

Case Name and Citation:

United States v Apple MacPro Computer, 851 F.3d 238 (3d Cir. 2017)

Facts:

An investigation into John Doe's residence on the claims of Doe's access to child pornography resulted in an Apple iPhone 5S and an Apple Mac Pro Computer with two attached Western Digital External Hard Drives recovered. These devices were found to be encrypted, and the defendant refused to decrypt the Apple Mac Pro computer and the additional hard drives. Forensic examiners were able to decrypt the Apple Mac Pro Computer successfully, which yielded evidence supporting the claim that the defendant was accessing child pornography and the terms associated with it. It was also found that Doe downloaded thousands of files that were stored on the encrypted external hard drives. Doe's sister was interviewed and provided information that hundreds of images were stored on the external hard drives. Doe provided access to the iPhone 6 Plus but not to a fourth encrypted application. According to the All Writs Act, a judge issued an order that required Doe to produce his devices in entirely unencrypted states. Doe did not comply and issued a motion claiming that the act of decrypting his devices would violate his Fifth Amendment privilege against self-incrimination; the judge denied this motion because the Government had the devices in its possession and knew that their contents included child pornography. Doe later appeared with the Apple iPhone 6 Plus and produced the passwords to the secret application, which contained further evidence; Doe then claimed he did not remember the passwords to the hard drives. The judge ordered Doe to appear before the District Court to explain why he should not be held in civil contempt for failing to decrypt the hard drives when ordered.

Issue:

Did the defendant's decryption and production of his hard drives constitute "testimony" and violate his rights against self-incrimination under the Fifth Amendment?

Ruling:

The court ruled that the defendant's decryption and production of his hard drives did not constitute "testimony" under the Fifth Amendment. The court held in a unanimous vote that the

Assignment 10: Brief a Case

Gunnar Yonker

act of decryption and production was a physical act rather than a testimonial one and, therefore, not protected by the Fifth Amendment. The defendant was found to be in civil contempt for refusing to comply with the Decryption Order.

Reasons:

In this case, the Third Circuit Court of Appeals decided that the defendant's decrypting and producing his devices did not constitute "testimony" under the Fifth Amendment. The court reasoned that decryption was a physical act, not a testimonial one. The court then further argued that the Government had not compelled the defendant to reveal any "mental processes" or disclose any information that he did not already possess. The court also argued that the act of producing the unencrypted devices was not testimonial either because the Government had already established the existence and authenticity of the evidence contained on the devices through other means. Thus, the act of production and decryption did not provide any new information to the Government's case. The court also held that even if the act of decryption and production could be regarded as testimonial, the defendant had waived his Fifth Amendment rights by creating and using the encrypted devices for illegal purposes. The court referred to the "foregone conclusion" doctrine, which says that the Government can force a suspect to produce evidence if it already knows with "reasonable particularity" the evidence's existence, location, and authenticity and that the evidence itself is not incriminating on its own. These reasons led the court to affirm the District Court's denial of the defendant to suppress the evidence obtained from the unencrypted computer and uphold his conviction and sentence.

Opinion:

I agree with the Third Circuit Court of Appeals' decision in this case because the court had, but also for a few additional reasons. One of the main reasons I agree with the court is through their use of the "foregone conclusion" doctrine that finds that the defendant waived his Fifth Amendment rights through the creation and encryption of these devices for illegal purposes. I believe that the Government had sufficient evidence to compel the production of the unencrypted devices in this case because the existence and authenticity of the evidence were already established through other means, such as the statement from Doe's sister and the information gathered by the forensic examiners. The "foregone conclusion" doctrine, along with this

Assignment 10: Brief a Case

Gunnar Yonker

evidence, is what allowed for the compelled production and decryption of the devices by the defendant because the Government already knows with reasonable particularity that the evidence exists. I think that overall, the Government did a comprehensive job of weighing the defendant's Fifth Amendment rights against the Government's interest in obtaining the evidence. Ultimately, this reasoning and ruling resulted in the act of decryption and production of the devices, not violating the defendant's constitutional rights. The court did an excellent job of protecting the rights of the defendant, as well as delivering the proper ruling. This is a circumstance where I think there is a guidebook way to rule on these issues until the specifics of the investigation and case are delved into.