Colorado woman must turn over computer hard drive

February 21 2012, By P. SOLOMON BANDA , Associated Press

(AP) -- Readily available, easy-to-use software can encrypt a computer hard drive so thoroughly it would take years for a hacker to break in. But that seems to be no impediment for government prosecutors, who have obtained an order compelling the disclosure of a computer's contents in one Colorado case.

It's a case that raises questions about whether requiring someone to unlock a computer's protected files amounts to a violation of the Fifth Amendment's protection against self-incrimination.

The judge's order establishes a "very dangerous precedent that a person may be forced to assist in her prosecution in a way the law has not seen ever before," said Phillip DuBois, who represents a woman charged in a mortgage and real estate fraud case.

On Tuesday, the 10th U.S. Circuit Court of Appeals refused to get involved, saying Ramona Fricosu's criminal case must first be resolved in District Court before her attorney can appeal.

Fricosu, of Colorado Springs, now has until Monday to turn over an unencrypted version of the hard drive of a laptop.

Federal prosecutors argue that not allowing the government access to encrypted computers would make it impossible to prosecute crimes such as terrorism, child exploitation and drug trafficking. The U.S. attorney's office declined to comment on Tuesday's appeals court decision.

The San Francisco-based Electronic Freedom Foundation has opposed the government's actions in the case because it believes easy-to-use encryption software should be used by everybody to prevent computer crimes and fraud, said Hanni Meena Fakhoury, an attorney for the foundation. The case could render those privacy protections useless, he said.

"The government is flipping that on its head and saying encryption is only good for criminals to hide what they're doing," Fakhoury said. "It's very decoder-ring-ish. But this is not some sleuth criminal tool."

A judge last month sidestepped the issue of ordering Fricosu to turn over her password, and instead ordered her to turn over an unencrypted version of the hard drive. Prosecutors had argued the password was like gaining a key to a lock box and other instances where a defendant signs documents to allow investigators to access overseas accounts.

U.S. District Judge Robert E. Blackburn noted that the contents of one's mind is off limits, but he ordered Fricosu to turn over the data, citing a Vermont case that stemmed from a 2006 border crossing search in which a man was later ordered to do the same.

The courts in that case noted that an Immigration and Customs Enforcement agent had found child pornography on the computer but couldn't access it later because of encryption, and turning over the unencrypted hard drive added nothing to the evidence the government already had.

Blackburn also noted there were only a few cases on which to base his ruling.

In Fricosu's case, "the government has no idea what's on that computer," DuBois said. That element makes it different from other cases, he said.

In a procedure agreed upon by DuBois and federal prosecutors, federal agents would meet Fricosu at a designated place with the laptop, which was seized during a search warrant. Then, the government will either look away or go to another room while Fricosu enters a password on her laptop and hands it back to agents so the hard drive can be copied.

But there's a twist.

"It is possible that Ms. Fricosu has no ability to decrypt the computer, because she probably did not set up the encryption on that computer and may not know or remember the password or passphrase," DuBois said in a statement Tuesday.

Fricosu and her husband, Scott Whatcott, are accused of targeting distressed homeowners in the Colorado Springs area. Prosecutors allege the two promised to pay off homeowners' mortgages but then filed fraudulent documents in court to obtain title and sell the homes without paying the outstanding mortgage.

DuBois described Fricosu as an immigrant from Romania who has two sons, no technical expertise in computers and whose computer was encrypted with what he believed was software available on the Internet or at stores.

Encrypted computers are no longer for the technological savvy. With a few clicks of the mouse, readily available 256-bit and 512-bit encryption software makes computer hard drives almost impossible to break into, even for hackers.

"Conceptually, it is possible to break encryption," but it could take years, said Jay Bavisi of the Albuquerque-based EC-Council, a so-called "white hat" and ethical hacker group that tests network and computer security. "It can be a time consuming and resource draining exercise in an already

stressed environment."

In one of the few examples of a similar case, a sheriff's detective under suspicion for improper use of a law enforcement database told investigators in King County, Wash., in 2004 that he simply forgot the password to the encrypted portion of his computer hard drive. The detective retired and the computer's hard drive was placed into storage.

"We apparently did not ever crack the code to get in," sheriff's spokeswoman Cindi West said.