

Attenzione: il presente testo è una bozza dell'articolo omonimo pubblicato nella versione cartacea della Rivista Scientifica "Cyberspazio e Diritto" (<http://www.cyberspazioediritto.org>). Si tratta di una BOZZA: può quindi contenere differenze e, soprattutto, imprecisioni, inesattezze o refusi che sono stati poi corretti all'atto della correzione delle bozze e della messa in stampa dell'articolo. Si consiglia, pertanto, di riferirsi, nelle citazioni, esclusivamente all'articolo pubblicato a stampa. Il riferimento dell'articolo che segue *Censorship 2000*, John Perry Barlow, in *Cyberspazio e Diritto*, 2000, Volume I, Numero III, pp. 477-496. Articolo tratto dal sito <http://www.cyberspazioediritto.org>

## Censorship 2000

John Perry Barlow<sup>1</sup>

*The Internet treats censorship as though it were a malfunction and routes around it.*

*John Gilmore*

When Electronic Frontier Foundation (EFF) co-founder John Gilmore stood before the Second Conference on Computers, Privacy, and Freedom and uttered those brave words, I believed them. I'm not certain I still do.

Of course, they remain true to the extent that cyberspace exists in an end-to-end data cloud through which any packet may travel to its address by multiple, unfiltered routes. But increasingly, those routes are being channeled and filtered, while their origins and ends get monitored and placed under legal constraint.

That the Internet's original absence of predetermined information circuits and central switches had political implications was, for some of its many fathers, a feature with intended social consequences. I once asked one of them if he had simply been thinking of designing a system that couldn't be decapitated by nuclear attack. «I can't speak for the others» he said, «but I was thinking of a system that didn't have a head». He knew, as Mitch Kapor subsequently and succinctly put it, that «architecture is politics».

Despite concerns over the combination of governmental zeal and cluelessness that led to the founding of EFF in 1990, I was a strong believer in the notion that the architecture of the Internet would always resist censorial control.

But of course, any sensible person knew even then that the great Powers That Were - meaning, the dominant forces of the industrial era - were not likely to stand idly by while their ability to control information within their areas of authority melted in the Net-borne solvent of anarchic packets. Too much was at stake.

It is true that information is power. But, more to the point, power is information. For most of the history of humanity, the primary method of asserting power, aside from force of arms, has been by the control of information. Of the many revolutions

---

<sup>1</sup> Il presente saggio è stato scritto dall'Autore per la pubblicazione di ISOC ([www.isoc.org](http://www.isoc.org)) On the Internet ed è pubblicato anche su *Cyberspazio e Diritto* per espressa volontà dell'autore stesso.

Attenzione: il presente testo è una bozza dell'articolo omonimo pubblicato nella versione cartacea della Rivista Scientifica "Cyberspazio e Diritto" (<http://www.cyberspazioediritto.org>). Si tratta di una BOZZA: può quindi contenere differenze e, soprattutto, imprecisioni, inesattezze o refusi che sono stati poi corretti all'atto della correzione delle bozze e della messa in stampa dell'articolo. Si consiglia, pertanto, di riferirsi, nelle citazioni, esclusivamente all'articolo pubblicato a stampa. Il riferimento dell'articolo che segue Censorship 2000, John Perry Barlow, in *Cyberspazio e Diritto*, 2000, Volume I, Numero III, pp. 477-496. Articolo tratto dal sito <http://www.cyberspazioediritto.org>

to be wrought by the Internet, the most profound lies in its long-term capacity to degauss all of the local reality distortion fields the mighty have spun among their subjects.

Now, all over the planet, the mighty have awakened to the threat the Internet poses to their traditional capacities for information control. As a consequence, even a thin summary of the institutions currently struggling to control online information distribution - as well as the nature of their specific immune responses - would fill a thick book. There is suddenly a global epidemic of virtual censorship.

### *The Censors and Their Excuses*

Generally, the entities that currently aspire to edit collective human consciousness fall into the following broad categories.

Nation-states

Local governments

Corporations

Religions

Cultural groups

One-to-many information distributors and other legacy media

Individual information 'owners'.

This would seem to be a diverse list, but my own sense-developed out of years of battling various aspiring Net censors is that once one has stripped away the superficial particularities of each censorial initiative, there remains one motivation: the retention of power and wealth by the traditionally rich and powerful.

It also seems that efforts to suppress material on the Internet come from without - largely on the part of institutions and constituencies that formed before the creation of cyberspace - and have little direct experience in the virtual environment. With one notable exception - those who would ban electronic junk mail - 'indigenous' digital culture seems to have a naturally libertarian disposition.

Examination of the various pretexts for proscribing information shows that they fall into several broad categories, most of them intentionally difficult to defend against. They are:

Protection of children from exposure to sexual or violent material

Prevention of the exploitation of children in the production of child pornography by banning its distribution

Political suppression of marginal groups - whether they be neo-Nazis in Germany or women in Saudi Arabia

Defense of national or commercial security - by preventing distribution of encryption, decryption, or hacking software

Attenzione: il presente testo è una bozza dell'articolo omonimo pubblicato nella versione cartacea della Rivista Scientifica "Cyberspazio e Diritto" (<http://www.cyberspazioediritto.org>). Si tratta di una BOZZA: può quindi contenere differenze e, soprattutto, imprecisioni, inesattezze o refusi che sono stati poi corretti all'atto della correzione delle bozze e della messa in stampa dell'articolo. Si consiglia, pertanto, di riferirsi, nelle citazioni, esclusivamente all'articolo pubblicato a stampa. Il riferimento dell'articolo che segue Censorship 2000, John Perry Barlow, in *Cyberspazio e Diritto*, 2000, Volume I, Numero III, pp. 477-496. Articolo tratto dal sito <http://www.cyberspazioediritto.org>

Protection of governments, corporations, and religions from destabilizing, inflammatory, or embarrassing expressions by dissidents, whistle-blowers, and turncoat insiders

Limiting of the exposure of a certain culture to the expressions of another it finds offensive, as well as access to those organizations that defend such expressions

Disarming of terrorists by preventing online distribution of information about explosives or weapons manufacture and acquisition

Reduction of the flow and consumption of illegal drugs by banning information regarding their production or by banning positive statements about their effects

Prevention of communication among criminals, particularly hackers, terrorists, and drug distributors

Protection of governments and companies from the damaging revelation of state or trade secrets

Protection of privacy by regulating the exchange of personal information

Restraint on the distribution of unsolicited solicitations, or spam

And, increasingly,

Prevention of the noncommercial distribution of copyrighted material, or what used to be called fair use

As I say, most of these goals have broad popular appeal, whether universally or locally. Almost no one on the planet is going to gladly proclaim the rights of kiddy pornographers, terrorists, neo-Nazis, drug lords, spammers, or hackers. Within narrower contexts, suppressing the expressions of gays, women, heretics, traitors, and troublemakers is politically popular.

Indeed, despite the lip service that is paid to freedom of expression in most parts of the world, people are generally inclined to defend only the expressions of others like themselves, failing to recognize that, in the words of John Stuart Mill, «Liberty resides in the rights of that person whose views you find most odious».

There has also been, in recent years, a widespread conceptual-and often legal-conflation of images with acts, depictions with deeds. For many, it is not sufficient that misuse of children is illegal. They contend that graphic expressions of such misuse must also be prohibited, including those artificially generated images that involve no actual children at all. By the same token, describing how to make a bomb is seen to be the same as detonating one, detailing the weaknesses of a computer system is as heinous as breaking into one, and so forth.

Furthermore, very few policymakers are sufficiently Internet savvy to recognize that when they attempt to regulate what may be expressed online, they are 'thinking locally and acting globally', imposing their legal will on people far beyond their jurisdictions. Often, their own constituents are as unaware of the online world as they are. Thus, for example, the wildly unconstitutional Communications Decency Act (CDA) was able to be enacted by the U.S. Congress by a lopsided margin - to the apparent satisfaction of an electorate that was still largely offline.

Attenzione: il presente testo è una bozza dell'articolo omonimo pubblicato nella versione cartacea della Rivista Scientifica "Cyberspazio e Diritto" (<http://www.cyberspazioediritto.org>). Si tratta di una BOZZA: può quindi contenere differenze e, soprattutto, imprecisioni, inesattezze o refusi che sono stati poi corretti all'atto della correzione delle bozze e della messa in stampa dell'articolo. Si consiglia, pertanto, di riferirsi, nelle citazioni, esclusivamente all'articolo pubblicato a stampa. Il riferimento dell'articolo che segue Censorship 2000, John Perry Barlow, in *Cyberspazio e Diritto*, 2000, Volume I, Numero III, pp. 477-496. Articolo tratto dal sito <http://www.cyberspazioediritto.org>

While it is unlikely that a similar bill could be passed by Congress today without an outcry from a much more wired public, there are many parts of the world where the online communities constitute as small a percentage of the population as obtained in the U.S. when the CDA passed.

In technologically sophisticated areas, censorial legislators are now using speed, stealth, and obfuscation to pass suppressive laws that would probably encounter stiffer opposition were the public aware of their implications. As I write these words, Congress is rushing to pass something called the Methamphetamine Anti-Proliferation Act. This bill would not only ban any online discussion of methamphetamine manufacture but also would criminalize positive statements about the use of methamphetamine and many other drugs, including marijuana. Few are aware of this bill, fewer are aware of its provisions, and, with a name like that, very few indeed are likely to publicly oppose it.

There have been a number of laws recently passed to serve the interests of institutional copyright holders. These laws have, in my opinion, grave consequences for the free flow of ideas. Very few citizens are aware of the chilling implications of, say, the Digital Millennium Copyright Act, which essentially eliminates fair use in digital media.

Other, related laws-in the U.S. and elsewhere-turn copyright violations into criminal acts, greatly lengthen the term of copyright, and generally extend to institutions of various sorts the ability to censor by asserting ownership. For example, Microsoft Corporation is currently forcing the removal from Slashdot.com of embarrassing revelations about the security weaknesses of its software on the grounds that some of these postings quote internal documents that Microsoft owns.

This is but the latest in a series of cases in which an institution has used intellectual property law to censor material it finds offensive, but I will defer for a moment a discussion of the larger relationship between current developments in copyright law and digital freedom of expression.

### The Emperor's new clues

I would continue to be sanguine about this global outbreak of legislative and regulatory bit-blockage, maintaining my faith in the ability of the Net to route around it - and, more important, in the persistent cluelessness of the oppressive - but I find that the forces of control have become more sophisticated. No longer can we assume that we will be spared their tyranny by their incompetence. They're getting smarter, and, moreover, they are being aided by various forces that, while they may be motivated more by commerce than morality, are creating systems that can serve either agenda equally well.

Currently successful or promising methods of censorship, whether by governments, organizations, or cultural zones, include the following.

Attenzione: il presente testo è una bozza dell'articolo omonimo pubblicato nella versione cartacea della Rivista Scientifica "Ciberspazio e Diritto" (<http://www.ciberspazioediritto.org>). Si tratta di una BOZZA: può quindi contenere differenze e, soprattutto, imprecisioni, inesattezze o refusi che sono stati poi corretti all'atto della correzione delle bozze e della messa in stampa dell'articolo. Si consiglia, pertanto, di riferirsi, nelle citazioni, esclusivamente all'articolo pubblicato a stampa. Il riferimento dell'articolo che segue Censorship 2000, John Perry Barlow, in Ciberspazio e Diritto, 2000, Volume I, Numero III, pp. 477-496. Articolo tratto dal sito <http://www.ciberspazioediritto.org>

### *Blocking of access.*

According to a recent report by Leonard R. Sussman, senior scholar at Freedom House, a New York-based human rights organization, at least 20 countries - including Cuba, Iraq, Myanmar, and North Korea - thoroughly restrict their citizens' access to the Internet. While this will likely change as satellites make the Internet available to anyone with a small dish in the attic, many of these same governments also restrict access to digital hardware in general.

In Myanmar, merely having possession of an unregistered computer can draw a 20-year jail sentence. Meanwhile, the government of Kazakhstan is studying Myanmar's laws and is expected to emulate them.

Many countries are also seeking to turn telecommunication carriers and Internet service providers (ISPs) into the content cops of the Internet. For example, the Swiss Federal Police Bureau recently proposed setting rules aimed at controlling racist and pornographic material on the Internet as well as at keeping organized crime and white-collar crime offline. Under the proposed rules, Swiss Internet service providers would be required to block their customers from accessing any sites proscribed by Swiss authorities.

Even placing the telecoms and ISPs in charge of controlling access may not be terribly effective, since proscribed material may be easily transferred to new sites - in a digital shell game that is faster than the observational capacities of the censors. Consider, for example, the explosive proliferation of international sites carrying the German magazine Radikal after the German government prohibited it on any site within Germany's borders. No German ISP could have kept up with the growth of new-and often disguised-repositories of Radikal.

### *Global cybercrime accords.*

In the Radikal case, freedom was preserved by the inability of the German government to effectively extend its authority beyond its borders. This seems about to change. Using the recent outbreak of the love bug virus as their justification, the Group of Eight industrial nations convened a mid-May conference in Paris to create, according to French interior minister Jean-Pierre Chevènement, «a world convention on cybercrime and to harmonize their laws to crack down on hackers, virus writers, software pirates, and other Internet fraudsters».

Chevènement and others attending the three-day conference called for an international cyberregime, consisting of governmental and corporate institutions that would prevent the creation of safe zones for 'illicit content or criminal activities' on the Internet.

Attenzione: il presente testo è una bozza dell'articolo omonimo pubblicato nella versione cartacea della Rivista Scientifica "Cyberspazio e Diritto" (<http://www.cyberspazioediritto.org>). Si tratta di una BOZZA: può quindi contenere differenze e, soprattutto, imprecisioni, inesattezze o refusi che sono stati poi corretti all'atto della correzione delle bozze e della messa in stampa dell'articolo. Si consiglia, pertanto, di riferirsi, nelle citazioni, esclusivamente all'articolo pubblicato a stampa. Il riferimento dell'articolo che segue Censorship 2000, John Perry Barlow, in *Cyberspazio e Diritto*, 2000, Volume I, Numero III, pp. 477-496. Articolo tratto dal sito <http://www.cyberspazioediritto.org>

«It is time», said Chevenement-in a phrase that should quicken aging hearts everywhere - «to restrain the excesses of an unfettered freedom» in cyberspace. G8 leaders are expected to take up the conference's recommendations at their annual meeting in July in Okinawa, Japan.

But of course, the love bug was especially frustrating because it originated in the Philippines, a country that has no laws covering illicit computer behavior. Thus, the industrial powers are suddenly eager that the authorities in technologically unsophisticated nations put into place laws, enforcement systems, and information prohibitions that those authorities themselves may not understand.

I have heard numerous reports recently from developing nations that the G8 nations - most notably the United States - are pushing hard for the passage of stern cybercrime laws as well as for the installation of radical new surveillance technologies. One of these, recently seen on sale at a cybercrime meeting in Norway, would enable law enforcement officials to implant undetectable Trojan horses in e-mail attachments that, once in place, could scan for any proscribed activity and make clandestine reports to the authorities every time the user went online.

Of course, once a government has put such granular cybercrime detection systems into place, the systems may be easily put to the task of looking for any material that might be deemed offensive. Worse, if the American government prevails in its efforts, it will install a global system for censorship so that no country could provide safe haven for any kind of information that discomforts certain stiff old men in Washington.

### *Filtering*

It is a great irony that the Platform for Internet Content Selection (PICS) standard, upon which most filtering is based, was originally devised to ward off government censorship by enabling families to filter out material they deemed inappropriate for their children. It was not anticipated that such 'families' as the People's Republic of China, large corporations, or embattled public libraries would find it equally useful. In any instance in which Internet traffic into and out of an area can be constrained to one channel, that channel can be filtered to pass only expressions considered inoffensive by those who control the channel.

Often, the determination of what is appropriate is made not by the authority imposing the filter but by the commercial creator of the filtering software. Most of the providers of such software don't reveal what sites are actually being blocked by their filters, thereby proscribing more than their customers may wish. In addition to blocking pornography, for example, many commercial filters also block access to Web sites that promote free expression.

Ratings systems. A particularly insidious new form of censorship is being developed in Europe in the form of a system that would classify and rate Web sites according to

Attenzione: il presente testo è una bozza dell'articolo omonimo pubblicato nella versione cartacea della Rivista Scientifica "Cyberspazio e Diritto" (<http://www.cyberspazioediritto.org>). Si tratta di una BOZZA: può quindi contenere differenze e, soprattutto, imprecisioni, inesattezze o refusi che sono stati poi corretti all'atto della correzione delle bozze e della messa in stampa dell'articolo. Si consiglia, pertanto, di riferirsi, nelle citazioni, esclusivamente all'articolo pubblicato a stampa. Il riferimento dell'articolo che segue Censorship 2000, John Perry Barlow, in *Cyberspazio e Diritto*, 2000, Volume I, Numero III, pp. 477-496. Articolo tratto dal sito <http://www.cyberspazioediritto.org>

whether or not they contain potentially offensive sexual, political, or violent material. The rating initiative is being driven by the Bertelsmann Group with legal assistance from Yale Law School. According to its proponents, the ratings system would ward off official censorship by setting up a system of 'voluntary' standards for evaluating the material Web publishers may place on their sites, in much the same way that film ratings by the Motion Picture Association of America have prevented government censorship of American movies.

The analogy is unfortunate. While it may be possible to set standards for American movies within the cultural standards of the United States, the Internet is a global communications environment. What might be an offensively explicit sexual site under American or Saudi Arabian standards might be considered quite tame in Sweden. By the same token, Americans are quite comfortable with depictions of violence that would be considered excessive almost everywhere else in the world.

Furthermore, once sites have begun to rate themselves, it is a simple matter for censors of whatever sort to make compulsory what might remain voluntary elsewhere. The well-intentioned designers of the proposed ratings systems would do well to study the lessons of PICS in this regard.

Finally, in accordance with the ever-useful follow-the-money rule, I think it worth nothing what entities are driving the filtering initiative. They are the major old media, Eurocrats, Yale, and other artifacts of the industrial period. Whether wittingly or not, they may be using ratings as a means of prolonging their attenuating longevities. That is, the use of ratings systems naturally drives expression toward traditional forms that fit easily into the categories being designed by those who are paying for their development. CNN.com is easy to rate. But what about Slashdot.com?

#### *Alteration of the architecture.*

Back in the days when the technical architecture of the Internet was being designed by the Internet Engineering Task Force (IETF), we could take comfort in the essentially libertarian culture of that 'technarchy'. Their decisions, motivated by a sense of engineering elegance as well as by a desire to see that packets flowed as freely and swiftly across cyberspace as possible, resulted in the end-to-end system that has so successfully resisted censorial control to this point. Most of them were academics and were thus free to serve their personal consciences rather than the economic goals of their employers.

This is now changing. Increasingly, the members of the IETF, of the World Wide Web Consortium, of the newly formed Internet Corporation of Assigned Names and Numbers (ICANN), and of other standards-setting bodies represent so-called stakeholders-corporate entities from the Internet industry-rather than individual Netizens or objective engineers and scientists.

Attenzione: il presente testo è una bozza dell'articolo omonimo pubblicato nella versione cartacea della Rivista Scientifica "Cyberspazio e Diritto" (<http://www.cyberspazioediritto.org>). Si tratta di una BOZZA: può quindi contenere differenze e, soprattutto, imprecisioni, inesattezze o refusi che sono stati poi corretti all'atto della correzione delle bozze e della messa in stampa dell'articolo. Si consiglia, pertanto, di riferirsi, nelle citazioni, esclusivamente all'articolo pubblicato a stampa. Il riferimento dell'articolo che segue Censorship 2000, John Perry Barlow, in *Cyberspazio e Diritto*, 2000, Volume I, Numero III, pp. 477-496. Articolo tratto dal sito <http://www.cyberspazioediritto.org>

In their quest for market share, corporations are naturally motivated to pursue standards that will direct traffic through their networks, servers, or operating systems. In each of these areas, troubling monopolies have formed. More than 80 percent of all of the routers in the world are made by Cisco Systems. Nearly half of all the servers on the Internet run Microsoft NT. A very high percentage of all packets travel through networks owned by WorldCom/MCI or AT&T. Despite the emergence of ICANN, Network Solutions continues to dominate top-level domain-name registration.

Any one of those companies is now in a position to unilaterally redefine the underlying elements of Internet architecture to its own commercial advantage. For example, if Microsoft decided to 'extend and improve' the TCP/IP protocol so that Microsoft-'flavored' packets flowed more swiftly through NT servers, the resulting commercial advantage would eventually put Bill Gates in a position of control over the flow of information. Given Microsoft's current efforts to censor expression on Slashdot.com, this is not a power I would care to entrust to him.

Meanwhile, pioneer Internet architect David Reed recently brought to my attention a Wall Street Journal article describing a new Internet consortium composed of Nortel Networks, AT&T, Qwest Communications International, Sun Microsystems, BT, and NBC that is setting standards for broadband networks. According to the article, «Part of the group's planned technology would enable high-bandwidth networks to identify the Web user». The resulting opportunities for censoring the expressions of such users are obvious.

This is only one of many initiatives that would move us away from the end-to-end, packet-switched model-the model to which John Gilmore referred in his quote at the beginning of this article-and toward a circuit-switched network rather like the phone system the Internet is replacing.

While the goals of these initiatives may be well-intentioned-real-time video interactions, reductions in latency to serve voice-over Internet protocol-the eventual effect likely could be the conversion of the data cloud into a complex of predetermined routes that would be easily monitored and censored either by those who operated them or by the governments within whose jurisdictions they operated. The problem is that all of these potential threats are of a highly technical nature and are being discussed in forums and formats that may be inaccessible to those most concerned with protecting their future liberties. Nevertheless, it is incumbent on those of us who want to pass on to our descendants a free cyberspace that we maintain an awareness of the decisions being made by these new corporate Internet architects.

*Surveillance and fear.*

Attenzione: il presente testo è una bozza dell'articolo omonimo pubblicato nella versione cartacea della Rivista Scientifica "Cyberspazio e Diritto" (<http://www.cyberspazioediritto.org>). Si tratta di una BOZZA: può quindi contenere differenze e, soprattutto, imprecisioni, inesattezze o refusi che sono stati poi corretti all'atto della correzione delle bozze e della messa in stampa dell'articolo. Si consiglia, pertanto, di riferirsi, nelle citazioni, esclusivamente all'articolo pubblicato a stampa. Il riferimento dell'articolo che segue Censorship 2000, John Perry Barlow, in *Cyberspazio e Diritto*, 2000, Volume I, Numero III, pp. 477-496. Articolo tratto dal sito <http://www.cyberspazioediritto.org>

It is often unnecessary to restrict access to the Net or to filter it in order to suppress both free expression and contact with it. There are innumerable current examples of efforts—official and private—to monitor Internet traffic. These include everything from the National Security Administration's Echelon project to current efforts by Britain's MI5 and Home Office to monitor all e-mail in the United Kingdom, to Metallica's compiling a list of all Napster users who have digitized copies of its songs. While the Internet greatly enables private communications, the fact that all of cyberspace is subject to automatic and rapid search makes it one of the most easily surveilled environments humans have ever inhabited.

It might be argued that surveillance and censorship are separate matters, but they are not. As Louis Brandeis pointed out in his historic dissent in *U.S. v. Olmstead*, the case that enabled wiretapping in the United States, the ability to communicate privately and without fear is essential to ensure freedom of expression. The mere possibility that one's words are being secretly monitored by censorial authorities produces a climate of fear.

The area in which this form of censorship is used most often and effectively is in the workplace. Slightly over half of American companies now routinely monitor their employees' e-mail, Web surfing, or both. One might argue that observing the sites they visit is not censorship, but I would strongly disagree. Freedom depends not only on the ability to speak but also on the ability to be heard. When employees of an organization - or citizens of a country - believe that accessing certain material may endanger either their livelihoods or their lives, the creators of that material are effectively censored. Indeed, it often seems the case that the best way to silence expression is to deafen the potential audience.

Of course, if censorship is related to the visibility of communications, to browsing behavior, or to the files one stores on one's own computer, then official policies regarding cryptography also play a key role in censorship. The current global situation regarding official policies toward encryption is now extremely confusing.

In December 1998, the Clinton Administration managed to bully the 33 member nations of the Wassenaar Arrangement into signing an agreement that bound them all to uphold the same strict (and unenforceable) embargo on the export of strong encryption technology that had dominated U.S. encryption policy since the height of the Cold War. This was particularly surprising, since several of the Wassenaar countries, notably Germany, had vowed publicly that they would not place any restrictions on encryption.

Shortly following this agreement, America's own ban on encryption export was overruled in federal court and then formally rescinded by the Clinton Administration this past spring after many years of battle between civil libertarians and both the National Security Administration and the FBI. On the other hand, the Wassenaar Agreement remains apparently in effect, leaving open the question of what principles

Attenzione: il presente testo è una bozza dell'articolo omonimo pubblicato nella versione cartacea della Rivista Scientifica "Ciberspazio e Diritto" (<http://www.ciberspazioediritto.org>). Si tratta di una BOZZA: può quindi contenere differenze e, soprattutto, imprecisioni, inesattezze o refusi che sono stati poi corretti all'atto della correzione delle bozze e della messa in stampa dell'articolo. Si consiglia, pertanto, di riferirsi, nelle citazioni, esclusivamente all'articolo pubblicato a stampa. Il riferimento dell'articolo che segue Censorship 2000, John Perry Barlow, in Ciberspazio e Diritto, 2000, Volume I, Numero III, pp. 477-496. Articolo tratto dal sito <http://www.ciberspazioediritto.org>

the U.S. government will uphold in this area, as well as of what it expects of the other member nations.

Meanwhile, the governments of France and numerous other nations maintain an outright ban on the use or possession of strong encryption. Whether this applies to proprietary media players is not known.

Weirder yet, the United Kingdom has proposed the Regulation of Investigatory Powers statute, which would compel citizens to decrypt any file that a law enforcement official believes to contain data needed for an investigation. Those who failed to do so and could not prove that they had lost, forgotten, or destroyed the presumed key could face two years in jail.

Even while the authorities in some areas are attempting to prevent the hiding of offensive materials through the use of encryption, another form of encryption-related censorship has arisen in the United States: the Digital Millennium Copyright Act (DMCA). The DMCA not only encourages entertainment companies to use strong encryption in the protection of their copyrighted products but also criminalizes efforts to break these codes as well as the possession of any tools designed for that purpose.

Last year a young Norwegian programmer created a program, DeCSS, that broke the copy protection code used on digital video disks (DVDs). His purpose was not to make possible the wholesale piracy of DVD-stored films but rather to address the fact that the members of the DVD Copy Control Association-an entertainment industry cooperative loosely affiliated with the Motion Picture Association of America (MPAA)-had failed to provide drivers that would make it possible to play DVDs on Linux systems. Only by breaking the protection code could such a driver be written.

In the fashion of the open-source community, DeCSS was widely distributed on the Internet. Shortly following this, every site where it could be found in the United States was ferreted out by the MPAA and charged with criminal violation of the DMCA. That proscribing this code might be an unconstitutional violation of expression apparently never occurred to Congress or the MPAA. But there are now several court battles under way to demonstrate legally that DeCSS is a form of speech and that efforts to prohibit it as a criminal instrument should be struck down. Despite the disparate legal horsepower of the contesting parties-Congress, the MPAA, and the record industry against the EFF, 2600 magazine, and a disparate group of Linux weenies-it may be that being right still counts for something. As this is being written, the EFF has succeeded in overcoming an MPAA motion to censor publicity about the New York trial itself. Showing astonishingly low regard for free expression, the MPAA had attempted to bar the press from reporting on the proceedings and to require the participants to refrain from public discussion of them.

*The ultimate censorship.*

Attenzione: il presente testo è una bozza dell'articolo omonimo pubblicato nella versione cartacea della Rivista Scientifica "Cyberspazio e Diritto" (<http://www.cyberspazioediritto.org>). Si tratta di una BOZZA: può quindi contenere differenze e, soprattutto, imprecisioni, inesattezze o refusi che sono stati poi corretti all'atto della correzione delle bozze e della messa in stampa dell'articolo. Si consiglia, pertanto, di riferirsi, nelle citazioni, esclusivamente all'articolo pubblicato a stampa. Il riferimento dell'articolo che segue Censorship 2000, John Perry Barlow, in *Cyberspazio e Diritto*, 2000, Volume I, Numero III, pp. 477-496. Articolo tratto dal sito <http://www.cyberspazioediritto.org>

The DeCSS case is almost certainly a harbinger of what I would consider to be the defining battle of censorship in cyberspace. In my opinion, this will not be fought over pornography, neo-Nazism, bomb design, blasphemy, or political dissent. Instead, the Armageddon of digital control, the real death match between the Party of the Past and Party of the Future, will be fought over copyright.

The Party of the Past seeks to turn all existing human creation into mere property. Not only does this debase human creativity; it is also economically inefficient, it diminishes the fertility of the creative ecosystem, and, finally, it can be done only by fundamentally curtailing freedom of expression. But you cannot own free speech.

During the time since Gutenberg made possible the industrialized distribution of information, a large number of powerful institutions have arisen worldwide to serve that purpose. And they have served it well. From 1500 to 1969, they provided almost the only media by which individuals could transmit their beliefs, expressions, and creative works to the masses, in whose minds they desired to plant the seeds of new thought.

Indeed, most creators were so desirous of proliferating their works that they were willing to convey the ownership of those works to the distributors. Originally, what was being conveyed was not considered property but rather the exclusive right to undertake commercial distribution of an expression for a limited period of time.

Interestingly, during the brief period since the Internet began empowering individuals with the ability to spread their works over a broad area of mind without using the traditional intermediaries, there has been a dramatic increase in the terms of copyright licenses worldwide, and the expression intellectual property has become popular.

Practically every piece of commercially valuable art, literature, music, and scientific discovery that has been created during the past century or so is now owned by those traditional distribution institutions-publishers, record companies, entertainment conglomerates, broadcasters, film studios, universities, scientific journals, and a host of other entities whose primary creative talents reside in their accounting and legal departments.

All of those institutions properly regard the Internet as their eventual undoing. There is almost no service of value that any of them provide that cannot be performed over the Internet more efficiently, more rapidly, and with far greater profit and control extended to the actually creative. Knowing this, they are clutching ever more tightly their only remaining assets: the expressions of millions who no longer own their own creations.

As I write this, a debate is raging over Napster.com, a pioneering site that indexes the music files on millions of personal hard disks so subscribers can exchange music directly. Of course, much of this music is copyrighted, and the music industry (and a few actual musicians) are extremely distressed at the potential loss. The industry is

Attenzione: il presente testo è una bozza dell'articolo omonimo pubblicato nella versione cartacea della Rivista Scientifica "Cyberspazio e Diritto" (<http://www.cyberspazioediritto.org>). Si tratta di una BOZZA: può quindi contenere differenze e, soprattutto, imprecisioni, inesattezze o refusi che sono stati poi corretti all'atto della correzione delle bozze e della messa in stampa dell'articolo. Si consiglia, pertanto, di riferirsi, nelle citazioni, esclusivamente all'articolo pubblicato a stampa. Il riferimento dell'articolo che segue Censorship 2000, John Perry Barlow, in *Cyberspazio e Diritto*, 2000, Volume I, Numero III, pp. 477-496. Articolo tratto dal sito <http://www.cyberspazioediritto.org>

working on shutting Napster down despite the fact that there is no copyrighted material being stored on its site, and the industry will probably prevail by sheer legal force.

The legal community has so far failed to address what is most fundamental here, namely, that there has arisen a profound disparity between accepted social practice - the behavior of millions of people who made Napster one of the fastest-growing phenomena in the history of the Internet-and a body of law that would declare all of them criminals.

Only the most brutal autarchies are capable of enforcing laws that almost none of their constituents instinctively support, and, in the long run, it will be no different here. The ethical standards emerging in cyberspace support the widespread, noncommercial sharing of copyrighted expression, and both the law and the economic models that support creative work will eventually adapt to that reality. Furthermore, the traditional distribution institutions will almost certainly either die or be transformed into entities that actually promote the spread of expression rather than constrain it.

Nevertheless, they could cause great harm on their way down. They may be capable of imposing the ultimate censorship, denying posterity most of the important works of the past 150 years. In their increasingly draconian efforts to prevent the wildfire digital reproduction of their property, they will likely ensure that the works they now own are not converted into open digital form and that those works that have been digitized are removed from cyberspace. Meanwhile, the traditional physical media in which those works are currently embedded will deteriorate, become lost, or run out of still-operating devices capable of extracting their contents.

By these means, the media giants might well go to their graves with all that they still own forever embedded in the corpses and lost to future generations. This process has already begun. Every day thousands of people decide not to risk digitizing and making works generally available because of the fear they may draw the attention of the copyright police. Given the immense amount of material in question, the conversion process will require the collective endeavors of everyone who is interested in preserving particular works. If the public is legally dissuaded from lending its efforts to the task, only those works already in the public domain will be digitized.

But works from the more recent past will be lost. Books and journals will forever go out of print and be forgotten. Music will remain imprisoned on LPs that no one can play. Filmstrips will rot into brittle shards of celluloid. In a hundred years, no one will know that much of the work we now treasure ever existed.

Of all the censorship efforts undertaken by the various institutions mentioned earlier, it is this last example-censorship to protect the property rights of the moribund-that I fear the most. It must not be allowed to take place.

Attenzione: il presente testo è una bozza dell'articolo omonimo pubblicato nella versione cartacea della Rivista Scientifica "Cyberspazio e Diritto" (<http://www.cyberspazioediritto.org>). Si tratta di una BOZZA: può quindi contenere differenze e, soprattutto, imprecisioni, inesattezze o refusi che sono stati poi corretti all'atto della correzione delle bozze e della messa in stampa dell'articolo. Si consiglia, pertanto, di riferirsi, nelle citazioni, esclusivamente all'articolo pubblicato a stampa. Il riferimento dell'articolo che segue Censorship 2000, John Perry Barlow, in *Cyberspazio e Diritto*, 2000, Volume I, Numero III, pp. 477-496. Articolo tratto dal sito <http://www.cyberspazioediritto.org>

*The future.*

Ultimately, I'm optimistic. I have believed, since I first came upon the Internet, that one day it would enable any people, anywhere, to express whatever they wished - distributing their expressions to all who were interested and ensuring their posterity - without fear of punishment or censure. I have believed that the Internet promises humanity more freedom of expression than we have ever experienced and that the fruits of that freedom will transform our species into one great and God-like Mind. I have realistic hope for a future in which economic productivity is vastly amplified by knowledge, in which inequities in distribution are leveled, and in which the meek might outthink the mighty.

I still believe in that future despite all of the efforts to forestall it that I've touched on here. I believe in it because I believe that the ripe force of unconstrained creativity is already working on methods to preserve itself. Even though Napster will probably be crushed, there are already new methods for storing and sharing proscribed materials, such as Gnutella and Freenet, that have no centralized servers or legally vulnerable entities to shut down. Moreover, there are already data havens springing up where rogue governments are defying the G8 and allowing servers within their boundaries to contain any information the users wish to place on it.

Mostly, I believe in that future because I fully expect most of the human species to have Internet access within the next decade. Once that has happened, the Party of the Past will lose its currently unwired constituencies, and there will be few left who believe the excuses it still uses to mute the human spirit.

Indeed, I believe that eventually the truth really will set us free.