**Search and Seizure from a Digital Perspective: A reflection on Kerr's Harvard Law Review Article**

After reading Kerr's "Searches and Seizure in the Digital World", I realized that on a larger scale, applying the current law system to computer crimes is a complex practice. The current law system of the United States did not take into account the "digital world" and laws need to be modified, edited, or amended to fit the requirements of the cyber world. As for the Fourth and Fifth amendments, some ideas came to mind about how they did not reflect on the digital world.

Primarily, it is important to note that the Fourth Amendment was written on the basis of retrieving and entering physical evidence. As Kerr explains, things do change when looking for digital evidence. Some important questions arose after reading more about the Fourth Amendment, such as when is a digital device searched? When is evidence seized on a digital device? Furthermore, how can we define a reasonable search and seizure in the context of the digital world?

It was apparent through the reading that in a physical search and seizure, the place, person or thing that is going to be seized is clearly described. In addition, a search warrant needs to specifically identify the place as coherently as possible, with limitations imposed within the search warrant on what could and could not be searched. This applies well to the physical world of search and seizure, but how well does this apply to digital devices?

This does not apply very well in the realm of digital devices. When looking at a computer system for instance, one is not looking at a physical house, with a certain number of rooms, furniture etc. A computer can have millions and millions of files and folders. Also, when looking at files and folders, one is not looking directly at the bits of ones and zeros or the magnetic part of a hard drive. In fact, looking at digital evidence

encompasses looking at a computer screen displaying the same information available to the average computer user.

As a result of the increase of hard drive capacities and computer usage over the last decade, a large amount of information is usually available on digital devices. So what can potentially be the limitation on a search warrant in the digital situation? Can a search warrant be given to a forensic professional to search through the whole hard drive? How should the law handle this limitation? Somehow, the amount of evidence needs to be identified in a specific search warrant, outlining the limitations of the warrant in order to help fix this problem.

Another important point stressed by Kerr is the creation of a forensic copy. Nowhere in the Fourth Amendment does it mention that evidence should be “copied”. I believe that this issue needs to be resolved and the law needs to fully understand the importance of creating a forensic copy. How should the incriminated individuals feel, knowing that their personal information is being copied? One can assume the violation of privacy laws when faced with this situation.

As for the Fifth Amendment, I find the issue of the double-jeopardy provision sphere to be interesting from a digital forensics perspective. The double-jeopardy provision explains that one can not be put back on trial, even if new evidence was discovered. This is important to mention, especially in the case of digital evidence. It is already difficult to acquire a sufficient amount of evidence, since digital forensic investigators do not know what they are looking for most of the time. With that said, digital forensic investigators need to make sure they are acquiring a sufficient amount of evidence before the end of the trial, so that the case is not closed before more evidence is found. However, this is somewhat dictated by the Fourth Amendment since it should impose where and what evidence can be seized and searched in the first place.

I feel that the world is heading towards a digital crime age. Crimes are continuously growing in the cyber world, and as I mentioned before in some of my interviews, it is very important for cyber forensic professionals to collaborate with governmental agencies and law officials so that they can both be in sync. I believe that this is going to take some time due to the nature of the law system, since it is difficult to change/edit and amend the law. However, I believe as cases become more prominent, the need to modify the law will become more apparent.

Sources:

Orin S. Kerr, Searches and Seizures in a Digital World, 119 HARV. L. REV. 531 (2005).