Is creating virus software protected as a first amendment right? Should posting virus software at a so-called "hacker" site be considered as "aiding and abetting" the commission of a crime?

Computer attacks by viruses and other means can cause widespread inconvenience, economic harm and even, at least indirectly, loss of lives. "Denial of service" attacks have disabled Yahoo!, Amazon.com and E*TRADE. Service has been interrupted at airport control towers and 911 systems. Clearly, controls need to exist to preserve safety and to ensure the smooth flow of electronic information.

What sorts of controls are possible?

Some believe it should be illegal to write computer viruses because of the damage they can do. However, the First Amendment gives the right to freedom of speech to all Americans. Free speech, though, has never taken precedence over every other right. Protection does not extend to speech deemed to be obscene, to fighting words, to libel, commercial speech advertising illegal activities or speech directed to incite imminent lawless action. The First Amendment protects the advocacy of a position, but not criminal solicitation.

Those who believe it is illegal to write computer viruses hold that the availability of viruses incites lawless action, and therefore writing the viruses is not protected under free speech. US Courts of Appeals have held that distributing "how to" pamphlets on tax evasion, illegal drugs manufacture and methods to murder can amount to aiding and abetting crime and may be punished as such. Many believe making computer viruses should also be punishable as aiding and abetting crimes, even though the virus writer may never have infected any computer with the virus.

Others, however, are adamant in their defense of the First Amendment right to free speech. They hold that when any information is deemed to be undesirable or potentially dangerous, therefore unprotected, it makes it that much easier to deem other information to be so, until only points of view held by those in power are permitted to be expressed. If freedom of speech is given up, all other democratic rights are called into question. Identifying angry people before they turn to violence is preferred over suppressing free speech.

Viruses can be created for research, especially by those who write code to protect against viruses. If writing viruses were illegal, the lawful community would not be able to write virus-catching software.

The "speech directed to incite imminent lawless action" exception to the right to free speech may not apply either. The Supreme Court Case, Brandenburg v. Ohio, makes it clear that mere advocacy of an illegal action is not illegal where

incitement to imminent lawless action is. For example, writing a "how to" manual on building a bomb is protected speech because it does not cause the immediate infliction of harm. The author does not know who will read his work, nor if they will act on the information he provides. Therefore, there is not "imminent" lawless action. Writing about crime is commonly done in the United States, and it is not illegal. If someone used the plot of a murder mystery to commit a crime, should the author be liable?

If the publication of computer viruses is protected under the First Amendment, what other laws are available to protect against the dissemination of viruses?

The Computer Fraud and Abuse Act is directed toward those who knowingly transmit malicious code. However, CFAA requires proof of intentional unauthorized access to a computer. Most virus creators access only one computer—their own--so the language of this law does not offer significant protection against the spread of viruses. Also, this Act requires proof that the defendant intended to cause damage.

Vandalism statutes may be used when computer virus crime is relatively small scale; terrorism statutes may apply, for larger scale attacks. Many states also have laws dealing with intentional interference with computer systems. All laws already on the books, however, will need to be reinterpreted to be used against this new type of crime.

Are Internet Service Providers liable when viruses are disseminated over their networks?

Internet Service Providers (ISPs) may be prime targets of negligence suits since they are likely to be more readily identifiable and to have more money than the virus writers are. ISPs may defend themselves saying they did not know what was on their network. Even if they did know, they may support their users' right to free speech. However, if users who breach "netiquette" can be ejected from the network, why not those who post viruses? After all, newsstands can choose not to carry pornography.

Can any U.S. law be sufficient to protect against the dissemination of computer viruses?

It would be shortsighted to be concerned only with U.S. laws. Computer viruses disseminated over the Internet could easily have foreign origins, distributions or targets. The recent Love Bug virus was investigated in the Philippines (where it is believed to have originated), according to the laws of that country. International agreements and international sanctions will be required to successfully address the dissemination of malicious software over the Internet.

Questions for Discussion

1. Publishing an inflammatory work, such as a bomb-making manual, is frequently seen as equivalent to publishing virus software, but there is a key difference. The bomb maker is not provided with the actual bomb but must go out and purchase all the ingredients and supplies. The virus software is both a publication and the weapon itself, requiring at most a standard software compiler. Given that the virus software generally includes the weapon as well as the instructions for use, do you feel it should be covered under the First Amendment as a freedom of speech issue?

2. Many experts feel that the explosion in hacking, computer viruses and digital piracy results from a national lack of computer ethics. The federal government is currently developing and promoting computer ethics programs in schools. What do you consider a computer ethics violation? --Copying someone's words or ideas into your paper without attribution? --Downloading an MP3 music file? Copying your friend's commercial word processing program? --Vandalizing a web site with electronic graffiti? Do you feel that those who consider such activities to be ethical issues are exaggerating? Given the many ways that property and intellectual rights can be abused on the Internet, is there any way to promote meaningful computer ethics to young Americans? Is the school the best avenue for computer ethics training or is this a private matter for families?

3. There is not international agreement among countries about what constitutes a cyber crime. Hackers, frequently students in other countries, may receive no punishment, and may even be perceived as heroes in their home countries, for successful hacker attacks against high profile U.S. businesses. Some analysts suggest that U.S. focus should be on negotiating international civil damages that require financial reparation by hackers, rather than criminal sanctions that would be difficult to apply. What is your opinion? What sanctions should be applied to virus distributors and hackers? If financial sanctions are applied, should the parents of offending minors be liable?

4. An Internet Service Provider is required for someone to provide access for web sites over the Internet. This ISP may be the primary point of presence for a regional area or a reseller such as Microsoft's MSN or America Online. Should ISPs have the right to refuse service to those who post virus software on the web? What if the virus software is not openly posted on the web but provided as an encrypted or password-protected file to specific individuals? Do we want commercial entities to provide this level of web policing?

5. Currently, numerous shareware and commercial antivirus packages, firewalls for networks and individual computers, and other security tools are readily available and well publicized. Should a company or an individual be allowed

to recover damages against a hacker or virus attack if they fail to take standard precautions against cyber attack? Precedents could include automobile accidents, where failure to wear a seatbelt or intentionally building a house in a flood plain may result in a reduced insurance settlement.