# Law of digital evidence

Law

Law of digital evidence General warrant Searching a suspect’s private belonging is illegal under the Fourth Amendment. Such arbitrary searches are gross violation of privacy thus basic human rights. Computers constitute private property that law enforcers can never search arbitrarily without approval from a judge. Law enforcers such as the police must always obtain court orders, also known as search warrants in order to search private belonging key among which are computers. Search warranties must indicate the type of searches they approve (Marshall & Baillie 5). Computer searches vary from general searches a fact that makes turning a computer search warrant into a general search. In case they do so, they must always prove a probable cause for such actions.

Plain view exception

Law enforcers should always seize evidence in plain view a feature that remains impossible in computer searches given the soft copy nature of such files. The plain view exception thus exempts computer searches from such conditions. However, law enforcers should always carry out an exhaustive search of the computer thus ensuring that they search every file in the computer and avail their contents whenever required.

Search protocol

I refute the idea of a observing a search protocol which requires the approval of a court of law before carrying out a search. Criminals can easily delete and manipulate any incriminating evidence in their computers thus making it difficult for the law enforcers to prove their guilt. As such, the law should permit law enforcers to confiscate computers at the time of arrest as they await search warrants. This way, they safeguard the evidence in the computers by making it difficult for the suspect to tamper with the contents

of the computer.

Work cited

Marshall, Casey & Baillie, Eoghan. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Burlington: Elsevier Science, 2011. Internet resource.