Exploratory Hacking, or non-malicious hacking, exists merely as a passage to gain knowledge and experience of a system. Dorothy Denning is a computer scientist who specialized in information security, cyber-crime, cyber-terrorism, and cryptography. In her book, *Concerning Hackers Who Break into Computer Systems*, she addresses the concerns of exploratory hacking. A first glimpse into the minds of exploratory hackers comes on page 141 when she explains the two key principles formed at the AI lab of MIT: Access to anything in the world that may teach you something should be unlimited and total, and all information should be free. These two points were the foundation for the ethical reasoning of exploratory hacking, but I believe it to be quite different than what was first laid out here. Some proponents of the ethical hacking movement may be taking the idea of learning and research further than is bound by reason. In her further interviews, one hacker wrote, "I always strive to do no damage, and never, ever, delete files…" (Denning 146).

To respond to the most basic principles of ethical hacking and what it entails, I must address each claim raised by Denning and her interviews. I believe that it is natural and ethical to learn and explore. Yet, we have such things as trespass laws because some places should not be explored without explicit permission. There are still those who choose to ignore the law and trespass in these areas but sometimes without realization of why they were not allowed to put themselves in danger or maybe even an endangered species who is at their final habitat and they accidentally crush a nest. There exist laws not for simply the art of controlling people and their property, but for good reason. This does not mean all laws should be considered final and as an immovable boundary, but certainly should be considered. Computer hacking is a mysterious place because of how new it is. There has been an abundance of new laws put in place because of hacktivist movements but it is still such a new concept that law is racing to keep up.

In this world, there is information and education that must be paid for. There is also free information. Accessing the information of a company that solicits that information to remain in business and then redistributing that information free of charge is a direct attack on that business and is more immoral than any argument of if the business has the right to solicit that information. Simply accessing a system to access the information in the system for any purpose, learning or not, is not exploratory hacking and should be considered malicious, such as the case of the hacker who wrote, "I will accept that it is… wrong to copy software… but it is more wrong to charge $6,000 for 25K lines…" (Denning 148). An ethical dilemma such as that belongs to the court of law and should be settled under proper authority and decided upon by more than just one voice. This is ignorant to those whose lives depend on that software and who spent much more than a simple $6k in research and development of it (most likely). If that is not the case, I am sure that either now or soon in the future, the courts would uphold that as must unreasonable.

Now, what should we define as ethical, exploratory hacking? This, in my opinion, as a cultivation of the ideas gathered from both sides, has a simple definition. Exploratory hacking should be used as a tool for understanding networking, discovering errors, and an attempt to create a solution. It should not be considered a learning opportunity if you simply address and exploit the mistakes of others. When else in any learning process is this a key step? Understanding where others went wrong and where their mistakes could be rectified is a key component of every breakthrough and discovery in history and science. Consider the first lightbulbs. If someone had taken apart Edison's lightbulb and said, "Well this is wrong, this could be much better," and then used that information to slander Edison's lightbulb, we may have never had the LEDs or advanced screen technology we have today. Instead, it was torn apart and reconstructed to be better than its original. This is the idea of learning and advancing. Exploratory hacking should be used as a tool to discover systems, highlight their flaws, and either attempt to fix them yourself or report them to its developer so they may have a try, in this usage, it is more than morally permissible but should be done by everyone. Simply discovering a flaw is something anyone can do and does not allow for learning or good use to come of hacking unless it is being used maliciously, then it is no longer exploratory, and no longer morally permissible.

Denning goes on to say that hackers are a proponent of information sharing and believe that all information should be public. To this, I criticize and believe that information should only be public as needed. Most people don't understand the information that large companies or the government process and could do much greater harm to them than keeping that information private until necessary to be public. There will be cases of course where companies, or governments choose to hide information with malicious intent but most common just because the public wouldn't understand. The only information that should never be private is that of how the system operates.

Systems and their operation advance often and quickly. This may be surprising to the consumer who relies on the consumer available systems which advance in other ways often but in their structure are not nearly as advanced. This idea retreats to a past topic of software patents. They exist originally as a way of protecting an invention until it can come to market so other inventors or companies cannot steal this idea and sell it as their own. It is what allowed many companies to start in such a competitive marketplace and has long protected the underdogs. This, in my opinion, should be all which protects a system from being in the hands of everyone. When the patent is up, everyone should be able to use and access a system for themselves without restriction. This can allow the world and its systems we rely on to advance far more frequently and in greater leaps.

These ideas align slightly between those of Denning and Spafford. While Spafford argues that no break-in of a computer system is ethical or should be allowed, companies often rely on these and the reports that ethical hackers generate to understand where their mistakes are and how to improve these systems as protection against greater threats. Next, Spafford argues that if all information was free, the world would be chaos. To this, I must agree, to an extent. If information is educational and may benefit the public's knowledge, it should be free and accessible. But there is plenty of information that often doesn't concern the public and could do more harm if public than good. To whom do my ideas more align, I may say Spafford. Not because ethical hacking is a bad concept, but because it can often be used as an excuse for why it is ok to illegally access the information on another system. It remains ethical until this information is accessed.