Control of internet 3427 essay

During the past decade, our society has become based solely on the ability to move large amounts of information across great distances in a very short amount of time and at very low costs. The evolution of the computer era and our growing need for ultra-fast communications has caused a global network of interconnected computers to develop, commonly referred to as the Internet or the world wide web. The Internet has influenced practically everyone’s life in some way whether it was done directly or indirectly. Our children are exposed to the Internet at school, and we are exposed to the Internet simply by just watching our television sets. The Internet has become the primary key to the future of communication in our society today. Because of this, the government feels that it has the right to regulate and control the contents of information distributed through the World Wide Web, contrary to the opinions of most Internet users, myself included. Freedom of Speech Over the Internet At the present, this network is the epitome of the first amendment, freedom of speech. It is a place where people can speak their minds without being reprimanded for what they say, or how they choose to say it. The key to the success of the Internet is its protection of free speech, not only in America, but in other countries as well, where free speech is not protected by a constitution. Because there are no laws regulating Internet material, people may find some of its content offending, ranging from pornography, to hate-group forums, to countless other forms of information. With over 30 million Internet users in the U. S. alone, some of the material is bound to be interpreted as offensive to some other Internet user. My advice to these people is to “ change the station if you don’t like what you see”. Laws and the Internet The newest waves of laws making their way through Congress threaten to stifle spontaneity of the Internet. Recently, Congress has considered passing laws that will make it a crime to send vulgar language or encryption software over the web. These crimes could result in prosecutions punishable by jail time. No matter how insignificant, any attempt at government intervention on the Internet will stifle the greatest communication innovation of this century. The government wants to maintain control over this new form of communication, and it is trying to use the protection of children as a smoke screen to impose these laws upon us. Censorship of the Internet threatens to destroy its freelance atmosphere, while wide spread encryption could help eliminate the need for government intervention. How Do We Interpret the Internet

The current body of laws existing today in America does not apply well to the Internet. Is the Internet like a broadcasting medium, where the government monitors what is broadcast? Is it like a bookstore, where servers cannot be expected to review every title? Is it like a phone company that must ignore what it carries because of privacy? The trouble is that the Internet can be all or none of these things depending on how it is used. The Internet cannot be viewed as one type of transfer medium under the current broadcast definitions. The Internet differs from the broadcasting media in that one cannot just happen upon a vulgar site without first keying in a complicated address, or following a link from another source. “ The Internet is much more like going into a book store and choosing to look at adult magazines” (Miller 75). Because our use of the Internet varies from person to person, its meaning may be interpreted in a number of different ways. Nudity on the Internet Jim Exon, a democratic senator from Nebraska, wants to pass a decency bill regulating sexual content on the Internet. If the bill is passed, certain commercial servers that post nude pictures, like those run by Penthouse or Playgirl, would of course be shut down immediately or risk prosecution. The same goes for any amateur web site that features nudity, sex talk, or sexually explicit words. Posting any sexual words in a Usenet discussion group, which occurs routinely, could cause a person to be liable for a $50, 000 fine and six months in jail. Why does it suddenly become illegal to post something that has been legal for years in print? Exon’s bill apparently would also “ criminalize private mail,” … “ I can call my brother on the phone and say anything–but if I say it on the Internet, it’s illegal” (Levy 56). Internet Access To Other Countries Congress, in their pursuit of regulations, seems to have overlooked the fact that the majority of the adult material on the Internet is sent from overseas. Many of the new Internet technologies, including the World Wide Web, have been developed overseas. There is no clear boundary between information existing in the U. S. and information existing in other countries. Data held in foreign computers is just as accessible as data in America. All it takes is the click of a mouse to access it. Even if our government tried to regulate the Internet, we have no control over what is posted in other countries or sent from other countries, and we have no practical way to stop it. The Internet was originally designed to uphold communications after a nuclear attack occurred by rerouting data to compensate for destroyed telephone lines and servers. Today’s Internet still works on a similar design. The building blocks of the Internet were designed to overcome any kind of communication barriers put in its way. For example, if a major line between two servers is cut, the Internet users will find another way around this obstacle, whether the servers reside in different cities, states, or countries. This characteristic of the Internet makes it virtually impossible to separate an entire nation from indecent information in other countries (Wilson 33). Internet Regulating Gone Bad Recently, a major university attempted to implement limitations on the Internet access available to its students, with results reminiscent of a 1960’s protest. The university had become concerned that it might be held responsible for allowing students access to sexually explicit material, after a research associate found quite a large collection of pornographic pictures (917, 410 images to be exact) that several students had

downloaded. Frightened by a local court case that had recently declared pictures

of similar content obscene, the school administration quickly removed access to

all these pictures and to the newsgroups where most of this obscenity had

susceptibly come from. A total of 80 newsgroups were removed, causing a large

disturbance among the student body, and shortly thereafter, the American Civil

Liberties Union and the Electronic Frontier Foundation became involved, all of

whom felt this was unconstitutional. After only half a week, the college had

backed down, and restored the newsgroups. This is a small example of what may

happen if the government tries to impose censorship (Elmer-Dewitt 102). Children

and the Internet Currently, there is software being released that promises to

block children's access to known X-rated Internet newsgroups and sites.

However, most adults rely on their computer literate children to install and set

these programs up, which inevitable defeats the purpose behind childproofing

software. Even if this software is installed by an adult, who’s to say that

the child can’t go to a friend’s house and surf the web without any

restrictions or supervision? Children will find ways to get around these

restrictions. Regardless of what types of software or safeguards are used to

protect these children, there will always be ways around them. This necessitates

the education of the children to deal with reality. Altered views of an

electronic world translate easily into altered views of the real world. When it

comes to our children, censorship is a far less important issue than good

parenting. We must teach our kids that the Internet is an extension and a

reflection of the real world. We have to show them how to enjoy the good things

and avoid the bad things. This isn’t the government’s responsibility. It’s ours

as parents. (Miller 76) Self Regulation of the Internet Some restrictions on electronic speech imposed by major online companies are not so bad. Most of

these communication companies have restrictions on what their users can

“ say in public forum areas” (Messmer). They must, however, respect their

customer’s privacy. Private e-mail content is off limits to them, but they may

act swiftly upon anyone who spouts obscenities in a public forum.

Self-regulation by users and servers is the key to avoiding government imposed

intervention. Many on-line sites such as Playgirl and Penthouse have started to

regulate themselves. Both of these sites post clear warnings that adult content

lies ahead and lists the countries where this is illegal. The film and video

game industries subject themselves to ratings, and similarly, if Internet users

want to avoid government imposed regulations, maybe it is time they began to

regulate themselves. Encryption Government attempts to regulate the Internet are

not just limited to obscenity and vulgar language. These attempts also fall into other areas, such as data encryption. By nature, the Internet is an insecure

method of transferring data. A single e-mail packet may pass through hundreds of

computers from its source to its final destination. At each computer, there is

the chance that the data will be archived and someone may intercept that data.

Encryption is a means of encoding data so that only someone with the proper

“ key” can decode it. “ Why do you need” encryption? “ It’s

personal. It’s private. And it’s no one’s business but yours” (Laberis). You

may be planning a political campaign, discussing our taxes, or having an illicit

affair. Or you may be doing something that you feel shouldn’t be illegal, but it

is. Whatever it is, you don’t want your private electronic mail or confidential

documents read by anyone else. There’s nothing wrong with asserting your

privacy. Perhaps you are not really concerned about encrypting your e-mail

because you believe that you have nothing to hide. I mean you haven’t broken the law in any way, right? Well then why not just write letters on postcards instead of sealed away in envelopes? Why not submit to drug testing on demand? Why require a warrant for police searches of your house? Do law-abiding citizens have any need to encrypt their e-mail? What if everyone believed those law-abiding citizens should use postcards for their mail for the simple reason that you have nothing to hide? Just because you haven’t done anything wrong, doesn’t mean that you want the whole world to have access to your letters or e-mail. Analogously, it would be nice if everyone routinely used encryption for all their e-mail, innocent or not, so that no one drew suspicion by asserting their e-mail privacy with encryption. “ Think of it as a form of solidarity” (Zimmerman). Until the development of the Internet, the U. S. government controlled most new encryption techniques. With the development of faster home computers and a worldwide web, the government no longer holds control over encryption. New algorithms have been discovered that are reportedly unable to be

cracked, even by the FBI and the NSA. This is a major concern to the government

because they want to maintain the ability to conduct wiretaps and other forms of

electronic surveillance into the digital age. Pretty Good Privacy To stop the

spread of data encryption software, the U. S. government has imposed very strict

laws on its exportation. One very well known example of this is the PGP (Pretty

Good Privacy) scandal. PGP was written by Phil Zimmerman, and is based on

“ public key” encryption. This system uses complex algorithms to

produce two codes, one for encoding and one for decoding. To send an encoded

message to someone, a copy of that person’s “ public” key is needed.

The sender uses this public key to encrypt the data, and the recipient uses

their “ private” key to decode the message. As Zimmerman was finishing

his program, he heard about a proposed Senate bill to ban cryptography. This prompted him to release his program for free, hoping that it would become so

popular that its use could not be stopped. One of the original users of PGP

posted it to an Internet site, where anyone from any country could download it,

causing a federal investigator to begin investigating Phil for violation of this

new law. As with any new technology, this program has allegedly been used for

illegal purposes, and the FBI and NSA are believed to be unable to crack this

code. When told about the illegal uses of his program, Zimmerman replied,

“ If I had invented an automobile, and was told that criminals used it to

rob banks, I would feel bad, too. But most people agree the benefits to society

that come from automobiles — taking the kids to school, grocery shopping and

such — outweigh their drawbacks”. Data Encryption Standard The government

has not been totally blind for the need of encryption. For nearly two decades, a government sponsored algorithm, Data Encryption Standard (DES), has been used

primarily by banks. The government has always maintained the ability to decipher

this code with their powerful supercomputers. Now that new forms of encryption

have been devised that the government cannot decipher, they are proposing a new

standard to replace DES. Clipper Chips This new standard is called Clipper, and

is based on the “ public key” algorithms. Instead of software, Clipper

is a microchip that can be incorporated into just about anything (Television,

Telephones, etc.). This algorithm uses a much longer key that is 16 million

times more powerful than DES. It is estimated that today’s fastest computers

would take “ 400 billion years to break this code using every possible key”

(Lehrer 378). The catch: At the time of manufacture, each Clipper chip will be

loaded with its own unique key, and the Government gets to keep a copy, placed

in escrow. Not to worry though, the Government promises that they will use these keys to read your traffic only when duly authorized by law. Of course, to make

Clipper completely effective, the next logical step would be to outlaw other

forms of cryptography. If privacy is outlawed, only outlaws will have privacy.

Intelligence agencies have access to good cryptographic technology. So do the

big arms and drug traffickers. So do defense contractors, oil companies, and

other corporate giants. But ordinary people and grassroots political

organizations mostly have not had access to affordable ‘ military grade’

public-key cryptographic technology. Until now. PGP empowers people to take

their privacy into their own hands. There’s a growing social need for it. That’s

why I wrote it. (Zimmerman) Signatures The most important benefits of encryption

have been conveniently overlooked by the government. If everyone used

encryption, there would be absolutely no way that an innocent bystander could

happen upon material they find offensive. Only the intended receiver of the data could decrypt it (using public key cryptography, not even the sender can decrypt it) and view its contents. Each coded message also has an encrypted signature verifying the sender’s identity. The sender’s secret key can be used to encrypt an enclosed signature message, thereby “ signing” it. This creates a digital signature of a message, which the recipient (or anyone else) can check by using the sender’s public key to decrypt it. This proves that the sender was the true originator of the message, and that the message has not been subsequently altered by anyone else, because the sender alone possesses the secret key that made that signature. “ Forgery of a signed message is infeasible, and the sender cannot later disavow his signature” (Zimmerman). Gone would be the hate mail that causes many problems, and gone would be the ability to forge a document with someone else’s address. The government, if it did not have ulterior motives, should mandate encryption, not outlaw it.

Conclusion As the Internet continues to grow throughout the world, more governments may try to impose their views onto the rest of the world through regulations and censorship. It will be a sad day when the world must adjust its views to conform to that of the most prudish regulatory governments in existence. If too many regulations are enacted, then the Internet as a tool will become nearly useless, and the Internet as a mass communication device and a place for freedom of mind and thoughts, will become nonexistent. There exists a very fine line between protecting our children from pornographic material, while still protecting our rights to freedom of speech. The users, servers, and parents of the world must regulate themselves, so as not to force government regulations that may stifle the best communication instrument in history. If encryption catches on and becomes as widespread as Zimmerman predicts it will,

then there will no longer be a need for the government to intrude in the matters

of the Internet, and the biggest problems will work themselves out. The

government should rethink its approach to the censorship and encryption issues,

allowing the Internet to continue to grow and mature on its own.

Bibliography

Elmer-Dewitt, Philip. “ Censoring Cyberspace: Carnegie Mellon’s Attempt

to Ban Sex From Its Campus Computer Network Sends A Chill Along the Info

Highway.” Time 21 Nov. 1994: 102-105. Laberis, Bill. “ The Price of

Freedom.” ComputerWorld (1998). Dialog Magazine Database, 036777. N. pag.

34 Apr 1994 < http://www. computerworld. com>. Lehrer, Dan. “ The Secret

Sharers: Clipper Chips and Cypherpunks.” The Nation 10 Oct. 1994: 376-379.

Levy, Steven. “ The Encryption Wars: Is Privacy Good or Bad?” Newsweek

24 Apr. 1995: 55-57. Messmer, Ellen. “ Fighting For Justice On The New

Frontier.” Network World (1997). Dialog Magazine Database, 028048

. Miller, Michael. “ Cybersex Shock.” PC Magazine 10 Oct. 1995: 75-76.

Wilson, David. “ The Internet Goes Crackers.” Education Digest May

1995: 33-36. Zimmerman, Phil. (1995). “ Pretty Good Privacy” v2. 62, [Online].

Available Ftp: net-dist. mit. edu Directory: pub/pgp/dist File: Pgp262dc. zip. Works

Cited Elmer-Dewitt, Philip. “ Censoring Cyberspace: Carnegie Mellon’s

Attempt to Ban Sex From Its Campus Computer Network Sends A Chill Along the Info

Highway.” Time 21 Nov. 1994: 102-105. Laberis, Bill. “ The Price of

Freedom.” ComputerWorld (1998). Dialog Magazine Database, 036777. N. pag.

34 Apr 1994 < http://www. computerworld. com>. Lehrer, Dan. “ The Secret

Sharers: Clipper Chips and Cypherpunks.” The Nation 10 Oct. 1994: 376-379.

Levy, Steven. “ The Encryption Wars: Is Privacy Good or Bad?” Newsweek

24 Apr. 1995: 55-57. Messmer, Ellen. “ Fighting For Justice On The New

Frontier.” Network World (1997). Dialog Magazine Database, 028048

. Miller, Michael. “ Cybersex Shock.” PC Magazine 10 Oct. 1995: 75-76.

Wilson, David. “ The Internet Goes Crackers.” Education Digest May

1995: 33-36. Zimmerman, Phil. (1995). “ Pretty Good Privacy” v2. 62,

[Online].

Available Ftp: net-dist. mit. edu Directory: pub/pgp/dist File: Pgp262dc. zip.