Below, I have addressed a number of questions proposed in the FTC p2p Filesharing Notice found online at https://secure.commentworks.com/ftc-p2pfilesharing/Notice.htm. Addressing Question A, number 2: For open source projects, such as the various Linux distributions (versions of the Linux operating system), the peer-to-peer protocol known as BitTorrent is an excellent solution. In a BitTorrent system, a tracker server is set up. Files known as "torrents" are then created. Within these torrents is a hash of the IP address of the tracker, the file name to be downloaded, and other tidbits to assist in the workings of the program. A user then downloads a torrent and opens it within his or her BitTorrent client. The client connects to the tracker and gets a list of other clients who have the file available. The client finally connects to these other clients and begins downloading the file. With this BitTorrent system, the purveyor of the file that these clients are downloading moves the download from his webserver to the people who wish to download the file. He is then able to serve his site without having to worry about incurring an additional bandwidth costs. I have vastly oversimplified this explanation for the sake of space, but I invite you to investigate the protocol further at its website, http://bittorrent.com. Addressing Question C, number 1: Risks involved are slim, outside of virus infection from downloading an infected file. However, if consumer is properly equipped with an up-to-date antivirus software or is using an operating less prone to viruses (i.e. Mac OS or any of the various UNIX-based OSes), that risk of infection becomes negligible. Also, an improperly configured or poorly written program could expose information to unintended parties. I refrain from saying "hackers" simply because hackers are rarely after any information of that sort. A "cracker" would, however, be one to explicitly search for that information. Crackers are malicious, hackers are not. Addressing Question C, number 2: If a peer-to-peer client is improperly configured by the authors of the program or the end user himself, information will be inevitably be available. However, this is not unlike any other real-life situation. An automobile owner who does not understand how to lock his vehicle leaves it open for potentially anyone to discover in its unlocked state. The normal passerby would think nothing of it, for they have no intent of opening the car. They might be able to see it, but they lack the impetus to find out if the car is locked. A hacker would see the car and perhaps test the door to find out its state. They'd find it unlocked, and they might crawl in to see what it's like inside or to make sure that there isn't a dead body or the like within, but they'd leave it intact. The hacker might leave a note saying, "I got into your car, you should lock it next time." Perhaps that hacker might even stick around to make sure no one else tries to steal the car and instruct the returning owner how to lock his car. Then, unfortunately, there are crackers. These crackers would see the car, do everything they can to get into the car, and steal things, if not the entire car itself. This car analogy fits perfectly to any computer system. Anyone who drives a car (owns a computer) should know how to lock it (protect themselves from malcious users). Addressing Question C, number 3: The searchable networks will return pornographic results if the user searches for something with a objectionable context. The vast majority of networks do not know if a user is a minor. If a consumer feels that a result is objectionable, he is under no duress to open that file. It is within the realm of human nature that children, who are slowly becoming adults, will be interesting in more adult-like forms of entertainment. If a parent feels that their child is not ready for such content, the parent should moderate their child's usage of a peer-to-peer service as well as the Internet altogether. A parent would not let a child drive a car if the child is not ready, now would they? Addressing Question C, numbers 4 and 5: Spyware and Adware are only an issue on primarily Microsoft's very insecure Windows operating system. Consumers can avoid this risk by calling for Microsoft to further secure their operating system, or by switching to an operating system that is relatively

unaffected by spyware, such as Mac OS or a UNIX-based OS. Addressing Question C, number 6: I direct you towards my explanation for Question C, number 2. Addressing Question C, number 7: Computer functionality is only impaired as a results of poorly written code or spyware/adware/malware. Some protocols and programs require more processing power than others, however this is a limitation of the program itself. To solve this problem, developers of the peer-to-peer program should be called to make their code more efficient. Addressing Question F, number 6: Is there empirical data showing that peer-to-peer filesharing has /not/ increased music sales? Data shown from the record industry are calculated projections, not empirical truths. The industry's missing of projected sales could be attributed to a plethora of other factors, from the United States' current economic recession to the rising price of a llama in India. Since true clairvoyance does not exist, the record industry cannot truthfully claim that they have lost any money to peer-to-peer services. As a matter of personal experience, were it not for my usage of peer-to-peer services in the days before the effectiveness of the Digitial Millenium Copyright Act, I would not have discovered many of the bands of which I am now a fan. General comments on the issue at hand: There's a saying derived from Murphy's Law (what can go wrong will go wrong), that goes like this: If you make something idiot-proof, someone will just make a better idiot. If someone makes a cracker-proof computer, somewhere out there, there is a better cracker who will invade that system. The Internet is, essentially, one massive peer-to-peer network. It will survive any nuclear holocaust, any biological terrorism attack, any worldwide disaster. It is decentralized so that if any one part goes down, it does not affect the rest of the network. This is the essence of peer-to-peer networks. No matter what happens to one, ten, or 100 nodes in the network, the rest of the network will still be there. No matter what happens, this is a force that cannot be stopped. We should embrace it as a world, not as just a single government.