

Exigent Circumstances When Handling Electronics

Description

In *United States v. Meyer*, the Eighth Circuit Court of Appeals considers a case that examines the application of exigent circumstances when handling electronics. This case delves into the rules and exceptions that apply when law enforcement officers seek to enter a home and search for evidence without first obtaining a warrant. Specifically, the court evaluates whether officers may enter a home without a warrant when there is probable cause to believe that evidence of a crime exists on the premises and the officers have reason to believe that the evidence may be destroyed if they wait for a warrant. The case also explores the circumstances in which the officers themselves may create exigent circumstances that would not justify a warrantless search.

When determining whether exigent circumstances exist, officers should consider several factors, as established by cases such as *United States v. Reed*. These factors include: (1) the degree of urgency involved, (2) the amount of time necessary to obtain a warrant, (3) whether the evidence is about to be removed or destroyed, (4) the possibility of danger at the site, (5) whether those in possession of the contraband are aware that the police are on their trail, and (6) the ease with which the contraband can be destroyed.

FACTS

After the government discovered financial ties between William Meyer and individuals in the Philippines who were livestreaming sex acts involving children, two federal agents visited Meyer at his home. After the agents knocked on his door, Meyer insisted on speaking with them outside, so the agents spoke with Meyer in their car. During their conversation, Meyer revealed a number of facts that stirred the agents' suspicion, including that Meyer had personal and financial ties to the individuals involved in the abuse. When Meyer admitted that he used a computer and cell phone to contact them, the agents asked Meyer if he would be willing to turn those devices over to them for an examination. Meyer told the agents that he was willing to turn them over later, after he had a chance to "check [his] email and stuff." Once the agents expressed concern that a delay would give him a chance to erase what was on them, Meyer still refused to consent, claiming that his house was "a mess" and "not . . . in any condition to entertain people." Then, after the agents mentioned the possibility of getting a warrant, Meyer suggested that the agents "come back later." One of the agents told Meyer that if they obtained a warrant, they would not tell him beforehand when they were coming to execute it. A short time later, Meyer went back inside his house.

Concerned that Meyer would destroy evidence if they waited any longer, one of the agents called a prosecutor for advice on whether "an exigent circumstance existed." When he was told that it did, the agents again knocked on Meyer's door, searched his home for electronic devices, and seized two computers, a cellphone, and a hard drive. Afterward the agents obtained a warrant to search the devices seized from Meyer's home. The search revealed child pornography videos and evidence that Meyer had sent money in exchange for the videos.

After the district court denied Meyer's motion to suppress the evidence discovered on his devices, he plead guilty to one count of sexual exploitation of children. On appeal, Meyer claimed that the agents' warrantless entry into his home violated the Fourth Amendment.

EIGHTH CIRCUIT COURT OPINION

In this case, the Eighth Circuit Court of Appeals held that exigent circumstances existed that permitted the agents to enter Meyer's house without a warrant and seize his electronic devices. First, by the time the agents decided to enter Meyer's house they had probable cause to believe that he was involved in criminal activity. Specifically, the agents knew that Meyers: (1) had ties to the individuals who were livestreaming sexual abuse of children; (2) had stayed with these individuals when he visited the Philippines; (3) had paid thousands to them and one of the minor victims; and (4) did not tell his wife about some of the money he sent, despite claiming that the payments were tied to his humanitarian work.

Second, the court held that the agents had probable cause to believe that there would be incriminating evidence on Meyer's devices, as Meyer admitted to the agents that he used a computer and cellphone to communicate with the abusers and had stayed in regular contact with them. The agents also knew that his Skype username was "prettyvirginfilipino" and that the profile he used was a variant of the first name of one of the minor victims. After Meyers admitted that these devices were in his home, the court concluded that there was a fair probability that the agents would find "evidence of a crime" inside his home.

Third, the court held that it was reasonable for the agents to believe that Meyer would destroy the evidence on his devices after he went back inside his home. Meyer told the agents they could examine his devices after he "checked his email and stuff." When the agents suggested that they accompany Meyer inside and look at the devices together, Meyer shifted his attention to the tidiness of his house and told the agents he would need "a few minutes to clean up first." The court concluded that Meyer's insistence that he have an opportunity to be alone with his devices gave the agents reason to believe that he was hiding something. Knowing that data can be deleted "at the touch of a button," the court found that it was reasonable for the agents to enter Meyer's home without a warrant and seize his devices. Finally, the court held that the agents did not create the exigency by "engaging or threatening to engage in conduct that violates the Fourth Amendment." By the time the agents mentioned their concern that Meyer might destroy evidence, he had already made a number of suspicious comments, including offering multiple excuses for his refusal to cooperate. Consequently, the court held that officers could not have manufactured or created an exigency that already existed.

TAKEAWAYS

Exigent circumstances can arise even more in computer cases before the evidence has been properly secured because electronic data is fundamentally perishable. Computer data can be effectively put out of law enforcement's reach with widely available and powerful encryption programs that can be triggered with just a few keystrokes. In addition, computer commands can destroy data in a matter of seconds, as can moisture, high temperature, physical mutilation, or magnetic fields created, for example, by passing a strong magnet over a disk. If I know all the ways in which the evidence can be destroyed, you can be sure that a criminal does as well. I do appreciate that the agents called a prosecutor to ask if exigent circumstances did, in fact, exist. It never hurts to double-check.

United States v. Meyer, 2021 U.S. App. LEXIS 35593 (8th Cir. IA Dec. 2, 2021)

Date Created

03/14/2023