

For this week's discussion, encryption and its effectiveness in protecting a user's information and speech from a legal perspective is discussed. Encryption is the process of obscuring information so that only authorized parties can view the unencrypted information, while third parties have no way to decipher the encrypted information. Encryption of stored data as it pertains to computer and Internet law is a double edged sword – on one hand, it helps to protect one's ~~personal~~ ^{personal?} information from third parties like the government, but on the other hand, it may limit the investigation and prosecution of a criminal. It is important to note that encryption is an effective means of protecting information for an extended amount of time, but that it does not protect the information forever. Given a machine with computing capacity that far exceeds our capabilities of today, the encryption standards that are regularly used now could easily be broken and the information retrieved. ✓

In ~~the particular court case of~~ *United States of America vs. John Doe*, the Court of Appeals for the Eleventh Circuit held that a defendant should not be required to give up the password protecting contents that were unknown to the prosecution. The anonymous defendant refused and cited his Fifth Amendment right to not incriminate himself to provide the password to his encrypted data in which the government believed, but had no proof, that child pornography might be contained within. Just as a locked safe may contain incriminating evidence, it does not mean that it does and the Court cannot force a defendant to provide its key, unless the information contents in question are known. 2012

In another case of *United States of America vs. Ramona Fricosu*, the defendant was forced by the U.S. District Court to give up the password protecting the contents of encrypted data in her possession. The distinction in this case from that of John Doe's is that Ms. Fricosu

had incriminated herself via a recorded telephone call by discussing to her co-defendant about an encrypted file on her computer linking her to the offense. Because it was known that a particular file exists that was of interest to the proceedings, the Court ordered that the defendant relinquish the password and allow the encrypted data to be searched, with penalties of being held in contempt of court if such information was not produced, and if the prosecution had not had the recording of her discussion, her case may have been ruled the same as John Doe's.

I agree with the outcomes of both of these cases, and they are important because they define when it is permissible for the government to force a citizen to decrypt data from a personal store. As long as the government cannot prove some of the contents of an encrypted file or file container, it is not required for a citizen to give up that information; however, if there is undeniable evidence that an encrypted file or file container contains information pertinent to the prosecution, it is permissible for the Court to order the evidence to be provided. Even without John Doe's consent to relinquish the password, the information can conceivably be saved until a machine of enough computational capacity could decrypt the information in a timely manner, similarly to how advances in DNA analysis have been applied to investigators' abilities to solve cases and convict criminals that might have otherwise gotten away, though until the technology becomes readily available, a case may need to carry on without it, less the government interfere with the person's Sixth Amendment right to a fair and speedy trial.

40 lines

probable cause?

98