Cyber Law, Cyber Space, Internet Regulation, Social Responsibility on the Internet

Brian Mock

April 14, 2010

Every American takes pride in the rights given to him or her. These rights are protected by the constitution, and are represented by the first ten Amendments. The First Amendment states that, Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances (U.S. Constitution Online). This means that Congress cannot make laws that infringe on a citizen's right to religion, freedom of speech, the right to peacefully assemble, and the right to petition the government to redress of grievances. Of that long list of freedoms every American is grateful for the freedom of speech, because it is by far the most used on a day to day basis. This also seems to be the right that is most often being questioned as to government involvement. For the safety of the general public the people have allowed the government to set limits to the amount of, free speech a person really has. It is easy to see when the freedom of speech is not being upheld in the real world, but can be difficult to detect in cyber space, for instance the internet.

The World Wide Web started as an idea that focused around the government's need to communicate quickly in the time of a crisis. The government scientists who were, developing networking technology in the 1960's knew that what they were building would be far bigger than themselves, (acm.org) few ever thought that the internet would ever be as big as it is today. Better technology was developed and approved for use by the government. On April 30, 1995, the Internet was released to the world; the government gave total control to the user and took all hands off (acm.org). The internet was off and was expanding at a very rapid rate.

Today we know that hidden within this vast amount of knowledge and entertainment there are many dangers. Despite the danger and risks associated with and around the Web, it should still be a safe haven, where people can speak their minds free from censorship.

The American government has tried to censor the content found on the internet. An example of this is the Communications Decency Act, or CDA, which was a part of the Telecommunications Act of 1996 (Supreme.lp.findlaw.com). This new law would make it illegal to transmit material that was thought indecent or offensive on the World Wide Web (Supreme.lp.findlaw.com). The Communications Decency Act was made law. The CDA was not about reinforcing existing laws, the CDA is not about child pornography, obscenity, or using the Internet to stalk children. These are already illegal under current law. Instead, the CDA prohibits posting indecent' or patently offensive' materials in a public forum on the Internet -- including web pages, newsgroups, chat rooms, or online discussion lists (ciec.org). This law breaks the First Amendment in an extremely flagrant and intolerable way. Due to the CDA, speech which is quite legal in a book or magazine should be banned from the Internet (acm.org) as stated by the Association for Computer Machinery, a group formed to both document the history of the web and fight for the liberties of its users. The CDA was soon over turned by the Supreme Court in June of 1997.

Besides speaking to a person face to face e-mail is the most common form of communication in today's age. People constantly send large amounts of information whether in a text format, picture, or video. At any given point in time a person's life could possibly reside in this virtual mail box. After September 11th the constant chatter about the phone tapping and the Patriot Act over whelmed the American people. Not only is this Act still in effect today, but its jurisdiction is far greater then phone tapping. The Patriot Act gives the Government Authority to intercept wire, oral, and electronic communications (epic.com). The Patriot Act also gives the government permission to do this without a warrant. At any point in time a complete stranger could be going through another person's e-mail possibly without a reason. The Patriot act also

broadens an act that is already in effect. The Foreign Intelligence Surveillance Act gives the Government the ability to collect intelligence from foreign agents and government leaders living in the US. (Cyber.law.havard.edu)The Patriot act opens the law so that any person in the united states who originated from another country. Now not only can the government check the personal information a person uploads to the internet if they are somehow a threat to nation security, but if this person originated from another country the Government can look at that information for any sort of criminal investigation. The Berkman Center for Internet and Society, a research center at Harvard Law School, says, USAPA significantly broadens the scope of situations where FISA intelligence authority can be invoked. . . For example, under USAPA, FISA surveillance authority may be used even if the primary purpose is a criminal investigation. This means that even someone who is not a threat can have their entire life exposed. Even if the people of America were willing to allow the government to poke around in his or her life for the sake of national security, this has gone too far. This infringes heavily on Americans First Amendment right. People can no longer say what they want freely. The fear that what a person says can be read forcefully read and then used against them in court constantly hangs over the American people.

Cyber Theft Networks and Services: Although Napster was the first big name in file sharing, it is not the only file sharing service. This is due in part to the popularity of peer-to-peer (P2P) sharing. Since P2P sharing, shares the connectivity between clients in a particular network, it makes it possible to use the cumulative bandwidth of a particular network rather than relying on the localized resources. This greater connectivity is useful for P2Ps main purpose; that being file sharing. File sharing usually consists of sharing content files containing audio, video and data files in varying file formats.

In years past, peer-to-peer (P2P) networks were configured to save and share files off of several centralized servers, while all the clients (the average user) merely downloaded from this resource. This P2P network, known as a centralized P2P network, was useful due to its structured nature. Since centralized P2P networks are structured, files are collocated with all other files making the search for even extremely rare files, an easy task. This collocation of files is also beneficial for its consistent existence. Meaning, once a file was chosen to be downloaded by a client, the file would be in one place (the server) making for a consistent download. The ultimate downfall of centralized P2P networks was the fact that they were unable to increase system resources while sharing files. This was due to the fact that there are a fixed number of servers which are arranged in strict client-server architecture. This client-server architecture lead to slower data transfers. For example, the more files being downloaded by clients meant a slower data transfer for all users due to the limited system resources.

Today the pure peer-to-peer network is what is commonly being utilized. This concept merely piggybacks the centralized P2P networks foundation, in that files are saved on servers which are in-turn downloaded by clients. Where the pure peer-to-peer network varies is in that instead of storing all the files on a couple of servers, it utilizes the client's machine as a server. By clients simultaneously functioning as both the client and the server on a network, all clients provide resources including bandwidth, storage space and computing power. By doing so, when a file is downloaded the demand on system resources is increased, which is in-turn mediated by the network's ability to increase the capacity of system resources. Pure peer-to-peer networks have their limitations as well. In fact, many of their limitation were centralized P2P network's strong points, these strong points being, a consistent existence and easy to locate file location. For example, a pure P2P network relies on personal computers to store and share files. When a

computer which containing a file shuts-down, looses network connectivity or deletes the file which is being downloaded by another computer, the peer-to-peer sharing comes to an instant halt. Locating a file is also harder due to the very same issue, if the client/server containing the file is off or not connected to the internet then other clients will be unable to locate the file.

Regardless of the type of network sharing taking place, certain fundamentals are always used. First off, the type of network and the network file sharing service being used will require the use of an interface. An interface is downloadable or ingrained software which makes it easy to manipulate the files being offered by the network file sharing service. With user friendly search and download options, a good interface turns a complicated process into something the average user can accomplish in minutes. A download manager is another downloadable software package which does exactly what the name implies, manages downloads. Although not all file sharing services require a download manager, utilizing one streamlines the entire P2P process. With a download manager the average user can manipulate how many files he or she wishes to download at one time and the bandwidth dedicated to each. In addition to controlling downloads the user may also control the server side of file sharing and limit which folders and files they wish to share.

Files most abundantly shared on a P2P network are audio and video files. These files are usually found in there common file formats. For audio, the usual formats one would find on a P2P network are the wav, mp3, mp4 formats. For video one would find mpeg, mpg, avi and wmv formats. These formats can typically be played on computers, mp3 players and some CD players. Certain household DVD players are now available with built in Codec software which is required to play many of the aforementioned file formats. This new development makes the option of P2P

sharing even more appealing to the everyday user since the user no-longer needs to be a computer genius to exploit all the benefits free media has to offer.

Napster Criminal? Napster in and of its self technically has not broken the law. On the website to join Napster it states that it is unlawful to download songs which are under copyright laws. The user that is offering the music is the person who knows if the songs are under copyright. The person downloading the music does not know if the music is under copyright laws however, these people can chat with each other. The people who share the files can speak to each other and ask whether or not the music has been downloaded legally.

Napster at face value did not break the law. However, when they went to court U.S. District Judge Marilyn Patel, fast becoming the Judge Jackson of free music, declared Napster "enjoined from causing, assisting, facilitating, copying, or otherwise distributing all copyrighted songs or musical compositions." (Time, 2000) The argument against Napster is someone cannot provide the software to infringe on copyright laws and then turn a blind eye to people using it illegally.

Title II, the Online Copyright Infringement Liability Limitation Act, creates limitations on the liability of online service providers for copyright infringement when engaging in certain types of activities (Copyright.gov) the copyright laws also states Under the knowledge standard, a service provider is eligible for the limitation on liability only if it does not have actual knowledge of the infringement, is not aware of facts or circumstances from which infringing activity is apparent, or upon gaining such knowledge or awareness, responds expeditiously to take the material down or block access to it. (copyright.gov)The argument from the music industry is that Napster knowingly did not stop the illegal downloading of music. When Metallica, and other artists showed Napster and the courts list of over 300,000 users illegally

using their songs, Napster kicked the users off for a time and they put them back on their service. Napster knowingly allowed these people to continue the illegal use of these songs. The music industry feels that this violates the copyright laws in regards to the digital portion of the law. Under the copyright laws Napster did break the copyright laws.

Law Enforcement the Big Hammer: There is an old analogy that says when there is a problem that needs fixing it is important to choose the appropriate hammer for the job. If you have a small problem, use a small hammer. If there is a large problem, use a large hammer. If you use a hammer that is too small for the job it will not fix the problem. If you use a large hammer on a small problem it will crush it and make things worse. In the case of Napster type file sharing, law enforcement is a large hammer. Law enforcement agencies actively investigating and arresting file sharing perpetrators will not make the file sharing problem worse but may make society less safe.

For example, a study by the Utah Commission on Criminal and Juvenile Justice reveals one out of five women in Utah will be raped in her lifetime (Fattah, 2005). Should we take law enforcement agencies and give them the task of investigating and prosecuting individuals who are sharing files online or try and lower the outrageously high number of rape victims and rapists in Utah? Yes, illegally downloading media and raping women are both against the law, but one has a far greater impact on society and should get the bigger hammer.

Conclusion: Many media centers and recording studios have hired investigators to find those who are illegally downloading their media. They then can file civil suits to stop the perpetrators. Law enforcement should only be brought in on extreme cases of downloading abuse or illegally downloading for commercial gain. Law enforcement should not be brought in against the teenager who has downloaded a few songs illegally.

Along with government intervention the Freedom of Speech is in danger from another source. Many schools and libraries use heavy filters on the internet. Granted there are things that should not be viewed at school, but these filters block large, very useful sections of the internet. Sonam Narayan, a student at Aloha High School, has this to say about schools and libraries restricting websites, I am taking an art class and am in a constant need for pictures off the Internet. . . Now I can't even get them because the school will not allow you to search for photos. Narayan cannot utilize the time given to her at school to work on her art project because the school censors the internet. The trouble with not being able to access the information needed on the internet stretches far beyond pictures, When I have an essay to do sometimes I have go to the library to work on it, because I don't always have access to a computer, but most of the time it is pointless. I cannot go on to the websites I need because they are blocked. I could not even go on to a BBC article the other day, says Hillsboro High School Student Ermine Todd. Harry Lewis, a reporter for the Boston Globe says, But to enforce the FCC standard, someone would have to decide where the "harmful" line should be drawn. What about medical illustrations, or a Globe story about female genital mutilation in Africa? To be safe for all ages, censors would have to exclude vast amounts of useful, lawful content.(Lewis) It is hard to filter material, because material that is of vast informational importance would be seen by the filter as harmful to its users.

It is important that the internet be kept as a forum free for free speech. People give the American Government the ability to deny the freedom of speech only in situation where it concerns the public's safety. The Patriot Act was intended for this purpose, but it invade peoples free speech on the internet. The Government has the ability to look through e-mails for the sake of public safety but there is nothing that stops them if that person is not a threat, and it also opens

the door for prejudging foreigners. The school and library filters are ineffective in that the censor useful information. This information is useful in a subject such as art, or hinder in the process of writing a paper. The Internet should be a place where people can explore thought and ideas without the worry of the First Amendment right of free speech might be denied.

References

U.S. Constitution Online.net 4/1997.

Fattah, G. (2005, April, 12) Utah Rape Rate Rising. Desseret News, p. a1http://www.time.com/time/nation/article/0,8599,51054,00.html Retrieved March 25, 2010 http://www.copyright.gov/legislation/dmca.pdf Retrieved March 25, 2010

http://www.usconstitution.net/const.html#Am1Supreme.lp.findlaw.com. March 25, 2010 http://supreme.lp.findlaw.com/supreme_court/briefs/02-361/02-361.mer.ami.nlccf.pdf.

Ciec.org. Citizens Internet Empowerment Coalition. 9/18/2002.

http://www.ciec.org/Clark, David. Student's Guide to the Internet. Indianapolis: MacMillan Publishing, 1995.

acm.org. The Internet's History and Development. http://www.acm.org/crossroads/xrds2-1/inet - history.htmlCyber.law.havard.edu.

The Berkman Center for Internet and Society The USA Patriot Act Foreign Intelligence Surveillance andCyberspace Privacy http://cyber.law.harvard.edu/privacy/Introduction%20to%20Module%20V.htmLewis, Harry The Dangers of Internet Censorship The Boston Globe 11/5/2008