard drive that might contain incriminating information. (The PDF of the ruling is here.) Forcing him to decrypt his data, the judge in the case argued, would violate Doe's fifth amendment rights to not offer any testimony that would incriminate himself. But the very same day, a federal appeals court rejected the appeal of a suspect for mortgage fraud named Ramona Fricosu, demanding that she give up the password to her encrypted laptop despite her plea that the computer–just like John Doe's–contained incriminating data.

Those two cases may seem on the surface like mere judicial confusion and contradiction. But the real difference between them, says Electronic Frontier Foundation attorney Hanni Fakhoury, is what investigators expected to find on those scrambled hard drives. Fakhoury cautions that the details of every case are different, but that broadly speaking, "if the government knows what they're going to find, they have no problem," he says. "If they don't, they can't make you decrypt anything."

In the case of John Doe, the suspect came to law enforcement's attention when the IP address of his computer and his name in a hotel's registry were tied to pornographic pictures of underage girls posted to YouTube. But when authorities seized his hard drives, parts of them were encrypted with the program TrueCrypt. Investigators were unable to decrypt them and–just as importantly–couldn't begin to guess what might be stored in those encrypted partitions.

That ambiguity allowed Doe to plead the fifth, according to the court's ruling. The court's opinion makes clear that if investigators had known what they were looking for, Doe would have had to decrypt that file. That situation would be a situation the ruling calls a "foregone conclusion," when the court knows that a piece of evidence is potentially incriminating, but the holder of that evidence won't make it available. Without that knowledge, however, the password to Doe's files is merely like any kind of testimony, and falls under Doe's fifth amendment protections.

"We find no support in the record for the conclusion that the Government, at the time it sought to compel production, knew to any degree of particularity what, if anything, was hidden behind the encrypted wall." it reads. "The Fifth Amendment protects Doe's refusal to decrypt and produce the contents of the media devices because the act of decryption and production would be testimonial, and because the Government cannot show that the 'foregone conclusion' doctrine applies."

Perhaps the most interesting line in the ruling deals with the question of whether the mere presence of encryption means that Doe must have had something specific he was trying to hide. The court rules it doesn't. "We are not persuaded by the suggestion that simply because the [hard drives] were encrypted necessarily means that Doe was trying to hide something," it reads. "Just as a vault is capable of storing mountains of incriminating documents, that alone does not mean that it contains incriminating documents, or anything at all."

In the Fricosu case, on the other hand, the authorities had a recording of the suspect talking to her co-defendant in which she mentions an incriminating file on her laptop. That's enough, Fakhoury says, for the court to compel her to turn over the password. Given that she had already incriminated herself in the recorded conversation, refusing to decrypt the hard drive just becomes a case of withholding evidence for which she can be held in contempt.

Fakhoury compares the situation to a 2008 case in Vermont where a child pornography suspect, Sebastien Boucher, had a file on his computer clearly labelled as graphic child pornography–I'll spare you the exact, disgusting phrase. In that case, the fact that the file was encrypted didn't help him–the mere title of the file was enough to bypass his fifth amendment argument against handing over the password.

Fricosu's case isn't nearly as black and white. But the nature of the encrypted contents is clear enough that the court has ruled the fifth amendment doesn't help her.

So what's the lesson for those that value their hard drive's privacy, even against legal intrusion? Fakhoury makes clear that the EFF isn't trying to help child pornographers avoid prosecution. But he offers two pieces of advice for others who hope to avoid handing over their passwords to the cops. "Encrypt everything," he says. "And don't label your files 'child porn.'"