# Seizing computers and obtaining electronic evidence in criminal investigations

Law

Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations

Given the nature of digital evidence, officers who execute any search warrant for computer devices can turn the search into a ‘ general warrant’. Is this a valid concern?

A search is considered as a violation of a person’s privacy. The law under the Fourth Amendment does not allow law enforcers to access and view information in a personal computer, which is considered personal and private. Law enforcers, therefore, have to obtain search warrants in order to search an individual’s computer or devices controlled by the individual. There have also been concerns over warrantless searches conducted by law enforcers, but in search cases, the court has to certify that the search was necessary. However, it is a valid concern if the officers turn a computer device search into general search. This is because the court issues warrant for a computer search separately from a general warrant. Therefore, it is illegal for law officers to turn the search into general warrant unless they can prove that there was probable cause to warrant the search.

Should judges require law enforcement to forego the plain view exception to the warrant requirement when they are executing search warrants on computer devices?

The plain view exception indicates that the search warrant holders should seize evidence in plain view. No warrant is needed to seize evidence that is in view. However, in computer devices this is not applicable. Courts have generally held that law enforcers are entitled to search the entire computer device for evidence in the case of a crime. The law enforcers are encouraged

to look for information in the entire device by reviewing every file in the computer. This is majorly because of the ease with which files in a computer can be camouflaged or hidden in different kinds of names and extensions. Assume that the courts in your jurisdiction are considering requiring a judicially approved ‘ search protocol’ before a judge will sign a search warrant authorizing a search of any computer device. Do you support or refute this idea?

Law enforcers are allowed to carry out a full search warrant if they arrest an individual as they pursue a lawful arrest. Computers can be used to manipulate evidence and make it difficult for authorities to obtain the required information to prosecute or find evidence. Even though, law enforcers are allowed to carry out a search warrant, if the courts deem it fit to curtail their mandate they would be forced to oblige, but at the risk of losing vital evidence (Marshall & Baillie 5). If courts restrict searches of computer devices up to the point when a judicial approval is received, suspects can manipulate their devices and do away with what can be incriminating. By the time the judicial approval is acquired, the criminals shall have absolved themselves from any wrongdoing in connection to what they were being accused of. I, therefore, refute this idea. However, if the judicial approval is needed before a search warrant, then the law enforcers should be allowed to have the devices in their possession to eliminate the risk of the accused tampering with the evidence. That notwithstanding law enforcers should be allowed to conduct searches on computer devices when they see any suspicious activities in the community.

Work cited

Marshall H. Jarrett and Baillie W. Michael. Seizing Computers and Obtaining Electronic

Evidence in Criminal Investigations: Computer Crime and Intellectual

Property Section Criminal Division (Department of Justice). 2009. Online.