James W. Lindenschmidt
JWL.Freakwitch.net

From Virtual Commons To Virtual Enclosures: Revolution and Counter-Revolution In The Information Age

Introduction

I begin to write this 36 hours into the invasion of Iraq by the US military machine under the command of George W. Bush. It has been declared "A-day," and it will be characterized by the "shock and awe" bombing campaign of "strategic targets" in Iraq. It is the latest chapter in the story of neoliberalism's struggle to maintain control of the world economic climate. The corporate media outlets are in the throes of their wargasms, showing the bright lights of explosions and tracer fire over Baghdad and the shiny metal of American warplanes, ships, and missiles. All of these media outlets are interchangeable; there is a very small set of stories being aired as Iraq is decimated. When one channel picks up an approved story by one of the "embedded" reporters with the military, many other channels pick it up too. Corporate media has full control over traditional media outlets; the corporate radio and television stations look all-too-similar to one another.

On the other hand, as I write this, I am using my computer. My computer runs Free software[1], with a high-speed Internet connection provided by Time Warner. I am listening to Amy Goodman's radio show, *Democracy Now!*, via streaming mp3 over the Internet. I am monitoring several alternative news websites, weblogs from people in Iraq, and emails from several listservs that provide first-hand accounts of the situation in Iraq and all over the world. In short, all of my information independent of corporate control, both incoming and outgoing, is mediated through my computer and the Internet.

The Internet represents perhaps the single most revolutionary element of the Information Age. At present, it allows anyone with computer access to communicate with anyone else, without being mediated by a corporate media outlet. Stories can be told, and heard, without interference by centralized control. It allows organization of countless different struggles around the world; as an example, the peace movement is mobilizing against this invasion of Iraq faster than any other peace movement in history. This unprecedented mobilization of peace activists is possible because of computers and the Internet.

Yet the free exchange of ideas as mediated by computers and the Internet is in danger. Every revolution has a counter-revolution, and the counter-revolution upon the free exchange of ideas is well underway. The Information Counter-Revolution is an attempt by corporate interests to assert control over the Internet, with the end goal of recasting it in terms of pre-Information Revolution media outlets, which treat information infrastructure as "content delivery systems" controlling what passive viewers may see. The counter-revolution seeks to accomplish these ends through two primary means: expansion of "intellectual property" laws and a re-architecting of the Internet to unilaterally enforce these laws through an infrastructure of centralized control; these are the virtual enclosures. The goal of this article is to trace both the ongoing revolution in information technology that have produced unprecedented gains in the struggles against neoliberalism and the counter-revolution that threatens the gains made. The Internet has allowed people to communicate, organize, and mobilize more quickly and efficiently than ever before; this phenomenon is demonstrated by struggles in Chiapas, Seattle, Genoa, Cancun, and the unprecedented mobilization of the

[1]For the best definition of "Free software," see "The Free Software Definition" available online: http://www.gnu.org/philosophy/free-sw.html.

worldwide peace movement against the current invasion of Iraq. The open, end-to-end architecture of the Internet—a key element of the virtual commons—allows it to be used for virtually any purpose, an enormous benefit to activists.

But the virtual commons is being enclosed; this enclosure will have a similar effect in both brutality and scope to the previous enclosure movements in history. The virtual enclosures threaten the very existence of the Internet as we know it, along with a person's ability to access his or her data on his or her computer. We are moving into a future where the civil rights of anyone using a computer to mediate information is under attack; where ownership of virtually all works created on computers will be controlled by software corporations, alienating the creative person from their creations; where advancing technologies will allow corporate interests to conduct pre-emptive strikes against all possible copyright violations; where ultimately, the mere thinking of certain copyrighted ideas will transform the thinker into a criminal.

From Virtual Commons To Virtual Enclosures

> We have entered a time when nature can be architected to control ideas and control their spread; when nature can be architected to defeat the free flow of information; when nature can be architected to close the open society. And all this closing can be done in the name of property.[2]

As Midnight Notes has argued elsewhere,[3] this current invasion of Iraq, along with other wars of neoliberalism already waged and yet to be ordered, are the death throes of a failed economic system that has concentrated power so narrowly that billions of people worldwide do not have what they need. With intelligent use of the world's resources, humanity could be on the verge of a post-scarcity existence. Yet greed, and the accompanying violence to justify and enforce greed, prevail. This socio-economic system that imposes itself upon the majority of the world, exploiting the masses to an unprecedented degree, cannot hold itself. It has reproduced itself so far and so wide that there is no room left for it to grow. Virtually the entire planet is now privately owned, enclosed from the common and made scarce. So to continue its insatiable lust for constant growth, capital must expand its enclosures to territories not of this earth.

Like the peasant lands of a few centuries ago, cyberspace is currently a commons. In order for capital to be able to exploit a commons, it must be enclosed. The virtual commons, which is itself a post-scarcity environment, is becoming the virtual enclosures, with artificial scarcities being imposed upon it. The virtual enclosures are being created and enforced in two primary areas that concern us. First is in the realm of ideas, where ideas are controlled through "intellectual property" laws. Under these laws, copyrights are being perpetually and retroactively extended, patents are being awarded for abstract algorithms and business methods, and a tangled web of lawyers and negotiators work ceaselessly to negotiate payments for the right to legally use the enclosed ideas. In addition, laws have been passed which transform sharing into "piracy" and "theft," using a peculiar conception of "property" as the ability to preemptively control the behavior of the individual, before he or she ever comes into contact with the intellectual property. This control, however, is in crisis because of the open, end-to-end architecture of the Internet, which brings us to the second area of concern.

---

[2]Lawrence Lessig, "Reclaiming a Commons," keynote address, The Berkman Center's "Building a Digital Commons," May 20, 1999, Cambridge, Mass. p. 6. Online.
http://cyberlaw.stanford.edu/lessig/content/articles/works/lessigkeynote.pdf

[3]See Midnight Notes, "Respect Your Enemies—The First Rule of Peace: An Essay Addressed to the U.S. Anti-War Movement." Online.
http://slash.autonomedia.org/print.pl?sid=02/10/27/1615237

Because the Internet as originally architected is a virtual, post-scarcity commons that has no tragedy and no borders, it represents a huge problem for the IP interests. In response to this threat, the Internet is being enclosed. These enclosures of the virtual commons are not enforced by shotguns or by depleted-uranium missiles. The virtual enclosures are perfectly enforceable, because the rules of enforcement are being architected into the code of the Internet itself. Cyberspace is malleable, and it is increasingly being cast into a space with an infrastructure of built-in, centralized control.

This control takes several forms. To more fully understand the nature of this control, we must first investigate the nature of the Information Revolution and specifically the nature of free and unfree software, open and closed data formats, and the architecture and capacities of the Internet.

The PC Revolution and the Rise of Proprietary Software

There is little or no scarcity inherent in software. Indeed software—or any other digitized bits of information—can be perfectly and easily copied from one machine to another over a computer network. In the first few decades of the computer age, it never occurred to anyone to try to prevent the free spread of software; computer hardware was so rare, large, and expensive (in other words, scarce) that it did no good for a person to have a copy of software, except in the capacity of studying the source code to improve one's understanding of programming techniques. Openness and freedom to study the code was the default; it is consistent with the scientific paradigm of openness, peer review, and repeatability that has been dominant for centuries. In those early days of computing, virtually everyone who directly interacted with a computer was a programmer, and it made no sense to obscure the inner workings of a computer system from those using it. However, the onset of the microcomputer brought about a paradigm shift, engineered largely by Microsoft (whose name is an abbreviation of "Microcomputer Software"), in the way society thought about software. Microcomputers, particularly the often-cloned "IBM PC," became a commodity item. PCs were designed so that an "average person" (that is, a non-programmer) could use them. For such users, who now constitute the vast majority of users, it made no immediate difference whether the software—more specifically, the source code readable by humans—was accessible to them or not. These computers ran MS-DOS, Microsoft's first product, as their operating system. MS-DOS—which was not an original Microsoft product, having been derived from another product called QDOS—was distributed in binary format, which made its underlying code unreadable to even the most highly-skilled programmer. Binary files, as opposed to source code, are gibberish to a human but are readable by the computer. In order to maximize their opportunity to profit, Microsoft treated its proprietary, deliberately-obscured software as carefully guarded Intellectual Property, imposing severe licensing restrictions in their End User License Agreements (EULAs). One could no longer legally copy software to share with friends. Those who continued to do so were termed "pirates," and sharing became equated with theft, plunder, and murder on the high seas. Microsoft had successfully imposed an artificial scarcity upon software, treating it by the same property rules of the old publishing paradigm.

Remember, copyright originally existed to control publishing a work, to control who could create copies of a work and sell them. It had nothing to do with what one could do with a copy of a published work. One is still (for the moment) free to share a book with a friend, free to burn it if it offends, and even free to sell it to a used bookstore or to another person. It is still possible to buy a used book, in which case no money goes to the publisher and no royalty is paid to the author. The single parameter controlled by copyright law, as it was originally conceived, is: who has the right to cause new copies of the work to come into being *and offer them for sale?*

But computers have tremendously complicated this system of regulation because the notion of what constitutes a copy has become hazy. The very functionality of a computer depends on its ability to copy information. For example, when you boot your computer, one of the first things it will do is to load its

operating system, whether it be GNU/Linux, Windows, or whatever else. This operating system is stored on the computer's hard drive, but "loading" it means that the operating system is copied into the computer's memory. The OS doesn't move from the hard drive; it (hopefully) remains stored there permanently. In other words, every time a computer accesses a file, it must make a copy of it. If one takes current copyright law literally, it would be illegal to run a computer because doing so entails making copies of copyrighted information. This reality alone represents sufficient proof that the copyright system, as applied to publishing, is incompatible with digitized information.

Yet Microsoft extended the publishing metaphor, with great success, to the software space. As a result of these maneuvers, you do not own "your" copy of Microsoft Office.[4] When you pay hundreds of dollars to Microsoft for a copy of MS Office, you are not buying the software, rather, you are buying legal permission to use the software. This distinction is crucial to understanding the IP crisis. No longer is copyright meant as "the right to produce and sell a copy"; now it is a regulation of users who must buy permission to use a "rightful copy." The shift in focus has gone from regulating publishers of information to regulating users of information.

Another troubling form of user regulation is through proprietary data formats. When a writer, for example, writes a piece using Microsoft Word, the data is saved in such a way that the information contained within the .doc file is obscured, and is only readable through Microsoft Word. In contrast, the Free software application, OpenOffice.org, uses an open data format. Even if one does not have a copy of OpenOffice.org, one can still access their data through a text editor, and it will be readable by a human, since it is based on the open XML data format. XML is similar to HTML, which is the technical language of most content on the Internet. To get an idea of what HTML looks like, go to any web page and choose the "view source" option on your web browser. It is a series of commands, called "tags," that organize the content in a specific way that can be displayed by the browser. The openness of HTML—the ability to see the underlying code of a webpage—is one reason the Internet grew so quickly. When the Internet was new, people needed to learn how to make web pages. Because HTML is an open format, it was easy to look at web pages and see what people were doing, and to learn from existing, well-designed pages. In a similar way, it is easy for other word processors to develop filters to read and properly display OpenOffice.org data files. So not only is the program free, but the data produced by the program is free and open. As an example of the difference between an open and a closed format, here are the first few lines of a .doc (Microsoft Word) file:

```
ÐÏ#à¡±#á>#þÿ##9#;#þÿÿÿ8ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
¥ÁY ##¿##ñ##bjbjóWóW##%>{#uÿÿ#ÿÿ#ÿÿj#j#j#j#j#j##Â#Â#Â
#Â#8ú###Â#×#ð###"#(J#J#J#J#J#J#œ##ž#ž#ž#ž#ž#ž#$Ç#ô#»
```

And here are the first few lines of an .sxw (OpenOffice.org Writer) file:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE office:document-content PUBLIC
"-//OpenOffice.org//DTD OfficeDocument 1.0//EN" "office.dtd">
<office:document-content
xmlns:office="http://openoffice.org/2000/office"
```

[4]Microsoft Office is just an example. This statement applies to virtually all proprietary software that exists.

```
xmlns:style="http://openoffice.org/2000/style"
xmlns:text="http://openoffice.org/2000/text"
xmlns:table="http://openoffice.org/2000/table"
xmlns:draw="http://openoffice.org/2000/drawing"
xmlns:fo="http://www.w3.org/1999/XSL/Format"
xmlns:xlink="http://www.w3.org/1999/xlink"
xmlns:number="http://openoffice.org/2000/datastyle"
xmlns:svg="http://www.w3.org/2000/svg"
xmlns:chart="http://openoffice.org/2000/chart"
xmlns:dr3d="http://openoffice.org/2000/dr3d"
xmlns:math="http://www.w3.org/1998/Math/MathML"
xmlns:form="http://openoffice.org/2000/form"
xmlns:script="http://openoffice.org/2000/script"
office:class="text"
office:version="1.0">
```
[5]

The first is gibberish; it is binary data that only a computer can decode, using the closed algorithms in the Microsoft Word document format. The second, however, is open; if one is willing to take the time to learn XML, one can make sense of this data.

So again we see the same pattern: openness vs. hiddenness, freedom vs. control, whether we refer to computer programs or the data generated and stored by those programs. Openness, in code or in data formats, lays the foundation for the virtual commons. When one considers what property means—the ability to control access to a specific resource—then openness becomes even more important. It can be argued, for example, that a writer who writes using a proprietary word processor such as Microsoft Word does not own his or her data, since access to that data is controlled by Microsoft; the writer cannot access his or her data except through using Microsoft Word.[6] So for this reason alone, it is highly desirable for any person using a computer to create documents or other works to run Free software using open data formats, an option that has become more and more viable with the extraordinary maturation of GNU/Linux desktop software. At this point in time there is little reason apart from inertia why the vast majority of computer users cannot use Free software exclusively in their day-to-day work, taking advantage of the growing virtual commons.

Revolution of the Virtual Commons: Commodity Hardware, Free Software, and Cyberspace

In what could be the crowning achievement of the Information Revolution, humanity is on the verge of an enduring virtual commons. The virtual commons consists of the Internet, electronic communication devices such as personal computers, and all the data produced and circulated using

[5]The .sxw file format shown is actually a compressed file format; it has been unzipped—or converted from a single file to a directory of several files—using common data compression utilities. After unzipping, the "content" file in the unzipped directory looks like the above.

[6]Happily, this claim is no longer entirely true when referring to Microsoft Office's proprietary data formats. OpenOffice.org, for example, contains filters that have been reverse-engineered, so that Microsoft Office documents can be imported into OpenOffice.org. However, these filters are imperfect, and the translation from the closed format of Microsoft Office to the open format of OpenOffice.org will in some cases be incomplete, with some document formatting errors or irregularities. This imperfection is due to the closed nature of the .doc data format. From my own personal perspective, these filters work well enough for regular use, on those rare occasions that I must work with someone else's Microsoft Office file. However, future ability to reverse-engineer closed file formats is in question.

these tools, prior to their (possible) enclosure. This section will analyze the nature of the virtual commons.

NYU law professor Yochai Benkler is credited with a very useful model of communications systems: the layer model. Any communications system—including the virtual commons—consists of three layers: the physical layer, the code layer, and the content layer. As Lawrence Lessig writes:

> At the bottom is the "physical" layer, across which communication travels. This is the computer, or wires, that link computers on the Internet. In the middle is a "logical" or "code" layer—the code that makes the hardware run. Here we might include the protocols that define the Internet and the software upon which these protocols run. At the top is the "content" layer—the actual stuff that gets said or transmitted across these lines. Here we include digital images, texts, on-line movies, and the like.[7]

Lessig applies the layer model to the Internet, but it applies equally well to the whole of the virtual commons, of which the Internet is part. For example, a single computer can be described in terms of layers; the physical layer is the computer hardware, the code layer is the computer software, and the content layer is the information created or processed by the computer. One of the key parameters of the layer model is the degree of control exerted over each layer. Again, Lessig:

> Each of these layers in principle could be controlled or could be free. Each, that is, could be owned or each could be organized in a commons. We could imagine a world where the physical layer was free but the logical and content layers were not. Or we could imagine a world where the physical and code layers were controlled but the content layer was not. And so on.[8]

Different communications media will have different combinations of freedom and control. For example, anyone is free to stand in the town square to rant, give a speech, or attempt to save the souls of the wicked. The physical layer (the town square) is a commons; the code layer (the language spoken) is a commons; and the content layer (the rant or speech or oration) is primarily free, having been created by the would-be orator. On the other end of the spectrum is cable television, where all the layers are controlled.

But the virtual commons is peculiar in that it has a mixture of freedom and control in all three layers. Access to computers and the Internet is controlled by the economic capacity to purchase a computer and rent an Internet connection or account. However, this control is not absolute; computers are available for public use in libraries, and the price of computers constantly fluctuates. Additionally, spectrum and wireless technologies provide a glimpse of a possible future where Internet access is ubiquitous, similar to cellular phone coverage. Whether spectrum should be organized in terms of property or a commons is currently a hotly debated topic.

The code layer of the virtual commons is equally ambiguous, as there is an abundance of both Free and proprietary software in use around the world. Put another way, computer users have a choice about whether the code layer of the virtual commons in their vicinity should be free or controlled. Those who believe it should be free will run Free software. On the other hand, those who run proprietary software have made their choice that the code layer surrounding them should be unfree. Regardless of this individual choice, however, much of the Internet is a commons, and furthermore, the survival of the Internet depends on the part that is a commons. Cyberspace is based on open

[7]Lawrence Lessig, *The Future of Ideas: The Fate of the Commons in a Connected World* (New York: Vintage Books, 2002), 23.

[8]Lessig, *The Future of Ideas*, 23.

protocols such as TCP/IP, HTML, HTTP, and FTP.[9] It is coded using an end-to-end (e2e) architecture, which stipulates that

> rather than locating intelligence within the network, intelligence should be placed at the ends: computers within the network should perform only very simple functions that are needed by lots of different applications, while functions that are needed by only some applications should be performed at the edge. Thus, complexity and intelligence in the network are pushed away from the network itself. Simple networks, smart applications.[10]

The Internet was originally architected using this e2e philosophy. The network was designed only to move packets of data back and forth, not to make decisions about the data or regulate the kinds of data being sent across the network. To use the "information superhighway" metaphor, a road does not and should not care whether a bicycle, a Ford, a Subaru, or a go-cart is being driven on it. These decisions are made by the drivers—or the users of the Internet.

The Internet's explosive growth coincided almost exactly with the explosive growth of another part of the code layer of the virtual commons: the Free software movement. The history of the Free software movement is well documented.[11] But the key to understanding the Free software movement is a legal device known as "copyleft," which is embodied in a unique software license called the GNU General Public License (GPL). The GPL was coded to use existing copyright law to establish and protect a commons for software. As Richard Stallman, the primary architect of the GPL, describes:

> Copyleft uses copyright law, but flips it over to serve the opposite of its usual purpose: instead of a means of privatizing software, it becomes a means of keeping software free. The central idea of copyleft is that we give everyone permission to run the program, copy the program, modify the program, and distribute modified versions—but not permission to add restrictions of their own. Thus, the crucial freedoms that define "free software" are guaranteed to everyone who has a copy; they become inalienable rights.[12]

Copyleft was a stroke of genius, as it worked within the framework of existing law to produce a commons of code—a commons that has grown by leaps and bounds in nearly two decades of work. More recently, the copyleft concept has begun to be applied to creative works in general, and not just computer programs; a good example is the Creative Commons set of licenses.[13]

The Free software commons has many advantages. First, it is a post-scarcity commons; there is no tragedy of the virtual commons. On the contrary, the more who use the Free software commons the better it gets, as there are more eyes to spot and report bugs and request features, more programmers to fix bugs and implement features, and more power users to write manuals and

---

[9]These acronyms stand for: Transmission Control Protocol/Internet Protocol, Hyper Text Markup Language, Hyper Text Transfer Protocol, File Transfer Protocol.

[10]Lessig, *The Future of Ideas*, 34.

[11]See the present author's "A Barnraising in Cyberspace: Linux and the Free Software Movement," in *The Maine Scholar* no. 13 (Fall 2000): 123-138; DiBona, Ockman, Stone, ed., *Open Sources, Voices from the Open Source Revolution* (Sebastopol, Ca.: O'Reilly Publishers, 1999); or Eric S. Raymond, *The Cathedral and the Bazaar* (Sebastopol, Ca.: O'Reilly Publishers, 2001). Much is also available online.

[12]Richard Stallman, "The GNU Operating System and the Free Software Movement," in *Open Sources*, p. 59.

[13]See http://creativecommons.org/learn/ for more information. This text is licensed under a Creative Commons license.

documentation. Indeed, the virtual commons contains a fundamental set of three values: "no one owns it, everyone can use it, anyone can improve it."[14] Second, there are methodological benefits to having a complete software system as a commons, in terms of the development of the software. New software, placed in the commons, tends to evolve quickly, becoming stable and usable over a very short period of time. Anyone can fix a bug, and make the fix part of the commons. As a result, the Free software community as a whole tends to be much more responsive than proprietary software corporations to the needs of its user base. There is no profit motive to get in the way of producing quality software. Third, the cost for Free software is nominal. It is easily affordable to almost anyone; it can be downloaded, copied, shared at will. Fourth, it does not obscure data behind proprietary formats. Fifth, it tends to be much more secure than proprietary software, for many of the same reasons bugs are fixed quickly. If a security exploit is discovered in a Free software program, a patch is usually available within hours, a patch that, too, is subject to peer review and public scrutiny to make sure that it actually does and does well what it is supposed to do.

The pragmatic benefits of free software are many. But increasingly, there are ideological benefits to Free software as well, benefits that are extremely important to the struggle against neoliberalism. Free software is being used extensively in the Third World; in many ways, the Third World is the key front in the battle over the virtual commons. Free software allows a Third World nation to construct state-of-the-art computer systems and networks for a fraction of the cost of using proprietary software. More and more people worldwide are viewing Microsoft (and proprietary software in general) as not only hostile, but as completely unnecessary. There is simply no good reason to spend millions of dollars lining the pockets of an American megacorporation, paying for the privilege of having less freedom and less control over one's data, while increasing one's dependence upon a profit-seeking enterprise. Peru, for example, is considering legislation requiring all government offices to use free software. In an open letter to Microsoft, Peruvian Congressman Dr. Edgar David Villanueva Nuñez explained the important points of the Bill they are considering:

> The basic principles which inspire the Bill are linked to the basic guarantees of a state of law, such as: Free access to public information by the citizen; Permanence of public data; Security of the State and citizens. To guarantee the free access of citizens to public information, it is indispensable that the encoding of data is not tied to a single provider. The use of standard and open formats gives a guarantee of this free access, if necessary through the creation of compatible free software. To guarantee the permanence of public data, it is necessary that the usability and maintenance of the software does not depend on the goodwill of the suppliers, or on the monopoly conditions imposed by them. For this reason the State needs systems the development of which can be guaranteed due to the availability of the source code. To guarantee national security or the security of the State, it is indispensable to be able to rely on systems without elements which allow control from a distance or the undesired transmission of information to third parties. Systems with source code freely accessible to the public are required to allow their inspection by the State itself, by the citizens, and by a large number of independent experts throughout the world. Our proposal brings further security, since the knowledge of the source code will eliminate the growing number of programs with *spy code*. [15]

This letter, which reframes discussion of "freedom" in terms of personal freedoms of citizens as opposed to corporate "freedom" to profit from technological monoculture, is highly significant for

[14]Doc Searls, "Patent Absurdities," *Linux Journal* no. 73 (May 2000): 75.

[15]Dr. Edgar David Villanueva Nuñez, "An Open Letter To Microsoft," Online.
http://www.pimientolinux.com/peru2ms/villanueva_to_ms.html

several reasons. First, it is a scathing critique of questionable marketing techniques used by Microsoft—termed "Fear, Uncertainty, and Doubt (FUD)" by Microsoft—used to argue against the use of Free software. Second, it brought a large amount of attention to Third World struggles against corporate control of information to the free software communities in North America and Europe. *Linux Today*, for example, noted that Villanueva's letter "has raised him practically to folk hero status amongst the open source community almost overnight."[16] Third, the letter points out contradictions in neoliberalist assumptions about what is important in decision about IT. For Microsoft, software adoption by government should be decided in terms of "intellectual property rights," "generation of income," and "growth of industry," all of which, according to Microsoft, should take precedence over Dr. Villanueva's concerns over access to and permanence of public data, along with his national security concerns. His argument completely trumps that of Microsoft:

> the simple existence of an effective free software tool for a particular IT function would oblige the State to use it; not by command of this Bill, but because the basic principles we enumerated at the start, and which arise from the very essence of the lawful democratic state.[17]

This struggle in Peru is emblematic of similar struggles occurring all over the world. The use of free software has grown steadily for years; it is common in India, China, Africa, Europe, and increasingly in North America. Free software in general, and GNU/Linux in particular, has millions of users. The Free software commons is proving to be very difficult for capital to compete with; Free software has changed the rules of engagement from competition to cooperation. But the revolution of the virtual commons is not limited to the commons itself. We now turn to the content layer, showing the tremendous use the virtual commons has been as a tool in global resistance to neoliberalism.

Resistance and The Value of The Virtual Commons

> The real fruit of [the workers'] battles lies, not in the immediate result, but in the ever expanding union of the workers. This union is furthered by the improved means of communication which are created by modern industry, and which place the workers of different localities in contact with one another.... The bourgeoisie itself, therefore ... furnishes the proletariat with weapons for fighting the bourgeoisie.[18]

It is questionable, and perhaps irrelevant, as to whether Marx could have foreseen the virtual commons and its extraordinary effect on the proletarian resistance to capitalism. But the fact is that Marx describes the effect of the virtual commons upon proletarian struggle almost perfectly. One of the first notable examples of this effect was in the 1994 Zapatista uprising in Chiapas. As Harry Cleaver writes,

> The role of the Internet in the international circulation of the indigenous rebellion in Chiapas developed quickly and has continued to evolve. Early on, the Internet provided a means for the rapid dissemination of information and organization through pre-existing circuits ... primarily at an international level and mostly in computer rich North America and Western Europe. News reports on radio and television were complemented in cyberspace by first-hand

[16]Dee-Ann LeBlanc, "Ending Microsoft FUD: An Interview with Peruvian Congressman Villanueva," *Linux Today*. Online. May 21, 2002.

http://linuxtoday.com/developer/2002052000626INLFPB

[17]Villanueva, "An Open Letter To Microsoft."

[18]Karl Marx and Friedrich Engels, *The Communist Manifesto* (New York: International Publishers, 1999), p. 18-19.

> reports of observers and more analytical commentary by specialists who could voice their opinions and enter into debates more quickly in cyberspace than in other media.[19]

The speed of communication through the virtual commons allows much more efficient and coherent organization and mobilization within any organizational structure that uses it. For the first time, a global infrastructure of communication is available to those struggling against globalization and neoliberalism. Marx's vision of "the ever expanding union of workers" has exploded in the past decade.

This expansion, left unchecked, shows no sign of slowing. In the decade since the Zapatista uprising, much has changed in cyberspace. Millions more computers are in the hands of the people worldwide. The cost of computing has dropped dramatically. Ironically, the accompanying proprietary software bundled with many new computers is often the most expensive component of a new computer system, a compelling illustration of the increasing value of Free software. Internet connections are widely available in many parts of the world; even the Third World is being wired at an exponential rate, often with Free software and secondhand hardware. Broadband connections allow the transfer of multimedia files; independent reporting is no longer limited to text. For instance, less than 24 hours after an aggressive police capture and detainment of peace activists in Portland, Maine, a video documenting the event was posted to the maine.indymedia.org website. There is no top-down hierarchy dominating information flow in the virtual commons; as a result, the organization of the wired anti-globalization movement mirrors the bottom-up architecture of the virtual commons. In a recent paper, James Moore of Harvard's Berkman Center for Internet and Society argued that this emergent collective of individuals is becoming "the second superpower," capable of challenging the global hegemony of the US, precisely because there is no top-down structure to limit its growth:

> What is perhaps most interesting about this global movement is that it is not really directed by visible leaders, but ... by the collective, emergent action of its millions of participants. Surveys suggest that at least 30 million people in the United States identify themselves this way—approximately 10% of the US population. The percentage in Europe is undoubtedly higher. The global membership in Asia, South America, Africa and India, while much lower in percentage of the total population, is growing quickly with the spread of the Internet. What makes the numbers important is the new cyberspace-enabled interconnection among the members. This body has a beautiful mind. Web connections enable a kind of near-instantaneous, mass improvisation of activist initiatives.[20]

One characteristic of capitalism making it especially difficult to overcome is the speed at which capital can evolve and assimilate any attempt to resist it. In this new, wired global movement, organized in the virtual commons, capital has for perhaps the first time faced a movement that can evolve and engage more quickly than itself.

In this movement, memes arise and spread very rapidly; dialogue and discussion catch on like wildfire. This meme pool may be the first true meritocracy in history; ideas spread precisely as quickly as people are moved by and react to them:

> Deliberation in the second superpower is evolving rapidly in both cultural and technological terms. It is difficult to know its present state, and impossible to see its future. But one can say certain things. It is stunning how quickly the community can act—especially when compared to government systems. The Internet, in combination with traditional press and television and

[19]Harry Cleaver, "The Zapatista Effect: The Internet and the Rise of an Alternative Political Fabric," p. 4 of 15. Online. http://www.eco.utexas.edu/faculty/Cleaver/zapeffect.html

[20]James F. Moore, "The Second Superpower Rears Its Beautiful Head," Berkman Center for Internet and Society, Harvard Law School. p. 1-2. Online.
http://cyber.law.harvard.edu/people/jmoore/secondsuperpower.html

> radio media, creates a kind of "media space" of global dialogue. Ideas arise in the global media space. Some of them catch hold and are disseminated widely. Their dissemination, like the beat of dance music spreading across a sea of dancers, becomes a pattern across the community. Some members of the community study these patterns, and write about some of them. This has the effect of both amplifying the patterns and facilitating community reflection on the topics highlighted.[21]

The nature of this global social organization is such that everyone engaged in struggle need not be aware of every single issue; so long as some people advance understanding of a particular issue, the movement as a whole will advance. This principle of emergence could be the missing piece of the puzzle that would enable direct, non-representative democracy to scale up to the global population, bypassing the oppressive concentration of power inherent in a representative democracy:

> There is a method for citizens to self-organize to deliberate on and address complex issues as necessary and enhance ... democracy without any one citizen being required to know and understand the whole. This is the essence of an emergence, and it is the way that ant colonies are able to "think" and our DNA is able to build the complex bodies that we have. If information technology could provide a mechanism for citizens in a democracy to participate in a way that allowed self-organization and emergent understanding, it is possible that a form of emergent democracy could address many of the complexity and scalability issues facing representative governments today.[22]

The virtual commons—as the crowning achievement of the Information Revolution—represents a clear, significant, and growing threat to establishment power structures, both political and economic. If left unchecked, the virtual commons could be the catalyst of the global revolution of the proletariat that Marx predicted. It is becoming increasingly clear, however, that capital recognizes this threat and is responding with its own counter-revolution.

Counter-Revolution: The Rise of the Virtual Enclosures

The structure of the Information Counter-Revolution will be familiar to any careful student of the history of capitalism: the commons is being enclosed. In this case, of course, it is the virtual commons that is being enclosed. These enclosures are being enacted in four ways that concern us here. Three of them have to do with law, or as Lessig describes it, "east-coast code." The fourth has to do with a technological infrastructure —Lessig's "west-coast code"—that will unilaterally enforce these laws, placing every computer under the control of the owners of the software—usually a corporation—running on the computers. First, there is the perpetual extension of copyright duration and the expansion of "intellectual property" laws, recently upheld by the US Supreme Court in the *Eldred v. Ashcroft* case. Second, there are new laws being passed that increase the power of capitalists to control the behavior of people interacting with "intellectual property," in the form of the Digital Millenium Copyright Act. Third, there is the Microsoft monopoly and the anti-trust fiasco. And finally, there is the so called "Trusted Computing Platform Alliance (TCPA)" and the associated "Palladium" mechanism of control over every individual computer. The aim of this section is to make these four aspects of the counter-revolution clear.

We begin with copyright law. On January 15, 2003, the Supreme Court of the United States ruled in the *Eldred v. Ashcroft* case, which "concerns the authority the Constitution assigns to Congress to prescribe the

[21] James F. Moore, "The Second Superpower Rears Its Beautiful Head," p. 4.

[22] Joichi Ito, "Emergent Democracy," p. 6 of 20. Online.
http://joi.ito.com/static/emergentdemocracy.html

duration of copyrights."[23] More specifically, the case sought to overturn the 1998 Sonny Bono Copyright Term Extension Act (CTEA). This act extended the duration of copyright term—both retroactively for existing works and for new works—to the life of the author plus 70 years, or 90 years for works for hire. This act was hardly the first to extend copyright term; at the birth of the United States in 1790, copyright term was 14 years, with the possibility of one 14-year extension if the author was still alive. The attitude of that time toward copyright was clear. Indeed, the US Constitution is specific; it states that copyright must be "for limited times" and that the function of copyright is to "promote the Progress of Science and the useful Arts," not to line the pockets of the intellectual property holders. But the CTEA was not the first such extension of copyright term. In the US, copyright law

> was built upon a constitutional requirement that protection be for limited times, and it was originally limited. Fourteen years, if the author lived, then 28, then in 1831 it went to 42, then in 1909 it went to 56, and then magically, starting in 1962, look—no hands, the term expands. Eleven times in the last 40 years it has been extended for existing works—not just for new works that are going to be created, but for existing works.[24]

Lessig's summary here is the essence of the complaint in *Eldred v. Ashcroft*: by repeatedly extending copyright term, Congress has in practice created a copyright of unlimited term. Each time a term is about to expire, another extension is passed. The CTEA is merely the most recent. As Lessig, who was chief counsel for Eldred, writes in reference to the CTEA:

> Those of us who love it know it as the Mickey Mouse protection act, which of course means every time Mickey is about to pass through the public domain, copyright terms are extended. *The meaning of this pattern is absolutely clear to those who pay to produce it*. The meaning is: no one can do to the Disney Corporation what Walt Disney did to the Brothers Grimm. That though we had a culture where people could take and build upon what went before, that's over. There is no such thing as the public domain in the minds of those who have produced these 11 extensions these last 40 years because now culture is owned.[25]

So not only is the CTEA in violation of the Constitution, the argument goes, but it also is harmful to the public.

The Supreme Court disagreed, ruling 7-2 to uphold the CTEA. The tone of the ruling is dismissive:

> Beneath the facade of their inventive constitutional interpretation, petitioners forcefully urge that Congress pursued very bad policy in prescribing the CTEA's long terms. The wisdom of Congress' action, however, is not within our province to second guess. Satisfied that the legislation before us remains in side the domain the Constitution assigns to the First Branch, we affirm the judgment of the Court of Appeals.[26]

With this one stroke, the existing paradigm of Intellectual Property was upheld, despite the fact that intellectual property is in a state of deep crisis. For example, think of current file-sharing peer-to-peer (p2p) networks such as Napster, Morpheus, Gnutella, and Kazaa. Napster was of course shut down because its architecture was centralized; there *was* a central server that controlled the entire network that could be shut down. The newer networks, however, are much more difficult to stop because there is no central server controlling them. The networks are completely decentralized. Furthermore, these networks have tens of

[23]Justice Ginsberg, opinion of the court, p. 1.

[24]Lessig, "Free Culture," p. 3 of 8.

[25]*Ibid*, emphasis added.

[26]Ginsberg, 32.

millions of users. Though some of the users are not engaged in the illegal trading of unauthorized, copyrighted files, it is clear that many are. One problem is that, given the current architecture of the Internet, copyright law is pragmatically unenforceable; as the Recording Industry is discovering, it is extremely difficult to arrest, prosecute, or sue tens of millions of people, though they are attempting to do exactly that, having already sued hundreds of individuals in an effort to curb p2p file sharing. This is another example of the interests being represented by copyright law; clearly a huge number of people recognize current copyright law as being outmoded or unfair and choose to ignore it. Like so many other areas of law, intellectual property laws are serving corporate interests, not popular interests.

With copyright law being firmly entrenched in the US legal code, the problem shifts to one of enforceability. In the virtual commons, it is quite difficult to protect copyrights. Additionally, any copyright protection mechanism is subject to hacking; there has yet to exist such a mechanism that is not circumventable by creative hackers. To fight this problem, the US Congress also in 1998 passed the Digital Millennium Copyright Act (DMCA), making it a felony not only to circumvent any sort of copy-protection mechanism or copyright management scheme, but also making it a felony to distribute such tools and technologies. Note that this law presupposes an answer to a very important question: is it even possible to technologically enforce copyrights over digital information? Despite the existence of the DMCA, many believe it to be impossible. As Steve Jobs, CEO of Apple, observed, "We have PhDs here who know the stuff cold, and we don't believe it's possible to protect digital content."[27]

This law, of course, has several consequences that are highly questionable, and the history of DMCA enforcement since 1998 amplifies these concerns. According to the Electronic Frontier Foundation (EFF),[28] the DMCA provisions "have been used to stifle a wide array of legitimate activities, rather than to stop copyright piracy"; specifically, the DMCA is being used to "stifle free speech and scientific research," to "unilaterally eliminate the public's fair use rights," and to "hinder ... legitimate competitors" to the copyright holders.[29]

There are several examples that demonstrate these tendencies. Perhaps the best publicized is the Dimitry Sklyarov case.[30] Sklyarov, a Russian programmer working for the company ElcomSoft, was arrested in Las Vegas, Nevada, when he came to the US for the DEF CON conference on electronic security. Sklyarov was

> charged with trafficking in, and offering to the public, a software program that could circumvent technological protections on copyrighted material, under section 1201(b)(1)(A) of the U.S. Copyright Act, which was made law by the 1998 Digital Millennium Copyright Act (the DMCA). He was also charged with aiding and abetting his employer, Russian software development company, Elcom Ltd (a.k.a. ElcomSoft Co. Ltd), to do that.[31]

This questionable software program, ElcomSoft's "Advanced eBook Processor," is a program that converts Adobe's proprietary eBook files into more widely accessible portable document format (.pdf) files. It is a

---

[27]Jeff Goodell, "Steve Jobs: The Rolling Stone Interview," *Rolling Stone* no. 938/939, (Dec. 25, 2003-Jan. 8, 2004): 32. Online.
http://www.rollingstone.com/features/featuregen.asp?pid=2529

[28]http://www.eff.org/

[29]Electronic Frontier Foundation, "Unintended Consequences: Three Years Under the DMCA," p.1 online.
http://www.eff.org/IP/DMCA/

[30]See http://www.freesklyarov.org/ for more information on this case.

[31]Electronic Frontier Foundation, "Frequently Asked Questions (and Answers) About the Dmitry Sklyarov & ElcomSoft Prosecution," Online.
http://www.eff.org/IP/DMCA/US_v_Elcomsoft/us_v_elcomsoft_faq.html#WhyInUS

textbook example of the DMCA in action; though the tool can be used to violate copyright law by converting eBook files into a format which makes them freely redistributable, the program also has legitimate "fair use" applications.

In addition to the question of the validity of the DMCA, this case also presents a problem of jurisdiction. The DMCA is the law of the land in America, but Sklyarov is a Russian citizen; furthermore, the "crime" was committed on Russian soil, where the "crime" is not a crime. Yet as soon as Sklyarov had stepped foot on American soil, he was arrested. As a result, there are many non-American programmers who, as a matter of both principle and self-protection, refuse to set foot on American soil. In the end, after a tremendous amount of "geek" activism and negative publicity for Adobe, Sklyarov and ElcomSoft were acquitted on all counts in late 2002, which provides some optimism about the DMCA as we move into the future.

The DMCA has also been used to stifle scientific research. A good example is the case of Princeton professor Edward Felten. Felten, along with other colleagues, took up the challenge of the Secure Digital Music Initiative (SDMI), who in September, 2000 goaded technologists into attempting to circumvent a digital watermarking scheme they had developed. Felten and his colleagues succeeded in removing the watermarks, and sought to present their findings at an academic conference. When they did so,

> SDMI representatives threatened the researchers with liability under the DMCA. The threat letter was also delivered to the researchers' employers, as well as the conference organizers. After extensive discussions with counsel, the researchers grudgingly withdrew their paper from the conference.[32]

Though the researchers were, after legal action, finally able to present their findings, it is clear that the DMCA impedes scientific progress. An important point is that scientific progress always builds on the past; indeed any scientific researcher, no matter how innovative, is always "standing on the shoulders of giants." But in this case, the giant has managed to throw the innovative thinker off his shoulders. Felten's innovation —which of course could improve the SDMI watermarking process by exposing and articulating a flaw, paving the way for that flaw to be fixed—has been thwarted. Free thought, which also builds on the past, has been denied.[33]

Another casualty of the DMCA is that fair use has been in effect eliminated. Fair use is

> the principle that the public is entitled, without having to ask permission, to use copyrighted works so long as these uses do not duly interfere with the copyright owner's market for a work. Fair uses include personal, noncommercial uses, such as using a VCR to record a television program for later viewing. Fair use also includes activities undertaken for purposes such as criticism, comment, news reporting, teaching, scholarship, or research.[34]

Because the "tools and technologies" that allow fair use can also be used to commit "acts of piracy," they are illegal under the DMCA. Therefore, the DMCA in effect has eliminated fair use in practice. Under the DMCA, "copyright owners can unilaterally eliminate fair use" by eliminating the tools and technologies of fair use. Many of these tools and technologies being repressed have to do with computers and the capabilities enabled by computers. To understand these capabilities, we must take a look at the state of computing today.

---

[32]Electronic Frontier Foundation, "Unintended Consequences," p. 2.

[33]There are many other examples of the negative effects of the DMCA in action; for a good starting point I refer the reader to the EFF and it's excellent essay, "Unintended Consequences: Three Years Under the DMCA."

[34]*Ibid.,* p. 5.

Perhaps the single most important fact about computing over the past few years is the dominance of the Microsoft corporation. They have been declared by the US courts to be a monopoly; indeed, over 90% of personal computers in existence run Microsoft's Windows operating system. In addition, Microsoft Internet Explorer is the dominant web browser, and Microsoft Office is the dominant office suite in use today. Both of these programs also command greater than 90% of their market shares. As a result, an extraordinarily large chunk of the virtual commons is accessed through Microsoft products. This in itself may or may not be a problem, but the fact that Microsoft was declared a monopoly and found guilty of "predatory business practices" to press its advantage to maintain and further its monopoly suggests that something is wrong.

In practice, there are several problems with the way Microsoft does its business. First of all, from the perspective of the computer user, the primary focus of Microsoft is not on what is best for the user, rather it is on extracting as much money as possible from its user base. This is evidenced by its cycle of perpetual upgrades. A decade ago there was Windows3.1. Then Windows95 and WindowsNT came out, followed by Windows98, Windows98SE, WindowsME, Windows2000, WindowsXP, and so on. All of these are essentially updates of the same product, with new features added, some bugs fixed, and inevitably new bugs added. However, Microsoft treats them all as new products, requiring a new purchase. This same problem of perpetual upgrades is also true with Microsoft Office; Office95 gave way to Office97, then to Office2000, and now OfficeXP.

Closed data formats have already been discussed. They impede the flow of information in the virtual commons, because by using these closed data formats, it ensures that all documents using these formats must be accessed through Microsoft products, giving Microsoft some amount of direct control over a staggering amount of information that has been produced in the last 2 decades. Additionally, Microsoft Internet Explorer, which is supposed to access web pages that follow the standardized HTML format, has historically encouraged the use of special, nonstandard pseudo-HTML tags that only work inside Internet Explorer. This is an example of one of Microsoft's problematic practices, "embrace and extend," designed to extend its sphere of influence over the virtual commons. It works by Microsoft products embracing current technologies in existence—often open standards such as the W3C specification for HTML—and then extending these standards with additional functionality that only operate using Microsoft products. And given the dominance of Microsoft's monopoly, these additional "features" become de facto standards, but controlled by Microsoft, and excluding all other software applications in competition with Microsoft.

Another problematic philosophy of Microsoft is their repeated use of "Fear, Uncertainty, Doubt (FUD)" marketing campaigns against competing technologies. This conduct involves sowing seeds of fear, uncertainty, and doubt about potential users straying from the "norm" of Microsoft products, claiming that the world outside of Microsoft is a gamble at best. It reinforces the idea that the only way to go with computing is through Microsoft, despite clear, beneficial alternatives such as those provided by Free software.

Finally, computer security is a very large issue when dealing with networked computers, but the state of security with Microsoft products—most notably Windows and the email program Outlook—is very poor. Indeed, there is an entire industry devoted to providing antivirus software for use with Microsoft products. It is interesting to contrast this situation with Free operating systems such as GNU/Linux; there are very few if any companies or organizations devoted to the development of antivirus software for GNU/Linux. Some assume that this is so because of the relative scarcity of computers running GNU/Linux; however, this is a bad argument because a majority of web servers—the very targets of many security attacks—run GNU/Linux and the Free web server, Apache.

Open source code, it turns out, is highly secure because it allows anyone to inspect the code, spot security flaws, patch the flaws, and release the patches to the community. This is in contrast to the proprietary software philosophy of "security through obscurity," which is organized around the belief that open source

code is itself a security risk, because a potential computer cracker can look at the code and exploit any flaws he or she may find. Though this argument appears to be reasonable, history has shown that it is weak. The openness of Free software turns out to improve security, because any vulnerabilities discovered are quickly closed. The record of security with Free software is overwhelmingly superior to proprietary software. Capital's response to the issue of security is not to emulate the successful, proven techniques in the Free software world. Rather, an infrastructure of control has been conceived and created under the pretense of increased security. This infrastructure, however, has other applications and will indeed make the world safe for draconian intellectual property laws and practices.

The most ominous form of this control is through the so-called "Trusted Computing Platform Alliance" (TCPA) hardware system, along with Microsoft's "Palladium," the software system used to control it. "Trusted Computing" is a mechanism built in to newer computer chips, a mechanism "which Intel referred to as the police state in every computer."[35] The pretense of "Trusted Computing" is computer security; by asserting a centralized system of control over every PC in existence, "Trusted Computing" claims to be able to guarantee the security of those machines. This control consists of a permission system; with applications that use "Trusted Computing," the programmers will be able to control precisely how the content created with that application is used. One obvious application of this system is in Digital Rights Management (DRM), which is an elaborate form of copyright protection. Under "Trusted Computing," for example, Disney would be able to sell you a movie that you could watch on your machine, but not watch on another machine, loan to a friend, or make a backup copy, all of which are normally legal under fair use laws.

In a sense, "Trusted Computing" is a pre-emptive strike against every computer user, regardless of whether each individual user is a breaker of copyright law. Rather than waiting for a "smoking gun" in terms of copyright violations, "Trusted Computing" removes from the gun the capacity to smoke, taking much of the functionality of the gun along with it. In other words, the baby is thrown out with the bathwater; by removing the capacity of a machine to be used to commit "illegal" acts, the right to commit legal acts using that same technology is also removed. The presupposition is that anything that *can* be used to break the law—even if it has legal uses—should not be allowed. Therefore, the reasoning goes, all computer activities should not be allowed, unless each act is given explicit permission by the software's creators. The key point is that under "Trusted Computing," everything that can normally be done on a computer can only be accomplished with these proper "permissions" which are encrypted and are not accessible to the user. Using this technology, the computer will be programmed to automatically take certain actions neither requested nor authorized by the user. For example, a computer could scan itself for any "unapproved" software or data at bootup, and automatically delete such files without consulting the owner of the computer. If a friend sends a file—say, a Microsoft Word document—that does not have explicit permission embedded in the file to run on Microsoft Word, then your copy of Microsoft Word could refuse to load it, leaving one powerless to access the "unapproved" data. In effect, the computer will no longer obey its owner or user, but rather it will obey those who wrote the software running on the computer. As Richard Stallman—who refers to "Trusted Computing" as "treacherous computing"—explains:

> The technical idea underlying treacherous computing is that the computer includes a digital encryption and signature device, and the keys are kept secret from you. (Microsoft's version of this is called "palladium.") Proprietary programs will use this device to control which other programs you can run, which documents or data you can access, and what programs you can pass them to. These programs will continually download new authorization rules through the Internet, and impose those rules automatically on your work. If you don't allow your computer

[35]Lawrence Lessig, "Free Culture," Keynote Address, Open Source Convention, 2002, p. 6 of 8. Audio recordings of speech are online at http://lessig.org/freeculture/. Text transcription of speech archived at http://www.oreillynet.com/pub/a/policy/2002/08/15/lessig.html.

> to obtain the new rules periodically from the Internet, some capabilities will automatically cease to function.[36]

When "Trusted Computing" is widely implemented and adopted—a process that is hardly guaranteed, depending on popular awareness and the mobility of opposition to it—central control of every machine that connects to the Internet will be a reality. An infrastructure of control will be in place to enforce the increasingly strict intellectual property laws being passed. As Lessig has argued, we are not far from a future

> where to use an idea, to criticize a part of culture, to quote "Donald Duck," one will need the permission of someone else. Hat in hand, deferential, begging, a society where we will have to *ask* to use; *ask* to criticize; *ask* to deploy; *ask* to read; *ask* to browse; *ask* to do all those things that in a free society—a society where no one man, or no corporation, or no soviet, controls—one takes for granted.[37]

Another problem with the "Trusted Computing" system is that there is no limit to its use by those in control of it, namely, the corporations that own the proprietary programs employing "Trusted Computing" technology.[38] For example, as the US government gets more and more aggressive in its restriction of civil rights in its so-called "war on terrorism," it would be trivial to force Microsoft to use "Trusted Computing" code in Windows to identify "unauthorized" or "objectionable" content that could be characterized as "terrorist activity." Such a maneuver is neither fantastic nor far-fetched; the US government has already imposed control over some Internet communications such as email through the so-called "USA-PATRIOT Act," and it is likely to extend this control through any available infrastructures in place. Complete control over computers through this infrastructure would hamper any community opposed to neoliberal expansion of capital, including all forms of activist movements such as the Free software movement and the peace movement. This control—the creation and enforcement of the virtual enclosures—is the Information Counter-Revolution. And if the counter-revolution is left unchecked, it will trump the gains made via the virtual commons and the Information Revolution.

The Enclosure of Ideas: Pre-emptive First Strikes in the War on Thinking

But the Counter-Revolution's effects on the peace movements and anti-globalization movements are only the beginning. To understand the full scale of the threat of the virtual enclosures, we must understand the effects of the previous enclosure movements in history. All these effects are variations on the same theme:

> Most people can find in their genealogy or in their own lives some point where their ancestors or they themselves were forced from lands and social relations that provided subsistence without having to sell either one's products or one self, i.e., they suffered *Enclosure*. Without these moments of force, money would have remained a marginal aspect of human history. These moments were mostly of brutal violence, sometimes quick (with bombs, cannon, musket, or whip), sometimes slower (with famine, deepening penury, plague), which led to the terrorized flight from the land, from the burnt-out village, from the street full of starving or

[36]Richard Stallman, "Can You Trust Your Computer?" in *Free Software, Free Society: Selected Essays of Richard M. Stallman* (Cambridge, Mass.: GNU Press, 2002). Essay available online. http://www.gnu.org/philosophy/can-you-trust.html

[37]Lawrence Lessig, "Reclaiming a Commons," p. 7.

[38]It is interesting how this battle over TCPA underscores the importance of the Free software paradigm as an opposition to corporate, proprietary software. It is questionable to give so much control over one's computer and one's data to a huge corporation with only one interest in mind: extracting as much profit from its user base as possible.

> plague-ridden bodies, to slave ships, to reservations, to factories, to plantations. This flight ended with "producers becoming more dependent on exchange" since they had no other way to survive but by either selling their products or selling themselves or being sold. Thus did "exchange become more independent of them, its transcendental power arising from the unreserved violence that drove "everyone" into the monetary system.[39]

There are for our purposes several points to consider about Enclosure. First, they are based on *force*. People are *forced* into a situation they do not want to be in. Second, this force separates people from their independent means of subsistence. Because newly-enclosed land has an "owner," the resources of that piece of land are no longer accessible in common, despite the fact that access to land is necessary for survival; the abstract notions of "property" and "profit" overrule even the basic human need for survival. Third, access to the enclosed resource is mediated through money; that is, people are forced to buy that which they once held in common. So not only do the land owners control the means of subsistence, but also they are placed in a power relationship over those who want to buy access to the enclosed property—access which remains essential to survival. Though the Enclosure movement represents the genesis of capitalist society, Enclosure did not stop at that moment. As Midnight Notes has argued, Enclosures

> are not a one time process exhausted at the dawn of capitalism. They are a regular return on the path of accumulation and a structural component of class struggle. Any leap in proletarian power demands a dynamic capitalist response: both the expanded appropriation of new resources and new labor power and the extension of capitalist relations, or else capitalism is threatened with extinction.[40]

So a further point to realize is that Enclosure represents a standard response of capital when its dominion is threatened.

Fast forward a few hundred years. The process of capitalist accumulation has grown to include "intellectual property"—literally, that ideas are now owned and are therefore exploitable and controllable by capital. The Virtual Enclosures, if they follow the same pattern of enclosure demonstrated time and again in the history of capitalist accumulation, will seek to enclose ideas (the stuff of intellectual property) from the common, preventing people from using the enclosed property without payment. While the concept of property has always been abstract and arbitrary, in the virtual enclosures the property *itself* is abstract and arbitrary.

The nature of the intellectual property culture is to presuppose answers to the most important and fundamental epistemological and metaphysical questions that have puzzled philosophers for thousands of years: what are ideas? Where do ideas come from? What is the nature of consciousness? The movement of capital into this new region of "virtual reality" only further exposes its illusory and arbitrary nature. Philosophers, psychologists, physicists, neurosurgeons, biologists, and theologians aren't even sure what ideas, thoughts, and consciousness are, yet they can be owned and, through the virtual enclosures, their use forbidden without payment.

How is this possible? Is there a way to forbid ideas without payment? As technology advances, the answer seems to be yes. We are not far from a future where the mere expression of an enclosed idea in a computer-mediated communication such as email would automatically deduct a fee from the thinker's credit card account. Copyright law has more or less thrown fair use out the window, replacing it with a system of centralized control. This change, as Lessig argues, is already happening with the Internet:

---

[39]George Caffentzis, "The Power of Money: Debt and Enclosure," *The Commoner*, N.7. Spring/Summer 2003, p. 2. Online. http://www.thecommoner.org/.

[40]Midnight Notes Collective, "The New Enclosures," *Midnight Oil: Work, Energy, War, 1973-1992* (NY: Autonomedia, 1992) p. 38.

> We are far enough along to see the future we have chosen. In that future, the counter-revolution prevails. The forces that the original Internet threatened to transform are well on their way to transforming the Internet. Through changes in the architecture that defined the original network, as well as changes in the legal environment within which that network lives, the future that promised great freedom and innovation will not be ours. The future that threatened the reemergence of almost perfect control will.[41]

Though Lessig is pessimistic, he is perhaps not pessimistic enough, for his scope of vision does not take into account the Enclosure movements in the history of capitalism. There is simply no reason to believe that once technology allows centralized monitoring of the very thought processes of individuals that capital, with its arsenal of intellectual property laws and mechanisms of control to enforce them, will jump at the chance to to extract payment from the act of thinking. But even if such control never happens, the destruction of fair use and the imposition of tighter controls threaten to transform thinkers of enclosed thoughts into criminals.

It is interesting to consider how the definition of "piracy" has changed in the past two decades. It is indicative of the success of capital in framing the intellectual property debate so narrowly that the term "piracy"—which once meant forced entry to a ship, armed robbery, rape, and murder, leaving nothing behind but corpses and flaming hulls of ravaged ships—is now reserved for those who share. If people who share ideas can be transformed into vicious criminals, why not people who think ideas?

To a 16th-century peasant, it was inconceivable that the land itself would be off limits to them. To Native Americans, the very idea that land could be owned was inconceivable. The Earth was a commons, available to all to use for their sustenance. Likewise, a person today may think it inconceivable that the vast spectrum of thought—the realm of all possible ideas—could be closed off to them. But given the mechanisms of centralized control being architected into our information infrastructure, given the historical pattern of capital's behavior in previous enclosure movements, and given the amount of "profit" at stake in the areas of Intellectual Property—from the entertainment industry to human genome research—one must conclude that these owned ideas, like the vast tracts of farmland 400 years ago, will also be enclosed from the common so that its owners may exploit it, extracting as much profit as possible in the brutal efficiency of the capitalist system.

The outlook from this perspective is indeed bleak. However, this outlook is not yet fact; there will be history between now and then. Furthermore, there is additional evidence suggesting that Lessig's conception of the problem is too narrow, and therefore that his pessimism may be misplaced. Perhaps the single most important fact about the Virtual Enclosures is that from a global perspective, cyberspace and the virtual commons are currently accessible to only a tiny minority. Lessig's lament may indeed describe the current situation in the United States. However, the virtual commons is undergoing a process of internationalization. These countries, many of which are poor, have experience resisting enclosure, structural adjustment, and other aggressive tactics of capital.

Recent events in Cancun bode well for the future of this struggle. The success of the G22 in holding their ground at the negotiating table, nudging the world's attention toward the imbalance of power inherent in the neoliberal economic climate, suggests that capital may be nearing its limits in terms of its ability to impose itself upon an unwilling population. The world, embodied by the G22 which represents the majority of the world population, is speaking in a clear voice. As Arundhati Roy noted,

> For all these reasons, the derailing of trade agreements at Cancun was crucial for us.... What Cancun taught us is that in order to inflict real damage and force radical change, it is vital for

[41]Lawrence Lessig, *The Future of Ideas*, xxi-xxii.

> local resistance movements to make international alliances. From Cancun we learned the importance of globalizing resistance.[42]

The virtual commons, I have argued, is a crucial element in the process of "globalizing resistance." Empire is, of course, resisting this process; in response they are imposing the virtual enclosures. Information infrastructure is a key battleground in the struggle against neoliberalism, and even today the dominance of proprietary software and closed standards in fortifying the virtual enclosures is troubling. But there is an alternative. Globalized resistance can still organize itself within the virtual commons, strengthening both itself and the commons the more it is used and its fundamental values as a commons (no one owns it, everyone can use it, anyone can improve it) are embraced, celebrated, and foregrounded in the dialogue within globalized resistance. The G22 countries, and indeed most of the countries of the world, are just coming in to the global, wired picture. These countries bring with them their vast populations. This fact—that the rate of adoption of the Internet is continuing to grow, especially in the Third World—is perhaps the single largest reason for optimism. Using the Free software and open standards of the virtual commons over the proprietary software and closed standards of the virtual enclosures is increasingly sensible; therefore, more and more of these new netizens will come in on the side of the virtual commons. Our numbers—and the power of globalized resistance to fight enclosure—can only increase.[43]

[42]Arundhati Roy, "The New American Century," *The Nation,* February 9, 2004. Online. http://www.thenation.com/doc.mhtml?i=20040209&s=roy