The New Panopticon- The Internet Viewed as a Structure of Social Control.

Tom Brignall III
Tennessee Tech University

Introduction

There is little doubt the Internet has progressed from a little-known entity of the military to a growing world cultural phenomenon in the last ten years. Television, radio, and newspapers are filled with "dot com" commercials, educational institutions are investing large amounts of money to move classes online, and corporations are investing millions in their company websites. According to Ramsey (2000), Internet usage has been growing at such a rapid rate that at the end of 2000 60% of US households were online.

With the growth of Internet usage, serious concerns about Internet security and privacy have arisen. Robert Lemos reports that the Electronic Privacy Information Center and Privacy International prepared a report that states, "many new technologies, in particular new Internet services, are eroding privacy worldwide" (Lemos, 2000: 1). The report also noted that the United States is leading efforts to remove legal restrictions limiting electronic surveillance. "The Clinton administration announced on July 17, 2000 that it would seek broad powers to compel Internet Service Providers (ISPs) to allow FBI monitoring of email messages" (Martin, 2000: 1). According to Reuters news (2001), in response to the terrorist strikes of September 11, the United States Senate Judiciary Committee chairperson Patrick Leahy announced that congressional leaders agreed on a comprehensive anti-terrorism bill. United States legislators are seeking to expand the power of law enforcement to wiretap suspected terrorists, share intelligence information about them, and track their Internet movements. However, the bill does not precisely define who or what a terrorist is. It is unclear how much power and freedom this bill will enable authorities to observe individuals online.

One can argue that there is a growing—and seemingly reasonable—perceived need for heightened Internet security in the United States. The topic of improving Internet security and content control is frequently discussed in popular media—and includes a consideration of topics ranging from pornography on the Internet, radical hate groups, bombs making plans, viruses, crackers, hackers, to employees using company time to sell and buy products on Ebay. However, a little known fact is that, given the current structure of the Internet, and due to the long-standing desire of the United States government to track and monitor Internet traffic, there may be no need to create a massive new Internet security infrastructure.

According to Miller, (1996) the FBI is using a program called Carnivore to randomly monitor all email. Carnivore could eventually be modified to allow individuals to monitor chat conversations, news posts, and peer-to-peer networks online. Carnivore is a variation of a software program typically used by Internet Service Providers (ISP's) known as a packet sniffer. It sorts through the stream of data entering an ISP to find the senders and recipients of email to and from the target of surveillance. Carnivore can be programmed to look for "keywords" in emails. A program like Carnivore can easily examine every email message handled through a given ISP. This form of surveillance is similar to telephone surveillance called "trunk side" wiretapping, which has been illegal in the United States for more than 30 years.

It can be argued that email should be protected by the Constitution against government intruders. However, according to Miller (1996), "The U.S. Court of Appeals for the Fifth Circuit ruled in November 1994, that email messages stored in a computer are not protected by the Electronic Communications Privacy Act of 1986, which prohibited the interception of private electronic mail" (p. 291). The ruling allowed the seizure by police of the computer and software housing the Bulletin Board System containing the email. In the opinion of the Court, the law as written only protects messages while they are in transit. Carnivore could easily be developed for ISP's and corporations as a tool to view what consumers want, are consuming, and what they are doing with the products

they consume. It could be justified based on national security, better safety from hackers and viruses, and protection from illegal sites from overseas servers.

If Internet service providers or police agencies randomly monitor Internet users, then the Internet begins to share similar properties with the panopticon prison structure. The panopticon as a conceptual structure can be applied to any physical structure that provides the ability of those in a position of authority to monitor the "inmates" without the "inmates" knowing when they are being monitored. What is unique within the structure of the Internet is that it allows multiple layers of observation to occur such that the "inmates" can become the observers of other "inmates". In such a situation, no one knows who is the observer and who is the observed.

This paper is an attempt to describe what the panopticon model is and to provide support that elements of the panopticon model inherently exist in the structure of the Internet. This paper provides examples of how Internet user's privacy is being overlooked in order for certain corporations to provide declared necessary services such as security against terrorists and hackers, control over illegal content (pornography, pirated computer, music, and film files, and dangerous information on how to build bombs etc.). Still, it remains too early to say that any kind of organized conspiracy exists with the goal to strip Internet users of their rights and monitor every interaction.

Authors like Levy (2001), Rohm (1998), Schwartau (1996), and Sunstein (2001), document the involvement of the military and multinational corporations in the development of the Internet. However, it is hard to prove the intentions of an organization investing large amounts of money into Internet development. Not all Military Internet investment is malicious. For instance, the military spends large amounts of money on Internet site development for training intelligence agents on how to recognize and evaluate a terrorist threat (*http://www.intel.army.mil/*), allowing troops to get a college degree (*http://www.esc.edu/navy*), and according to Schwartau (1996) for national security. Although there Internet users can be subject to viruses and online theft, Levy (2001), Sunstein (2001) talks about the misunderstanding and over-inflated fear of the existence

of evil Internet hackers and crackers as promoted by companies that stand to gain a profit from the purchase of their software or services.

Currently, it is impossible to say that one central organization is implementing the panopticon on the Internet in order to maintain some form of social control. However, the panopticon might emerge as a desirable structure for the perceived need for the protection of national security Internet user safety. There are abundant warning signs of the potential for an organized movement to control the flow of information over the Internet. The ACLU (*http://www.aclu.org/action/carnivore107.html*) issued a warning against the recent Patriot bill passed by the United States Congress and Senate to combat terrorism. According to the ACLU "to accept the FBI's arguments in favor of Carnivore is to reject that core premise of the Fourth Amendment by giving the FBI carte blanche access to the communications of innocent people" (1). The recent trends of Internet monitoring need to be disseminated to Internet users in order for them to make informed decisions about the future of their Internet rights. This paper is meant to be a warning to Internet users of the potential future problems of Internet privacy. This paper is also meant to make readers aware that certain elements of the panopticon have in the past been implemented by various military, police, and corporate entities.

Jeremy Bentham's Panopticon Model

As Jeremy Bentham proposed in his ***Panopticon; or The Inspection House (1787)***, a model for efficient prison and neighborhood control would be the panopticon. The intention of the design of the panoptic structure was to be an architectural algorithm that could be used in prisons, schools, cities, and factories for reinforcing a system of social control. Bentham argued that those inside the panopticon should always think they are under inspection at any time. It is important "that the persons to be inspected should always feel themselves as if under inspection, at least as standing a great chance of being so" (Bentham, 1843: 44). Not only are the prisoners under the possibility of constant surveillance but the panopticon also serves to keep "the under keepers or inspectors, the servants, and subordinates of every kind, to be under the same irresistible control with respect to the head keeper

or inspector, as the prisoners or other persons to be governed are with respect to them"(Bentham, 1843: 45). Bentham believed the omnipotent potential to be observed at anytime appealed "to the humanity of the principal for redress against the neglect or oppression of subordinates in that rigid sphere" (Bentham, 1843: 45).

A typical panopticon prison as described in Bentham's book, was a building shaped in an octagon. Individual cells were built into the circumference of the building, around a central well. An inspection tower atop the well was constructed, and lighting was used in such a way so that the cells were lit, but the inspection tower dark was not visible to the prisoners. This made it possible for one person in the tower to monitor the activity of many people. The prisoners knew they were under surveillance, but none of them knew exactly when. It was precisely this mental state of being seen without being able to see the watcher that Bentham meant to induce. When you can induce that state of mind in a population, you do not need whips and chains to restrain them from rebelling. Ideally, the prisoners would attempt to modify their own behavior in order to avoid punishment for an infraction. Unlike prisons that use cameras, or fixed guard positions, there is nowhere to hide in a panopticon prison.

Bentham believed the panopticon could extend beyond the prison to be used to help control cities and businesses. The Internet is a structure that is inherently similar to the panopticon in that Internet service providers can observe their customers' online activities at any time without the customers' knowledge. The Internet is also inherently similar to the Bentham panopticon prison structure because the dissemination of power and control is in the hands of the "jailers". However, an Internet based panopticon is freed from most of the architectural constraints of Bentham's stone and brick prototype. With wireless technology, the Internet can be viewed from almost anywhere on the planet. With an Internet panopticon model the social totality comes to function as the hierarchical and disciplinary panoptic machine. Only those that refuse to use the technology will be free from being observed. Even if individuals do not use the Internet, friends, family, and peers may use it thereby extending some of that social control over non-users. It is bad enough when a structure that is viewable to

individuals is employed in order to gain social control (for instance cities employing cameras to watch the city streets). It is an Orwellian situation when a panopticon model can never be viewed in its totality, where it has no physical structure or permanent location.

I am not suggesting the Internet is transforming into a jail per se. Instead, the application of Bentham's concept could assist in converting Internet users into behaved disciples of Internet capitalism. Reflecting the growing disciplinary power in the United States, the Internet currently exists as a hierarchical structure where the application of supervision and normalizing occurs. Normalization occurs when Internet sites are shut down because of their content, either by arrest, threat of a lawsuit, court injunction, pressure against the website provider, or pressure from a special interest group. Examples of normalization include websites that contained nude pictures (disappearing or becoming pay per view sites), Napster and MP3.com (mp3s), the latest Hollywood films (mpeg rips), pop culture cites (X-files fan clubs), and computer news sites (Apple hardware news sites) that have been shut down because they contained content that was considered an infringement of privacy, decency, or copyright laws. I argue there will always be rouge sites but as they become known, most of them will tame their content, present the content in a legal fashion (pay to download), or disappear.

The integration of supervision and normalization could help to provide an examination process of Internet users by those who choose to do the observing. The justification of supervision and normalization would be to protect people from copyright violations, terrorists, or crackers. However, monitoring could also be a freelance activity, in which individuals monitor others for pay. With the plethora of hacking tools available to Internet users, it is arguable that certain individuals already have the ability to monitor online interaction and collect massive amounts of private information. Many online companies such as American Online openly admit to monitoring all transactions in order to make their service family oriented. American Online has their own customers observe other customers in exchange for services. Using the inherent elements of the Internet, and employing the principles of a panoptic structure, the

Internet could be used as an information gateway that would allow a governing body (whether corporate, national, or international) the ability to maintain a powerful grip on the flow of information that travels through the Internet. A tight form of social control could be exercised over those who choose to use the Internet as a main source of information, communication, research, product purchasing, and community building.

Michel Foucault's Adoption of the Panopticon Model

Foucault states that "the major effect of the panopticon: is to induce in the inmate a state of conscious and permanent visibility that assures the automatic functioning of power" (Foucault, 1972: 201). The panopticon model helps to eliminate unwanted group collectivity and helps reinforce the power of the authorities that have implemented social structure and control. Therefore, no one using the Internet can know whether they are interacting with a trusted ally or with an agent of the state. A collective identity of individuals in a panopticon model "is abolished and replaced by a collection of separated individualities. From the point of view of the guardian, it is replaced by a multiplicity that can be numbered and supervised" (Foucault, 1972: 201). The major effect of the panopticon is to induce in individuals a state of conscious and permanent visibility that assures the automatic functioning of power. The belief that individuals need to be protected, and are free as long as they do not break the law becomes the dogma of those who are self oppressed.

According to Foucault, the panopticon model becomes an architectural apparatus that allows a power relation to be viewed as independent of the person who exercises the power. "The inmates (are) caught up in a power situation of which they are themselves the bearers" (Foucault, 1972: 201). Those individuals that exist in a panopticon model become their own agents of oppression. The panopticon model can become a form of hegemony while also allowing those who control the model to make a profit. Ultimately, individuals in a panopticon model eventually will not be weary of "Big Brother", but weary of "Little Brother" (or other inmates) who may be willing to keep track of group members for a profit. The power of the panopticon becomes "a faceless gaze that transformed the whole social body into a field of perception:

thousands of eyes posed everywhere, mobile attentions ever on the alert" (Foucault, 1972: 214).

The Panopticon is Already in Place

One does not have to wait for the passage of an anti-terrorist bill to see elements of a Panopticon model being currently used on the Internet. Companies like America Online, Prodigy, and Microsoft Online openly admit to monitoring their users' communications in an effort to protect their customers. I argue that large parts of the Internet are transforming into panopticon structures. A private Internet service provider (ISP) does not need to uphold certain constitutional laws when providing a private service to its customers.

When it comes to the gathering of private personal information, Internet technology has a jaded history. I will review Prodigy's stage.dat install file as an example of a private firm monitoring their customers. When Prodigy was a bulletin board service (BBS) in the late 1980's and early 1990's customers needed to use a proprietary piece of software to access Prodigy. A person who wanted to use Prodigy had to install Prodigy's software on their personal computer. To gain access to the Prodigy BBS, a person had to submit personal information (where they live, gender, age, et cetera) and a credit card number. When a user logged on to the Prodigy BBS, the user unknowingly granted Prodigy access to all of their computer files. The ability of Prodigy to access their customer's hard drives was not written in the installation manual, discussed in the service contract, or mentioned anywhere on Prodigy BBS site.

The fact that Prodigy had access to their customers' hard drives came to users' attention when a mysterious file appeared on hard drives. In the article, "A Slice of Life in My Virtual Community" (1993b), Rheingold argues Prodigy was able to create customer profile files on users' hard drives and was also capable of reading any private information on the customer's computer. I can attest to this as a result of my own personal experience with the Prodigy stage.dat file.

When I was working for a small computer store in the late 1980s, a customer of ours installed the Prodigy software on his computer. Two days later, the customer called and complained that his virus checker had found a questionable file on his hard drive but he could not

determine whether the file was a virus. The computer file was in the Prodigy directory so I thought maybe the Prodigy install disk had installed the file on the hard drive. I told him to delete the whole Prodigy directory and reinstall the software. After he reinstalled the Prodigy software, I told him to look for the stage.dat file on his hard drive. He said it no longer existed on his computer hard drive. He then logged onto Prodigy and then logged off. The stage.dat file appeared on his hard drive again. I asked him to bring the system in so that I could inspect the file. When I opened the file in the program "dbase 3" the customer's personal information including where he had spent his time online was included in the file.

When I contacted Prodigy about this alarming situation, their official response was that the stage.dat file served as a means of recording customer usage patterns in order to enable Prodigy to provide "better" consumer service. In other words, Prodigy officials stated that the stage.dat file contained recorded transcripts of what its customers had done, and Prodigy would freely access such valuable information whenever its customers were logged on. Prodigy justifies the use of the stage.dat file as a convenient and efficient way to track customer trends. They offered to refund the customer his money if he did not like their policy, but insisted they were doing nothing illegal.

Prodigy is not alone in its desire to observe their clients. American Online (AOL) recruits volunteers to be "guides". Guides spend nine hours online a week policing the AOL service and an additional two hours reading email and filling out reports. Guides greet new members and make them feel welcome, answer user questions about AOL, promote online attractions and events, complete market research, and enforce the AOL's terms of service. Guides monitor chat rooms, newsgroups, and email messages. AOL expects guides to report to AOL officials and to enforce the AOL's rules by warning rule violators.

Peer-to-Peer Networks: A New Hegemonic Mythology

Software like Napster, Hotline chat, Morpheus, and Gnutella offer Internet users the ability to exchange electronic files. These electronic files include music, films, computer games, video games, books, art, and the conversion of anything in an electronic format. Internet

users and corporations are characterizing software companies, such as Napster and Gnutella, as everything from pirates and thieves to heroes of the free content movement. Peer-to-peer network program suppliers declare that they are helping to emancipate all electronic information.

I argue that the unlimited exchange of electronic information amounts to online piracy: individuals are not paying for the intellectual products of others. Supporters of such trading software claim that they are doing nothing more than previewing the material they download in order to make an informed decision about whether they want to buy it. Some users argue that free downloads of products will help the content creator become famous. Others argue that digital audio and software are so expensive that they need to be free because people should not have to pay exorbitant costs in order to enjoy art.

Such forms of "emancipatory piracy" provide a hegemonic myth that the Internet is not a panoptic mechanism of social control, but a structure for emancipation. I argue that whether or not these consequences are intended, peer-to-peer networking will strengthen the power of large multinational corporations, and make it far easier to monitor Internet users. Companies like BMG, Sony, and Warner/AOL are making deals with Napster and other peer-to-peer networks to control the flow of computer files in order to create Internet profit centers.

Internet Programs like Gnutella allow users to view all the programs and content on another user's hard drive. Many users of Gnutella do not mind this (or are unaware of this) because they are happy to be able to download files from other users. While, Gnutella users can select specifically which hard drive directory they prefer other users to view, many users voluntarily allow other users to view and download anything from their specified hard drive directory. However, not all peer-to-peer users want to share the information on their hard drives, and, again, in Gnutella's program preferences, it is possible for the user to turn off the ability of others to access part or all their hard drives. Thus, it can be argued that peer-to-peer networks are secure because only individuals that have access to the network have access to files from a particular hard drive. However, security and privacy

issues arise when using programs like Gnutella because they are based on a peer-to-peer network technology.

Most peer-to-peer technology relies on open source programming. An open source program allows anyone to have the computer programming code used to create the program in order to create modifications. Open source programs easily allow crackers and hackers to create modifications to programs such as Gnutella that allow an individual the potential to gain access to other users' hard drives and networks without permission. Even if a peer-to-peer software client does not allow others to view their source code, arguably it is easy enough for some crackers to de-compile a piece of software and make modifications.

One may argue that individuals should be willing to share information in the era of the open source. Users in chat groups based on the topic of Napster are rallying around Napster, against Metallica and the RIAA based the assertion that music (and other electronic information) should be free. Many of these individuals also argue that all Internet content should be free. The hegemonic myths that perpetuate the idea that content should be available to everyone free of charge reinforces the idea that it is acceptable for unknown users to emancipate everything from any source. Thereby it becomes unfashionable to protect information via legal apparatuses because, presumably, all information should be free. Interestingly, this myth is not spread by the artists or the culture industry, but is more often propagated by the consumers (or pirates) of electronic resources (*http://www.xnapster.com/*, *http://www.xnapster.com/*, *http://wwww.campchaos.com/*, *http://www.boycottmetallica.org/*, *http://www.killmetallica.com/*, *http://www.expage.com/napsterlives*, *http://www.mp3newswire.net/stories/2000/studentnap.html*).

It does not seem to matter to the individuals who spread cultural hegemony laced with discussions of technology and freedom that file "sharing" does not exist among most computer pirates. According to Reuters news service (2000), the Xerox Palo Alto Research Center reported that 70% of the people who use Gnutella to download music, do not share any of their own files. The

report revealed that 1 percent of the users served close to 50 percent of the requests and 25 percent served 98 percent of the requests. Similar reports reflect similar numbers for Napster, Hotline, and Music City Morpheus users.

This lack of sharing seems to contradict the proposed purpose of companies like Napster, and Morpheus and the emancipation of art from corporations into the mass's hands. However, the lack of sharing files helps to develop the myth that peer-to-peer software is intended primarily for the emancipation of information. I believe the real issue is peer-to-peer software users are enhancing the potential for others to observe their Internet actions and data files. Downloading electronic content using peer-to-peer software becomes a form of cultural conditioning. If users of peer-to-peer software are awarded "free" content, arguably many will more willingly relinquish their privacy.

Corporate Adoption of Peer-To-Peer Networking

Peer-to-peer software companies like Napster and Gnutella have captured the imagination of some corporations such as Intel. Intel executives are now claiming that peer-to-peer software will transform business information solutions. "In peer to peer networking, individual computers talk to one other, allowing computing tasks to be managed among those computers instead of or in addition to using a centralized network" (Fried, 2000: 1). A peer-to-peer network means that online users no longer navigate strictly within the confines of the current manifestation of the Internet. Instead, users log into a peer-to-peer network using software that allows all users to share information, navigate the Internet, and view all other systems on the network. According to Fried, not everyone is convinced that this is a great innovation. "At a press conference this week, a Belgian technology reporter suggested that any corporate computing manager who approved using peer-to-peer networking should be fired because of the security risks involved" (Fried, 2001: 1).

There may be security risks, but, in fact, the greatest risks are not to the creators of the main system software, but to the users who log onto the system. The main providers and creators of the peer-to-peer software can create a program that allows them to monitor and dominate the

dissemination of information via their network. For instance, Napster originally claimed that they could not monitor or control files that were uploaded or downloaded on their site. Yet, Napster reserved the right to approve all modifications to their program. If Napster detected a user running a modified program, they kicked the user off the network.

Spyware

Peer-to-peer software is not the only threat to Internet privacy. Another example of software that can allow users to be observed is called spyware. Some software when installed on a computer will allow the software company to observe a user's actions online. According to Steve Gibson (2001), Internet software companies such as Morpheus and Real Audio create and distribute spyware software. "Spyware" refers to any type of software that employs a user's Internet connection to send information from the user's computer without the user's knowledge or permission. Software such as Real audio can be used to track the actions of users while they run the software, and in some cases, even when the software is not running. The spyware program does not have to be an Internet based program. Any program from a video game to a word processor can use the user's Internet connection to relay information about the user and the computer to a software company's Internet server.

The Internet Becoming a Cultural Necessity

The Internet can become a cultural necessity if people believe that the Internet is the best way to communicate, consume information, or consume products. If individuals use the Internet as a primary source to communicate, read the daily news, buy products, or download a movie—increasingly because of a lack of other viable choices—then the Internet becomes a cultural necessity. If the classic institutions of information dissemination such as newspaper, radio, and television, continue to choose the Internet as a preferred vehicle for their distribution of information, the Internet may become the main source for many societies to disseminate cultural information. Further, the implementation of the panopticon model may be perceived by users as a necessity if they are convinced that such a structure

would protect them or make their transactions online more efficient. I argue that for many United States citizens, the Internet is already an important primary source for information. According to Holohan (2000), "the UCLA Internet Report found that over 67% of the study's users think that the Internet is an important or extremely important source of information" (Holohan, 2000: 1).

Theoretical Considerations for the Sacrifice of Internet Privacy

No longer do governments, multinational corporations, or politicians need to exert force when trying to maintain social control. Cooptation of powerful minority groups through the fear of observation makes it possible to eliminate the perception of tyranny. Adorno and Horkheimer provide a theoretical discussion on the culture industry. Their discussion helps to provide additional possible explanations as to why anyone would want to implement a panopticon model. "Tyranny leaves the body free and directs its attack at the soul. The ruler no longer says: You must think as I do or die. He says: You are free not to think as I do; your life, your property, everything shall remain yours, but from this day on you are a stranger among us. Not to conform means to be rendered powerless, economically and therefore, spiritually to be self employed" (Adorno and Horkheimer, 1998: 133). If self-oppression and conformity become the normal course of behavior for individuals who wish to avoid punishment, then the culpability of oppression shifts from the oppressor to the oppressed.

In order for a society to request the existence of an Internet panopticon model, it is important that the model is perceived to be socially legitimate. According to Berger and Luckmann (1966), in order for structures to become culturally legitimate a system of ideas and symbolic representations needs to be created that supports the oppressive structure. "Incipient legitimation is present as soon as a system of linguistic objectifications of human experience is transmitted" (Berger and Luckmann, 1966: 94). Through pop art technology, legitimation takes place by means of symbolic totalities. The symbolic universe used by pop culture elements can allow a panopticon model to look desirable to many Internet users. Laws passed by Congress that contradict the

constitution, and eliminate Internet privacy seem filled with patriotic intention. The portrayal by mass media that the average Internet user needs protection from the evil of hackers on the Internet helps to reinforce the justification for the need of the presence of an Internet panopticon model. All counter-hegemonic ideas are logically explained away, swallowed up, reformed, co-opted, and spit out with new meanings attached (there is a hegemony.com website that promotes e-commerce techniques). Berger and Luckmann believe technology has strengthened the power of hegemony. Technology has made it easier to continually recreate a modern and hip system of signs that perpetuates the legitimation of oppressive structures.

The Internet Viewed as a Structure of Liberation

In contrast, technology theorists such as Rheingold (1993) suggest that the Internet could be a tool for liberation. The question is what type of liberation is attainable from Internet based interaction. Is the distribution and dissemination of ideas sufficient to foster and create a social revolution? It is probable that individuals that use the Internet will develop counter cultural ideas. Without a physical group struggling with real life situations that involve such things as group cooperation, interaction rituals, mores, and values how can any revolutionary ideas be considered plausible? Are virtual struggles and interaction valid and meaningful replacements for physical realities? Without a developed and tested group identity and without the use of group social praxis, any declaration of Internet group solidarity is merely a paper tiger. Therefore, I would suggest that Rheingold's assumption that the Internet could be a tool for liberation is another hegemonic myth.

Identity and truths conveyed on the Internet are merely symbolic gestures of the alpha and numeric variation. Words and numbers only have the meaning we attribute to them, so how can the Internet be a structure for freedom, when no physical act is manifested directly from the Internet. The only action or reaction from the symbolic structure of the Internet is spawned from the interpretation of symbols and behaviors that follow. Individuals are confusing the concrete structure of the Internet (wires, modems, computers) with the abstraction of freedom. To say the Internet is a structure for freedom

is reification. The Internet is nothing more than binary code. There is only perceived freedom or enslavement, but the Internet itself is helpless to do anything. Instead, Internet users ultimately decide what will be done. Even with live video chats, a simulacrum of social interaction defuses the struggles individuals have in day-to-day group activities. Identity and truths, when reduced to mere signs, make it problematic to separate the individual from the masses. In turn, it becomes difficult to convey to an individual the necessity for social cooperation even when it may not be cost beneficial to an individual. Not only is there a lack of quality interaction on the Internet among individual producers of products, there is a competitive nature created in many individuals. The lack of quality interaction only strengthens an Internet panopticon model because an individual may feel compelled to be the monitor of those that are monitoring him or her.

Conclusion

While a fear of a nationwide conspiracy is highly romantic, I doubt that a national governmental organization has the entire Internet under control. However, it may not be the government that Internet users need to fear. As more corporations merge, less United States business competition occurs. The companies left after all the recent mergers are likely to look for ways to know their customers better to maximize their profits. The ultimate corporate goal may be to develop a cultural structure that assists producers of products to know what consumers want before the consumers even know. Inherently, given the availability of such customer information resources with existing technologies, the Internet structure itself can easily be thought of as a panoptic structure.

If Internet users demand protection from online theft, crackers, terrorists, and pirates by demanding the privatization of the Internet, then issues of constitutionality and privacy disappear. When private groups take control of public institutions, individual constitutional rights no longer apply. A popular idea among many leading conservative Internet gurus (including Bill Gates, and Al Gore) is that if the Internet were to be run and policed by private industries, then the

Internet would become a safer, more efficiently run mechanism.

If the panopticon model is nothing more than a marketing tool used by corporations in hopes of knowing their customers better, this is still an invasion of privacy. Having the potential to observe everything a customer does is highly detrimental to democratic values and issues of personal privacy and freedom. Do consumers desire to be catalogued so that all corporate product decisions might be preordained based on statistical demographic studies? Do mass-market surveys based on Internet usage and traffic accurately reflect what consumers truly desire? If these events should occur with more frequency than they already do, is this not a form of social control?

If the Internet is completely privatized and the trend of corporate mergers continues, computer technology will be marketed according to the dominant culture's societal values. I argue that capitalist corporations base their social values on individualism and competition among citizens. Advertisements present illusions of computers and the Internet freeing individuals from the constraints imposed by the previous dependence on others. Because of the Internet, individuals can now work at home with much greater ability to be "fully productive". Corporations and groups can meet online. If Internet based social interactions bore us, we cut the machine off. As Internet users, we seemingly have no obligation to anyone but to please ourselves. The reality is that a privatized Internet offers us little social interaction. In return, a privatized Internet does offer users the opportunity to become virtual slaves to the new Internet life system created by multinationals, with little hope of creating our own independent Internet except within the realms of Virtual Reality. I argue that Internet cultural marketing will only strengthen the growing apathy of United States citizens. Such attention to the production of homogeneous cultural artifacts will continue to produce creativeless, bland, and sterile cultural icons such as Brittney Spears and Barney. Any counter pop creative culture will continue to be drowned out if it does not look like a big money maker.

A purely economic Internet panopticon model, with no illusions of controlling the world in any other way but economically, is still an efficient mechanism for social

control as a consumer-based simulacrum of social interactions. The ability to choose what is marketed and sold (based on the majority of consumer desires) limits individuals of real choice by only allowing them a certain amount of decisions based on the demographic make up of the masses.

I challenge that the invasion of privacy of most Internet service providers is highly detrimental to democratic values and issues of personal privacy and freedom. Is it desirable to further the possible mass homogenization of culture in order to maximize profits? Many speakers take the position that the Internet will only help U.S. citizens if it is privatized. The real force behind this move is the debasement of our culture and the freedom of business to pursue profit without constraint from the non-market institutions that are the repository of community values, using their hired hands in the advertising industry to lead the way. Behind the veil of lies and rhetoric, there appears to be more to the multinationals desire for a secure Internet.

The private sector will build the Internet; the financing will come from consumers, and the government will stay out of the way, while noncommercial enterprises will be kept on the sidelines. President Clinton's former Secretary of Commerce, Ronald Brown, has stated on television that the ultimate goal is the removal of most of the judicial and legislative restrictions on all types of telecommunications companies. Some would say that this would promote a free Internet culture with no censorship. I argue that quite the contrary will end up happening; censorship will actually increase, as experts for what is morally correct will be the chairs of companies who stand to profit from regulation of information. If everything online is privatized, our constitutional rights will be thrown out the window. Only if nudity, violence, and strong language can make a profit for some corporation, will our so-called freedom prevail. Who will be the technological lord that will make the decision for what is nudity and what is art? What is violence and offensive, and what is culture?

One may argue that such discussions of corporations controlling culture are based on conspiracy theories and myth. However, if corporations are being controlled by a few people, and if the merging of corporate giants

continues, a valid argument can be made that a few people do have the power to decide what the masses have access to.

According to Miller (1996), the *Wall Street Journal* (9/9/94) reported that power in multinational corporations is becoming more centralized. Now top executives call the shots themselves either like "old fashioned corporate dictators or as new global specialists with the clout to rule their particular niche of the business from Hong Kong to Houston" (40).

I believe that if the government drops federal funding and allows the Internet to completely privatize, the freethinking spirit of the Internet and its potential as a teaching and community tool will disappear. In its place will be a cultural leviathan, making sure we do not do anything that would result in fewer profits for multinationals.

References

Aboba, B. (1993). The Online User's Encyclopedia: Bulletin Boards and Beyond. Reading: Addison-Wesly.

Adorno, T. W. & Horkheimer, M. (1998). Dialectic of Enlightenment. (Rev. Eds.). Trans. J. Cumming. New York: Continuum.

American Civil Liberties Union. (November). Urge Congress to Stop the FBI's Use of Privacy-Invading Software. Aclu.org *http://www.aclu.org/action/carnivore107.html*

Argyle, K (1996). Is There a Body in the Net? Pp 58-69 in Cultures of Internet: Virtual spaces, real histories, living bodies. Rob Shields (Eds.). London: Sage Publications Ltd.

Bentham, J. (1843). Works. (Eds.). Bowring. Endinburgh: William Tait.

Berger, P., L. & Luckmann, T. (1966). The Social Construction Of Reality: A Treatise In The Sociology Of Knowledge. New York: Doubleday.

Foucault, M. (1995). Discipline & Punish: The Birth of the Prison. Trans. A. Sheridan New York: Vintage Books.

Foucault, M. (1972). The Archaeology of Knowledge & The Discourse On Langua*e*. Trans. A. Sheridan. New York: Pantheon Books.

Fried, I. (August 24, 2000). Intel Execs: Napster-like Sharing Will Transform Businesses. Cnet.com.

http://news.cnet.com/news/0-10032002603611.html
Gibson, S. (2000) The Anatomy of File Download: Spyware. Gibson Research
Corporation. http://grc.com/downloaders.htm
Gnutella Corporation. *http://gnutella.wego.com/*
Holohan, M. (August, 16 2000). Users Trust Information on Internet, UCLA Study Shows. Yahoo.com. *http://www.yahoo.com*
Jones, G. S. (1995). CyberSociety: Computer-Mediated Communication and Community. Thousand Oaks: Sage Publications.
Kroker, A. (1996). Virtual capitalism. Pp.167-180 in Techno Science and Cyber Culture. Aronowitz S., Martinshons, and Menser M. (Eds.). Routledge: New York.
Lemos, R. (July, 24 2000). House Committee to Tame Carnivore? Zdnet.com. http://www.zdnet.com/zdnn/stories/bursts/0,7407,2606759,00.html
Levy, S. (2001). Hackers: Heroes of the Computer Revolution. New York: Penguin.
Martin, P. (August 2, 2000). Clinton Administration Plan For FBI Spying On Email. World Socialist Web Site. *http://wsws.org*
Milgram, S.(1974). Obedience To Authority: An Experimental View. New York: Harper & Row.
Miller, E. S. (1996). Civilizing Cyberspace: Policy, Power, And The Information
Superhighway. New York: ACM Press.
Music City Morpheus Corporation. *http://www.musiccity.com*
Napster Corporation. *http://www.napster.com*
Poster, M.(1989). Critical Theory And Post Structuralism: In Search Of A Context. Ithaca: Cornell University Press.
Postman, N.(1992). Technopoly. New York: Vintage Books.
Ramsey, G. (2000). The E-Demographics And Usage Patterns Report: September 2000. E-marketer.com. http://www.emarketer.com/ereports/ecommerce_b2b/
Real Player. *http://www.realplayer.com*
Reid, B. (1993). Usenet Readership Summary Report. Palo Alto CA: Network Measurement Project at the DEC Western Research Laboratory.

Reid, E. M. (1991). Electropolis: Communication and Community on Internet Relay Chat. Honors Thesis, University of Melbourne.
Reuters News. (August 21, 2000). Study Finds Volumes of Free-Riders On Gnutella. *http://www.reuters.com*
Reuters News. (October 18, 2001). Congressional Leaders Agree on US Anti-Terror Bill. http://biz.yahoo.com/rf/011018/wat025047_1.html
Rohm, W.G. (1998). The Microsoft File: The Secret Case Against Bill Gates. New York: Random House.
Rheingold, H. (1993a). The Virtual Community: Homesteading On The Electronic Frontier. Massachusetts: Addison-Wesley Publishing Company Reading.
Rheingold, H. (1993b). A Slice Of Life In My Virtual Community. Pp. 57-82 in Global networks: Computers and International Communication. Harasim L. M. (Eds.). Cambridge: MIT press.
Sennett, R. (1976). The Fall Of Public Man: On The Social Psychology Of Capitalism. New York: Vintage Books.
Schwartau, W. (1996). Information Warefare: Cyberterrorism: Protecting Your Personal Security in the Electronic Age. New York: Thunder's Mouth Press.
Shields, R. (1996). Cultures of Internet; Virtual Spaces, Real Histories, Living Bodies. London: Sage Publications Ltd.
Sunstein, C. R.(2001). Republic.com. New Jersey: Princeton University Press.

Theory & Science

Citation Format

Brignall III, Tom (2002). The New Panopticon: The Internet Viewed as a Structure of Social Control. *Theory & Science*: 3, 1 [iuicode: http://www.icaap.org/iuicode?105.3.1.x]

Source: http://theoryandscience.icaap.org/ 2002