

Nowhere and Everywhere: the Electronic Freedom Frontier

Revised

Paper

2005.Nov.7 12:59 AM

“Man is born free but everywhere he is in chains.” - Rousseau

1. Introduction: Rousseau and Barlow

Man is born free but everywhere he is in chains. The renowned first line of Rousseau's *The Social Contract* is hereby restated(1) as a classic phrase which can still be re-interpreted to describe the contemporary state of affairs. **I will argue in this paper that it is the nation state that enslaves mankind, while the postmodern in general and cyberspace in particular provides an outlet of individual freedom that is difficult to challenge. More specifically, I deal with the problem of space and extraterritoriality in a conflict between online civil liberties and nation states.** Rousseau - as practically anybody of any significance from the last 400 years or so for that matter(2) - can be nominated for a place amongst the founding fathers of the project of modernity. His principal work “outlines the basis for a legitimate political order” (Wikipedia, 2005a). It is a journey from (then-) contemporary society to the beginnings of civilisation and back again into an anarcho-communist utopia. His assumption is that government as such is (a) illegitimate and (b) repressive. He first envisions a primitive state of mankind in a natural state of free competition, where everyone is in war with everyone, and life hazard is complemented by people being vitally dependent on each other. Rousseau argues that such chaotic conditions are a threat to the survival and the freedom of man. At this point actors either perish or draft a constitution termed The Social Contract - which sets the rules of coexistence and cooperation. Rousseau emphasises that people have to make their decisions collectively by direct participation. Direct involvement in decision making is at the core of his utopia, which provides for order being both philosophically legitimate and practically enforceable. The former, as the decision-makers and subjects are identical, so that everyone signs to the order by their own free will. The latter, as people are expected to understand and conform to their own laws. Critics have naturally pointed out that direct decision-making scales very badly, and would be impossible to implement for a whole nation. The relevant Wikipedia article (2005a), however, notes that the advent of advanced telecommunications technology might change that. Rousseau describes his utopia in terms of sovereignty rather than government, which is an antietatian position. Rousseau's thought is a struggle for individual and social freedom, in opposition with representative democracy or the nation state. The initial task of the present paper is to rethink these ideas in the context of the political evolution of the Internet. Therefore, let's start again from the beginning, now that we know what is behind the slogan.

In the light of the above paragraph it is a modern phrase, where space (e.g. “everywhere”) is a metaphor for the nation state. Indeed, a considerably concrete metaphor, as most of the surface of the Earth are covered by nation states. However, with the rise of the postmodern frontiers take up gravity, and the real increasingly leaks into the fictional. The philosophical science of hermeneutics deals with the correct interpretation of texts. One of its most

prominent figures, Gadamer (1990) teaches that the meaning of a text (or a sentence for that matter) is best grasped in two distinct steps. Firstly, the authentic meaning shall be reconstructed from the words themselves. Secondly, the authentic meaning shall be applied to the reader in light of his existential and historical situation. That is the task here, to explore what possibilities does our motto hold for us.

Man is born free but everywhere he is in chains. (Rousseau 2005) *But what if there is a space outside “everywhere”?* We can say with the founding father of cyberspace that [o]urs is a world that is both everywhere and nowhere, but it is not where bodies live (Barlow 1996).

The definition is restated from John Perry Barlow's manifesto *A Declaration of Independence of Cyberspace*. It foregrounds the fact that the real chains that enslave mankind - for example the state monopoly on physical violence - are powerless in cyberspace. As Barlow puts it: “[o]ur identities have no bodies, so, unlike you, we cannot obtain order by physical coercion.” Of course, Rousseau uses “chains” primarily as a metaphor for the binding laws that are imposed upon individuals by the state. However, laws are also highly dependent on territory and the real. Barlow phrases it as: “Your legal concepts of property, expression, identity, movement, and context do not apply to us. They are all based on matter, and there is no matter here.” Naturally, the central claim and demand of the *Declaration* is that cyberspace is not - and shall not be - a part of any country, and no one but the user community exercises control over it. It is proclaimed to be a sovereign territory without government - just what Rousseau thrived for in the 18th century. Indeed, Barlow calls for a Social Contract of Cyberspace. “We are forming our own Social Contract. This governance will arise according to the conditions of our world, not yours.”

Interestingly, Barlow uses the word “governance” instead of “government”, similarly as Rousseau uses “sovereignty” to contrast his concept of social order with the nation state. More interestingly, Barlow's usage reflects a radical recent development in the history of Western thought: the focus shifting from nouns to verbs. In pre-Socratic philosophy, notably at Heraclitus (about 535 - 475 BC), and in the mainstream of 20th century philosophy it is a basic assumption that being is more important than existence. Whether that is an independent development in philosophy or it is a genuine historical change in everyday reality is hard to tell, although Jean Baudrillard makes a point in the motto for his book *The Transparency of Evil*: “Since the world is on a delusional course, we must adopt a delusional standpoint towards the world. - Better to die from extremes than starting from extremities.” (Baudrillard 1993)

Indeed, Jerry Everard, the author of the 2000 book *Virtual States*, professes that Internet itself will bring about this paradigmatic change, which spreads from language into reality (Everard 2000).

“Perhaps it will bring a philosophically more significant change: from an economy of objects to an economy of signs, and from a philosophical world of nouns, to one of verbs. Already the distinctions are blurring within language, as verbs become nominalised, and nouns are transformed into verbs. We 'email' each other, 'satellite-in' the news, become 'informationalised', 'cycle' to work, or 'network.’” (Everard 2000:156)

Thus the *Declaration* announces the eventual victory of the fictional over the real. That

is how the Internet arises as a new historical battleground. Rousseau's slaves flee in increasingly large numbers to the shelter of cyberspace, where a civilisation of exiles emerges. Exiles from the body and from the real, as well as from the nation states. Not a conglomerate of people in constituent states, but a set of "identities" nurturing "constituent cultures" who "will create a civilization of the Mind in Cyberspace. May it be more humane and fair than the world your governments have made before."

Beyond the broad philosophical statements above it is outside the scope of this document to inquire upon the impact of cyberculture on nation states. It is more relevant to look at the other side: whether nation states can exert their power on cyberspace, and to what extent.

The *Declaration* was an answer from side of the Electronic Frontier Foundation (3) - the mightiest stronghold of Internet powers - to the 1996 *Telecommunications Reform Act*, especially Title V., termed the *Communications Decency Act*. It was the first attempt at legislating against the Freedom of Information, and it still remains a prototypical example, since the many similar laws since passed have had similar fates. It prohibited intentionally communicating "by computer in or affecting interstate or foreign commerce, to any person the communicator believes has not attained the age of 18 years, any material that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs." Passed on February 1, the *Declaration* was issued two weeks later, and stated with clearvoyance and clarity that "[y]ou have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear." In another formative organ of electric citizen consciousness, Dr. Richard Barbrook,(4) published an article critical of both *Act* and *Declaration*. *Ctheory*(5) published the article on May 6 in the same year. It is worth citing at length from the article, as it evaluates the situation from a perspective of a few month and demonstrates the confusion around the issue very well:

"It is obviously a fantasy to believe that cyberspace can be ever be separated from the societies - and states - within which these people spend their lives. Barlow's *Declaration of Independence of Cyberspace* therefore cannot be treated as a serious response to the threat to civil liberties on the Net posed by the Christian fundamentalists and other bigots. Instead, it is a symptom of the intense ideological crisis now facing the advocates of free market libertarianism within the online community. At the very moment that cyberspace is about to become opened up to the general public, the individual freedom which they prized in the Net seems about to be legislated out of existence with little or no political opposition." (Barbrook 1996)

This paragraph gives the impression that Barbrook is glad that individual civil liberties are wiped out of the wires. Earlier in the article he cites with indifference the example of radio, where official regulation of the airwaves enabled mainstream access and simultaneously removed the interactivity of the medium. It seems that the author does not think that the electronic frontier would be out of reach of the nation state. However, some pages later he refutes his own basic assumptions:

"Contrary to the predictions of the pessimists, it is possible to win the struggle against both the political and economic censorship of cyberspace. Although the state can - and should - prosecute the small minority of paedophiles and fascists, the resources needed to spy on everyone's email and Web sites will make the imposition of moral puritanism very difficult to

enforce.” (Barbrook 1996)

That is how the scene looked at 1996. Almost a decade has passed, and Barbrook's paradoxical statements still ring true. The struggle continues, and the firewalls of cyberspace are yet to be taken. Nation states and cyberspace advocates fight on three fronts: legal regulation, technological race, popularity. During the course of the paper the argument will tacitly move through each perspective. Naturally, these factors are mutually interdependent. Extraterritoriality is perhaps the most important challenge nation states have to overcome before they can take the initiative, and interestingly it is their very essence as well. However, they have dealt with extraterritoriality before in several instances. Perhaps a brief analysis of this accumulated experience would be instrumental in finding out about the dynamics of the clash between states and the virtual community.

2. Legal Challenges of Extraterritoriality

There are at least three realms apart from the Internet that poses the challenge of extraterritoriality to the states. These are the outer space, the high seas and the Antarctica. Generally, these differ from cyberspace in a very important aspect. As all space, they were initially no-man's-land. There could have been a war fought for the control of either, but nations thought out of enlightened self-interest to preserve them as extraterritorial. The Internet, however, emerged in its most recognisable form in the United States, and it is technically speaking still maintained in the United States, and in some essential respects **by** the United States. The difficulties and dangers arising from this will be elaborated in the sections about the WSIS process. In the proceeding sections each of the extraterritories will be briefly discussed, with outer space having a longer treatment.

2.1. Outer Space

This section is mostly based on Anna Maria Balsano's paper published by UNESCO in the 'Law of Cyberspace' series in 2000 (Balsano 1998).

She writes that “[a]s stated above, outer space, like the high seas and Antarctica, is an area outside any state sovereignty and cannot be appropriated. According to general international law it can be considered a **res communis**.” Thus, outer space law is a **lex specialis** of international law.

In a way outer space is similar to cyberspace in that it is not directly habitable by the human species. As a consequence, almost all operations in outer space require special machines to mediate between man and space. “Both outer space and cyberspace activities are carried out regardless of geographical boundaries, in a medium that is used to achieve certain goals.”

Moreover, they are both frontiers in more than one sense of the word. First, they are frontiers in an almost ontological way, precisely because of their technical requirements - that they do not lend themselves easily for everyday use(6). Physically outer space is just more place. However, the question is whether it manifests itself in human experience as yet-more-space

for colonisation and warfare, or constitutes something different - a realm that is probably not adequately described by the word space. In other words, if there is a quantitative or a qualitative difference between space on Earth and outer space. The same ontological issue is at stake with cyberspace, and the answer might determine the outcome of the struggle for its control. Perhaps the question was first taken up by William S. Burroughs:

“This is the space age, and we are here to go.. However, the space program has been restricted to a mediocre elite who — at great expense — have gone to the moon in an aqualung. Now, they're not really looking for space, they're looking for more time. Like the lungfish, and the walking catfish; they weren't looking for a dimension different from water, they were looking for more water” (Wikipedia 2005b).

In a second way, outer and cyberspace are frontiers in a very definite sense: that they have no clear boundaries. Outer space has been widely theorised to be continually expanding, and the same has been claimed about cyberspace. Such notions of limitlessness are very interesting to the human mind, and surely contribute to these spaces being associated with freedom and peace. So far that applied to the frontiers of these frontiers. In a third way these are frontiers because there is no clear boundary between home country - the “real” - and the extraterritories. A plethora of cyberspace definitions are on the intellectual market, including Barlow's, and Balsano notes regards outer space that “[t]here is, as yet, no legally accepted boundary between air space and outer space” (1998). Interestingly, that does not prevent lawyers to legislate over them. Five international laws apply to outer space:

- The Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including Moon and other Celestial Bodies, 1967. January 27.
- The Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects.. 1968 April 22.
- The Convention on International Liability for Damage Caused by Space Objects, 1972 March 29.
- The Convention on Registration of Objects Launched into Outer Space, 1975, Jan 14.
- The Agreement Governing the Activities of States on the Moon and.. 1979 Dec 18.

The first and the last requires further explication here, the rest are not relevant and pretty straightforward anyway. It is not an exaggeration to state that the Principles and the paragraphs of the 1979 Agreement lay down rules for technical management and content management as well as warfare. Some examples are considered here, followed by a number of concluding remarks, to highlight the lessons learned from the legal exploration of outer space. Technically, the registration of orbital objects is a prime instance. Article VI. makes provisions for the “[s]tate's responsibility for and supervision of private activities”. However, similar problems emerge in the application of this law than in the case of cyberspace, where it is oftentimes hard to decide whether to apply the sender's country's laws, the receiver's country's laws, or perchance the server computer's country's laws. Regarding the objects in outer space, international law does not make it explicit which state is responsible for private activities - the launcher citizen's state, or the state from which the object was launched. The same inherently flawed approach is taken up in nearly three decades later regarding

cyberspace, when the already quoted *Communications Decency Act* referred to “community values”. Whose values? Or whose objects?

Clearly the principal problem here is a question of principle: what is a state? Is it a territorial entity or a group of people? It is possible to argue that it is in fact a third - a legal entity. However, such a solution achieves nothing but merely reformulates the question: does national laws apply to the physical territory of the nation state or its citizens? Naturally, both are true to a certain extent.

The greatest space-faring nations have forged national-level laws to answer these questions and to ensure the observance of Article VI. Sweden, for instance, goes for sure and regulates the activities carried out on its soil as well as the activities of its citizens elsewhere. The United Kingdom regulates only its citizens. Despite these difficulties there are no problems with the implementation and operation of the registration system, and the taking of appropriate responsibilities. It would be logical to argue that given a relatively low number of actors in the space field, the same was not true for cyberspace, where as many users communicate with each other as there are stars in the sky. However, it is not the case. Experience shows that the legitimacy and purposefulness of technical standards is widely accepted and adopted by member states and other actors out of pure enlightened self-interest. The sole challenge for international technical standards are the multinational corporations, who tend to introduce their own (potentially undocumented) 'standards' that are mutually exclusive. That has happened during the so-called browser wars between Microsoft and Netscape - but the general tendency is strongly against that. It can be safely stated that technical standards and specifications scale very well. From a political point of view a possible explanation is that the involved actors generally all profit from the introduction of standards, while other regulations aim to restrict certain actors. Of course any oppressed actor will attempt to resist the (proposed) regulations - which means that the enforceability of the latter type of laws will depend on the power of the disadvantaged to resist. Naturally, the current standards are one of the factors that are used to assess the power of one or other party, so that technical management and other questions are deeply entangled, but at the moment it is more useful to consider them separately.

The best examples of content-management in outer space and in cyberspace are intellectual property laws. A number of international fora examined the question, and they “concluded that, due to the international character of outer space and the territorial working of national patent laws, it is unclear whether the use of an invention protected by a patent falls under any patent regulation and thus whether patents in outer space can be protected” (Balsano 1998). Balsano emphasises that “new services and products resulting from space activities are difficult to integrate into the existing legal doctrine” (2000). The well-established practice prevails here as well, that international law only provides loose principles, and the actual interpretation and application of these principles is carried out by each national jurisdiction separately. However theoretically prudent that may be, such an approach proved to be highly ineffective, for example in connection with the International Space Station. The first intergovernmental agreement on the space station was signed in September 1988, and a more elaborate version was ratified on 29 January 1998. The new agreement is completely rewritten but the section on intellectual property, and it says that each country should legislate on whether their particular patent law applies or not. For some reason solely Germany lived with the possibility in 1988, and no one else since then.

The United States - which sees nothing in space outside its national borders but territories for colonisation - have chosen a more effective way and unheeding to the international consensus on a system that obviously did not achieve its goals, established its own practice with the Patents in Space Act, adopted in 1990. It extends the widely criticised U.S. Patent Law to objects in outer space. Such a unilateral move clearly goes against the agreed principle laid down in Article I. of the Outer Space Treaty, the "Right to use but not to appropriate Outer Space." This latter strategy is perhaps more effective, but apart from being completely illegitimate it proliferates a legal framework that is inherently flawed and which faces widespread resistance all over the world anywhere the U.S. government and the spearhead of neoliberal globalisation (the World Intellectual Property Organization) attempts to force it on other governments. In conclusion, neither international cooperation (as it is not heavy enough) nor national commitment to colonisation (as it is too strong) solve the problem. In a beautiful instance of extraterritorial legislative vacuums fusing together as the two ends of wormholes, the very same problem is directly relevant to the cyberspace intellectual property debate, as some satellites are part of the telecommunications infrastructure of the Internet. The rapid development and growing availability of space technology also presents similar problems to cyberspace:

"One lesson that can be learned is the need to avoid the pitfalls that occurred when the international community attempted to regulate specific space applications - for example, direct satellite broadcasting - on the basis of their technical characteristics rather than their general effects on states" (Balsano 1998:143).

Balsano concludes that "[c]yberspace activities are currently subject to a wide variety of national regulations that reflect the state of the activities taking place in a given country and the legal appreciation in that country of those activities. This situation is the reverse of the way in which space law developed; at first only internationally agreed principles were formulated and, in some cases, later 'transposed' into some national regulation. However, as with space activities, the basic legal problems arise from the inherently extraterritorial character of activities, which can have effects outside the control of individual states." (1998:143)

The state of affairs is further proof that in developed societies economy took the lead, and military power is only there to enforce its rule. That is another inversion, because previously military power was the primal tool of domination. Such a turn in sociological reality is further developed in cyberspace, so that it is worth considering the experiences that arise from space research.

Section IV. provides for the "Obligation to use Outer Space for Peaceful Purposes." It is draconian regarding celestial bodies like the Moon, and prohibits the insertion of weapons of mass destruction (including nuclear weapons) elsewhere, which continues and encourages the historical process whereby the focus changes from the active oppression of physical coercion to the passive oppression of personal surveillance (Foucault 1975). It has been already argued above that outer space is undecidedly 'real' and 'virtual' as well. It is worth noting here that its special situation makes it extremely fit for both physical surveillance of 'real' territory and technological surveillance of 'virtual' territory such as the electronic superhighway. That is another point where content management and technical management entangle, and here even the third - military use - is involved in the process. Two thirds of orbital satellites at the moment serve military purposes, and the global Internet sniffing

systems Echelon and Carnivore make use of satellites. Interestingly, that means that in the fight for the electronic freedom frontier, the strategic goal of the libertarian defenders of cyberspace is more tight legislation of outer space. On occasion that the principle held by some countries (including the U.S.) that an object launched from/by a nation state into outer space is considered quasi-territory would be dismissed, there were more accountability. That is a very important point, because at the moment the countries involved in the operation of the Echelon/Carnivore system use every single possibility to deny its existence to the very point of absurdity. As far as cyberspace is considered as a first amendment battleground during the course of this paper, the Echelon/Carnivore project stands out as the Internet filter of constitutional democracies, which - in contrast with internet filters mounted on the firewalls of dictatorships - clearly compromises the free speech of the people all over the world, not just in one particular country.(7)

In conclusion, outer space invokes the concept of the unity of humankind, and treated as a common reserve maintained in principle for the good of all and for scientific research, and in practice for military and spy operations. Technical management of outer space is wide and functional, while certain legal issues are still unresolved. It also stands as a promise of peace and unity, while most applications of it serve passive oppressive measures. The United States is as dominant a power here as anywhere else, taking unilateral action to disrupt international processes aiming for a consensus.

2.2. Antarctica

Antarctica is less interesting from a political, economical and scientific point of view. It is in many aspects similar to outer space in its workings. Although it conforms to a greater extent to ordinary human notions of space as a physical space, the requirement of highly sophisticated technology and the great cost of exploration still reserves it a mythical air, something akin to an ontological difference. Going to the Antarctica is not a travel but a voyage - an existential experience. That aspect is foregrounded in contrast with cyberspace, which is on one hand an organic part of everyday life in developed societies, and on the other hand it is less real than any extraterritories. Cyberspace offers a subtler experience which is, however, more ontologically marked.

As mentioned above, the Antarctica is not habitable by traditional means. It is not infinite in the physical (as outer space) or logical (as cyberspace) sense of the word, but it is the 5th greatest continent and the one with the least population. Reserved almost exclusively for scientific research, there is plenty of space for any nation or individual to use. On the other hand, there is some kind of requirement for licence, in an indirect way similar to outer space - as scarcely can one enter these realms without the aid of a nation state or a multinational corporation. Entering cyberspace is a lot cheaper and requires little official cooperation. Treaty states meet regularly to communicate with each other regarding the affairs of the continent, which means some level of cooperation and surveillance. Such an intergovernmental (and hopefully multilateral) discussion platform for cyberspace will perhaps be established as a result of the WSIS process.

In slight contrast with outer space it is a completely demilitarised zone, but there are at least 27 nations that claim territories on Antarctica, and some claims do overlap. The space treaty

was the first international treaty signed by both the U.S.A. and the U.S.S.R. in the cold war era. Similarly, after a brief intermezzo by Argentina, the Antarctic Treaty System was established, which explicitly prohibits military operations on Antarctica, although it permits the use of military hardware in scientific pursuit.

Article 3 of the Treaty provides for the “free exchange of information and personnel in cooperation with the UN and other international agencies” (Wikipedia 2005c), so once again the situation is more clear-cut than in outer space, and there is less struggle for the appropriation of inventions. Criminal law is similarly simplified, although that may pose more practical problems: each person is judged by their own nation state, wherever that may be. As some complication, Chile and Argentina (the closest countries) reserve the right to judge criminal cases in their vicinity and defendants may choose which country's court they shall face. Moreover, the U.S. features here as well with some unilateral action, as parts of the U.S. law “including certain criminal offenses by or against US nationals, such as murder, may apply to areas not under jurisdiction of other countries” (Wikipedia 2005c). There are a great number of national and international environmental laws that apply to Antarctica, but they are mostly beyond the scope of this paper.(8)

In conclusion, it seems that the international community has tackled successfully with the challenges offered by Antarctica, and it is a peaceful and intellectually free area, where nation states hold the steering wheel firmly in their hands.

2.3. High Seas

The High Seas is the most ancient of the extraterritories. It is the archetypal end-of-the-world, between fiction and reality. Interestingly it still retains some of its legendary glory, while from a legal point of view international regulations are still controversial. A more lengthy explication of the High Seas will be added in a later version of this document.

2.4 Conclusion of Extraterritorial Experiences

The above treatments showed with convincing detail that extraterritories have many things in common, and there exists a tradition of establishing and maintaining extraterritories that are used for the benefit of nation states and thus humankind in general. The population of these realms generally require some special equipment and some degree of technical competence and understanding, and therefore there is a great degree of technical management required to run them. Nation states of the international community widely recognise that fact and act in accordance with international law and recommendations that are in force. In contrast, non-technical legal management is underdeveloped, and the research and thinking in general that takes place in these realms poses serious challenges to nation states, who are reluctant to cooperate as an international community regarding these matters, especially intellectual property rights. These realms are generally considered demilitarised zones as *res communis*, although infringements upon these principles are common. The international policy regarding Antarctica is more elegant and sufficient, perhaps because its lower political, military and scientific potential.

Cyberspace, however, is more open for participation and little international law exists that would regulate it in any way. That's not solely because it is still an emerging phenomenon, but also because it is partly under the national jurisdiction of the United States, as we shall see in the next section. Being a purely technical medium, the operation of the Internet depends on the conformance to technical standards and specifications of nearly all actors involved. Albeit these actors are much more numerous than in any other extraterritorial realms, common understanding and enlightened self-interest is enough to ensure critical requirements. However, standard-setting and conformity consciousness are not purely emergent processes, but coordinated by an industry consortium independent of nation states called the World Wide Web Consortium. The Consortium does not regulate anything, but produces **recommendations** to spread conformity. Moreover, the Internet Engineering Task Force is a non-localised international civil society entity, which is concerned with largely the same matters. Therefore it seems that the Internet is a self-regulating entity to some extent. That poses critical challenges for nation states in the areas of criminal and intellectual legislation, and it seems that it may be simply beyond the reach of nation states and international policy making. Indeed, the very purpose of the present paper is to explore how and to what extend does that proposition stand.

There are at least two factors that are novel in cyberspace compared to other extraterritorial realms that emerged before it. These factors make the Internet qualitatively different, and are especially hard to overcome from the point of view of nation states. One is an ontological problem; namely that people in cyberspace are in a real place at the same time, presumably - but not necessarily - in a nation state. The second is a political problem; that the Internet became so popular so fast that its population acquired a certain level of consciousness. This desire for freedom is examined in the first section of this paper and exemplified by Barlow's *Declaration of Independence* and manifest in the activity of the Electronic Frontier Foundation. On the other hand, it materialised in the common practice of everyday young people in developed societies. If the two factors are put together, it shows that the Internet is a medium of two-way communication. Regarding regulation that is very problematic as perhaps the single most established freedom in democratic societies is the freedom of speech - and cyberspace is virtually nothing but speech. It is interesting to note that freedom of speech has been the most firmly grounded freedom in democratic societies.

3. Recent Developments in Internet Governance

After presenting the battlegrounds and the opening moves of the cyberspace war of independence, the experiences and strategies of nation states has been surveyed along with their weaponry. Section three deals with the front of the war on the nation states' home land - on the battleground of international law. A subsequent section will deal with the battleground inside cyberspace - technology. Internet governance as used in the title of this section means the attempt by nation states to establish their control over the extraterritory of cyberspace. Internet governance proposes rules and regulations which aim to provide an international legal framework for dealing with the internet. The very same thing has happened with all the extraterritories described above: instead of governments these realms are simply under **governance**. Another instance where nouns verbify, as has been hinted upon earlier.

As the area of Internet Governance is mind-bogglingly complex, the sections will concentrate solely on the major players, while retaining a level of actual examples in order not to lose touch with reality. However, the author apologises about the excess of organisation names in the preceding sections.

3.1. Internet governance in the 20th century

The Internet emerged from a variety of government-funded research projects. A major financial source was the United States' Department of Defense, through its DARPA (Defense Advances Research Project Agency) programme, although actual development was carried out by morally responsible pioneer programmers, who made their contributions free for all humankind without copyright.

For example, Jon Postel, one of the Fathers of the Internet (119) in the specifications for TCP/IP, the protocol for all Internet communication (9), included the Robustness Principle, which **can be read as both a moral principle and a technical principle**:

“TCP implementations will follow a general principle of robustness: be conservative in what you do, be liberal in what you accept from others.”

Jon Postel was also editor of the *Request for Comments (RFC)* documents, in which Internet standards have been traditionally defined. He has also been the distributor of Internet addresses as IANA (Internet Assigned Numbers Authority), and described by *The Economist* as “God of the Internet”. Thus, it is fitting to start exploring the issue of Internet Governance from Jon Postel. RFC and IANA are the first links in two separate stories: the mechanism of setting standards for the Internet (10), and the assignment of names and numbers (11).

To understand this, one has to see clearly that in the 1980s the Internet was not primarily a mainstream medium or an essential telecommunications infrastructure, but a research project. As a research project, it was “governed” in an informal way, and it retained its informality to some extent to the present day.

3.2.1. Setting standards for the Internet

Even now, the development of standards for the Internet is undertaken by various informal groups without legal standing, who all pass their input to the Internet Society, a non-profit organisation that was founded “to assure the open development, evolution and use of the Internet for the benefit of all people throughout the world” (Internet Society, 2005)

Two organisations are coordinated by the Internet Society - the World Wide Web Consortium (W3C) and the Internet Architecture Board (IAB). “These two bodies are the closest the Internet has to an executive.” (Terret 1995:18) The latter is developing deeper communication standards, while the former is working on standards involved in the organisation and presentation of actual content. “The Consortium is headed by Tim Berners-Lee, the original

creator of the World Wide Web and primary author of the URL (Uniform Resource Locator), HTTP (HyperText Transfer Protocol) and HTML (HyperText Markup Language) specifications, the principal technologies that form the basis of the Web” (Wikipedia 2005d). These organisations gain their legitimacy from the leadership of these historical figures and their informal and open mechanism which ensures independence and transparency. The overwhelming bulk of the work is done online, taking advantage of mailing lists with open archives and free membership. Indeed, some have suggested that the anarchic nature of the Internet was influenced by the fact that most network development and policy decisions were the results of online discussions from the beginning.

“W3C operations are supported by a combination of Member dues, research grants, and other sources of public and private funding. W3C operations are jointly administered by the MIT Computer Science and Artificial Intelligence Laboratory (CSAIL) in the USA, the European Research Consortium for Informatics and Mathematics (ERCIM) headquartered in France and Keio University in Japan. W3C also has World Offices in fifteen regions around the world.” (W3C 2005) Membership include academic institutions, organisations from civil society and the private sector. Membership is fee-based, but smaller organisations are expected pay less. Thus, the World Wide Web Consortium is a truly open, international, multi-stakeholder entity.

The other body which in closer partnership with the Internet Society is the Internet Architecture Board (IAB). The IAB coordinates two other informal entities, which both have their hard-core leadership body. On the one hand, there is the Internet Engineering Task Force (IETF), headed by the Internet Engineering Steering Group (IESG). On the other hand, a later development for faster workflow is the Internet Research Task Force (IRTF), led by the Internet Research Steering Group (IRSG). The Engineering Task Force emerged from a series of events initially funded by the U.S. Government, and then transferred to the Internet Society. The Steering Groups have more formal membership, but the Task Forces are all-volunteer organisations open to all, and does not require a formal membership procedure other than taking one's part in the research. The most wonderful about these organisations is the following: they operate in a completely autonomous manner, so that their very organisational principles and internal rules are published as contestable standards under the Request for Comments (RFC) series.

None of the standards worked out by bodies in partnership with the Internet Society are legally binding. The World Wide Web Consortium (W3C) names its finished standards Standards in order to distinguish them from other standards. The Task Forces publish their results in the RFC series, which are nothing more than plain text (ASCII) files that are uploaded to various servers. These have cultic value in the technical circles, and thus they are widely followed and accepted. Commentators note that “RFCs are most remarkable for how well they work - they manage to have neither the ambiguities that are usually rife in informal specifications, nor the committee-perpetrated misfeatures that often haunt formal standards, and they define a network that has grown to truly worldwide proportions” (12).

The contest between the International Organisation for Standardisation (ISO) and the Internet Engineering Task Force (IETF) offers insight into the efficiency of informal self-organisation and transparent open processes. The ISO should have been in charge of setting the standards. It defines itself as a non-governmental organisation, but its membership entails both governments and private sector actors. Standards set by the ISO become incorporated in

national laws and thus are often legally binding. Moreover, ISO standards specifications are not freely accessible. The greatest challenge of the 1980s in standards was offered by connecting different networks in order to form the Internet. The IETF published RFC 793 in 1981, which described the basic operation of TCP/IP, the protocol used for 95% of Internet traffic. ISO started its own programme, the OSI (Open Systems Interconnect) in 1982, publishing standards of low technical quality and lengthy description. The ISO OSI initiative simply collapsed in 1996, resulting in a major loss of reputation for ISO and great financial loss for its members. Since then, **the Internet is considered a separate realm in the area of standards setting, and internauts research and define their own standars in their own way (which are published as standards themselves), and rely on community values not legal binding power for the ensurance of their universality and wide-spread implementation.** Thus, the standards-setting battle was won by the inhabitants of cyberspace.

3.2.2. Assignment of Names and Numbers

Initially, the assignment of names and numbers was managed by Jon Postel. Later, the Internet Assigned Numbers Authority (IANA) was formed to legalise the situation. With the rise of the Domain Name System (DNS) numbers could be assigned human-readable names, so that strings of words corresponded with strings of numbers.⁽¹³⁾ First, the names were assigned by a private firm called VeriSign which received its monopoly from the United States government. In 1998 the Internet Corporation for Assigned Names and Numbers (ICANN) was formed by the United States Department of Commerce to undertake the assignment of names and numbers, and IANA came under the authority of ICANN (Peake 2004). Adam Peake notes that “The avowed intention behind ICANN's creation was to privatise and internationalise the DNS, to introduce competition, and over time hand over responsibility for DNS management to the global Internet community. ICANN has introduced competition to the registrar business for domain names, and has created a very limited number of new TLDs. However, the United States is showing few signs of loosening its oversight on ICANN.”(2004:27) The conflict between ICANN and other players in Internet Governance will be discussed at length in subsequent sections, but in order to understand that conflict it is necessary to know more about the operation of the ICANN and its relationship to other entities.

The entirety of all possible names and numbers under a certain regime is called a namespace. Namespaces are owned by ICANN, and strictly speaking anyone else only rents them. Assignment of numbers is done by the IANA, which assigns chunks of the namespace to Regional Internet Registries (RIRs), which typically redistribute these to Internet Service Providers (ISPs). Organisations and individuals buy Internet access from these companies, who in turn assign numbers to them when they access the Internet. Thus broadly speaking every computer on the Internet has a number (commonly called the IP address) which identifies it. If a computer connects to the Internet through a Local Area Network (LAN), it usually has the IP address of the computer which connects directly to the Internet (called a Gateway). RIRs collectively form the Address Supporting Organisation, which takes part in the decisions of ICANN.

On the other hand, the right to sell domain names is given by ICANN. The concept of TLDs

is central to its domain name policy. TLDs are Top Level Domains, that is, suffixes that form the last part of Internet addresses like “.com” (for commercial organisations), “.org” (for non-profit organisations) and “.fr” (for France) or “.uk” (for United Kingdom). As seen from the examples, there are two kinds of TLDs: gTLDs (generic top-level domains) and ccTLDs (country code top-level domains). The right to sell gTLDs is granted to “certified domain registrars”, huge corporations that resell their rights to smaller companies or other organisations. The right to distribute ccTLDs is granted to the first applicant from every country, who can set their own redistribution policy. This system has led to a great deal of problems. Registrars of ccTLDs and gTLDs also form bodies that take part in ICANN's system of decision making. These are the Country Code Name Supporting Organisation and the Generic Names Supporting Organisation respectively.

The most important factor and one that incites primal fear in some of the more Internet-conscious countries is that while ICANN is charged with the distribution of names and numbers, **the U.S. Department of Commerce retained the right to control the root zone file, which defines the TLDs.** All modifications to the root zone file is to be signed by the Department of Commerce. This means that in effect the U.S. government has the ability to remove entire countries from cyberspace. For example, on deletion of the “.hu” top level domain, all addresses with that suffix would become unreachable. Moreover, it has raised considerable concern that almost all of the root servers are on U.S. soil, and all other servers learn the addresses from these computers. This has been partly resolved by now by the introduction of the Anycast system, but the origin of all address information is still the United States, which allows it to play complicated yet highly dangerous games with its data monopoly.

Moreover, ICANN has been under criticism since its creation for having an initially flawed operational structure which lack the essential openness, transparency and multi-stakeholder composition that would be fitting for an international organisation that undertakes such important work. The starting point for the next section will be a line from Adam Peake's paper where he writes that “too many of ICANN's decisions are still ad-hoc” (Peake 2004:29).

3.2. WSIS I. in Geneva

WSIS stands for the name of a United Nations conference entitled World Summit on Information Society (WSIS). While Internet Governance and related issues has been addressed in a wide range of international fora in the past decades, it is the two rounds of WSIS in Geneva (2003) and Tunis (2005) that promised major changes in the Internet Governance regime. Alan Toner's introduction to WSIS and the events that preceded it on the international legal battleground surveys these fora briefly (Toner 2003).

The WSIS was advertised by its organiser, the U.N. body called International Telecommunications Union (ITU) as a “new kind of summit” (ITU 2003:1), characterised by a multi-stakeholder approach. Three kinds of stakeholders were invited to the summit: governments, corporations and civil society. However, even before the summit took off, members of the civil society caucus voiced alarms about their treatment. The WSIS Secretariat attempted to ensure that civil society delegates would not even meet other

stakeholders, which ensured that they are not involved in decision making.

“NGO participants discovered that while decisions on procedural form were to be discussed in the ITU building (where Pakistan and China were doing their utmost to have participation limited strictly to state-actors), they themselves were to be quarantined across the road where a programme of discussions had been scheduled for them by the Civil Society Directorate.” (Toner 2003)

Worst still, preliminary talks suggested that even governments who shared the concerns of civil society members would be rendered powerless by the unilateral policy of the strongest countries which defiled the spirit of international talks. As the summit drew close, it became increasingly clear that no real decision is to be expected, and most participants interpret the summit as a spectacle for the media to display their false commitment to popular social issues and increase their credit. Civil society was coopted by the powers-that-be:

“Without the NGOs the emptiness of the windy sermonising might be all the more apparent.” (Toner 2003)

Naturally, the counterculture organised itself as well, both inside and outside the summit. Inside, critical NGOs gathered in a platform called Communication Rights in the Information Society (CRIS), which was born at the World Social Forum in Porto Alegre in November 2001 from a pre-existing alliance of NGOs known as the Platform for Communication Rights including such organisations such as the Association for Progressive Communications and Computer Professionals for Social Responsibility. On the outside, grassroots critical media activists set up a place called Polymedia Lab, where a series of events took place under the title “WSIS? We seize!”. One of the outstanding achievements of the cooperation between the two groups was the discovery and subsequent scandal over the usage of RFID in the WSIS entry cards. All official participants of the WSIS received these cards, and the Secretariat used the RFID technology to trace their precise movement inside the conference, mapping the social network of the Summit. Even the heads of states and the CEOs of multinational corporations were unaware that their privacy is being breached and their behaviour is tracked with bleeding edge surveillance technology.

Eventually, both official documents and independent commentators agreed that any real decision was impossible in the framework of the summit, given that participants did not even know what they were talking about. Even those with a sincere commitment were unable to articulate their position.

Karen Banks from the Association for Progressive Communications writes that “many of the debates during Phase I were complicated by a general lack of understanding and confusion around how the internet works” (Banks 2005:3).

Adam Peake voices a strikingly similar opinion: “ICANN and the technical and policy processes associated with it were at the heart of Internet governance discussions. There was some misunderstanding about what ICANN does, and particularly about what it controls and the nature of that control, but there were also genuine concerns about its operations.” (Peake 2004:9)

In fact, the participants could not even agree on what Internet governance is. The results? The

final documents stressed “capacity building” for decision makers in order to face the challenges posed by the incoming Information Society, and the U.N. Secretary General was kindly asked to create the Working Group on Internet Governance (WGIG), which developed a definition of Internet governance and some alternatives for addressing related problems.

Once again, Barlow's outcry from 1996 hit the mark: “You do not know us, nor do you know our world.”

Furthermore, Alan Toner of Autonomedia surveyed the battleground and called the people of cyberspace for civil disobedience: “[f]rom Ogg to DivX, setting up file-sharing systems to disabling firewalls, technologies of sharing are being deployed, expressing our identity as commoners, confronting cartels with mass illegality.” (Toner 2003)

The WGIG worked between the two phases of WSIS (2003 Geneva and 2005 Tunis) with a limited number of participants. Civil society members made extensive efforts to gather comments from a wide variety of sources, and the final report was born on 14 July 2005. Once again, the second phase of the WSIS could begin with the possibility of a meaningful discussion on Internet governance. Decisions could be made about international treaties and laws addressing the global challenges which nation states face in their desperate situation of being surrounded by the Internet and its unlawabiding cybernauts.

3.3. WSIS II. in Tunis

The negotiations for the Tunis round were overshadowed by two considerations - both foregrounding inherent controversial elements in the forum organisation itself. For one, the Bush administration continued to deface multilateral efforts by releasing a statement on 30 June 2005. While at the WSIS discussion revolved around the reform or superseding of ICANN, and the WGIG spent much of its time working out alternatives to ICANN's control, the statement of the U.S. government emphasised that “ICANN is the appropriate technical manager of the Internet DNS” (U.S. 2005:1). Such a proclamation coupled with the other pronouncement that the “United States Government intends to preserve the security and stability of the Internet's Domain Name System (DNS)” (U.S. 2005:1) means that the Department of Commerce retains its control over the root file, which is the most contested element of the current Internet governance regime.

For two, from the very beginning of the summit many found controversial the selection of the host country: Tunisia. Its disasterous human rights record is topped by the fact that its laws and constitution are hypocritically democratic. Most specifically, its one of the few countries that filters political content on their network. As of October 2005, an online journalist and freedom advocate - a honorary member of the international Pen Club - has just died after two hunger strikes in prison. Local authorities ruselessly repress any demonstation on the street, so activists are organising a virtual protest in cyberspace at www.yogi.org. The chief organiser is an organisation called Association for the Promotion and Defense of Cyberspace. The very existence of an organisation by that name is telling of the local situation.

However, that would not necessarily affect the outcome of the summit itself, but the first consideration about the United States thrashing the most important points of the final WGIG report the situation does not promise much. The second phase begins on 16 November 2005, offering no major change in the ordering and governance of the physical infrastructure. Without reforms to the fundamental institutions and infrastructures, these talks will not bring about a new era in electronic freedom.

3.4. The IP Front in the Court

Countless cases have been won and lost by corporations and cyberspace advocates since the advent of the Internet. Today, the foremost front of the battle is defined by intellectual property.

The issue hit the mainstream with the advent of peer-to-peer file sharing systems, of which several generations were developed during the 90s. These have been under continuous legal attack in the U.S. and to a certain extent elsewhere. Offensive and defensive strategies in the legal and technological areas has become increasingly sophisticated. The whole story is way too long to recite here, but two major cases are summarised in brief, in order to give a snapshot of the IP front of the cyberliberty battle.

As always, the focus of efforts is the United States. The first ruling that defined the path of later debates was the so-called “Betamax” ruling in *Sony v. Universal City Studios*. Here, the court affirmed that no technology which has “substantial legal uses” can be held illegal, neither its manufacturer held responsible for infringements carried out with their product. Betamax was a home video cassette format in the 70s and 80s, and court used the analogy of cassette recorders to acquit Sony.

In the next round, showbusiness corporations turned to suing peer-to-peer users themselves, but it soon turned out that lawsuits incited much resistance in the media and they could not go large-scale, which meant that their deterrence value on the population of cyberspace as a whole was limited.

However, a case which seemed to be on the right track for the Electronic Frontier Foundation suddenly changed everything. After triumphs at all preliminary levels, the Supreme Court decision ruled against the EFF in the *MGM vs. Grokster, Streamcast* case. Justice David H. Souter wrote that

“[w]e hold that one who distributes a device with the object of promoting its use to infringe copyright, as shown by the clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties ... [t]here is substantial evidence in MGM's favor on all elements of inducement” (Tech Law Advisor 2005).

The decision is a land-mark in the IP debate, as it partly rules over the Sony decision, and seems to secure both the copyright economy and the progress of technological innovation. On the other hand, it means that software developers shall be judged in the future according to their **intent**. Now, intent is a rather vague term. In hermeneutics, the science of

interpretation, and in aesthetics in general, intent has been ruled out a long time ago as the “intentional fallacy”. It was argued in convincing detail throughout the course of the tradition that judging the product on basis of the intention of the maker misses the point. Having said that, the MGM decision was not a decisive blow on peer-to-peer file sharing systems. Precisely because its vagueness, it only requires more vigilance from software developers in the continuation of their mission - bringing the people what they need.

4. Conclusion of Policymakers' Answers

The paradoxical problem with illegal material on the Internet is precisely that there is no law under which it would be illegal. Nation states has been making increasing efforts to control the part of the information superhighway that wires their country, but human rights, especially freedom of speech and privacy, are posing significant problems for them. As John Gilmore's famous quote goes: “The Net treats censorship as a defect and routes around it.” (WikiQuote 2005) The consequence is that just like any extraterritory, Internet policing too has to be global to be effective. There is good reason to argue that the necessary first step on such a route would be policing the physical infrastructure on an international level. Content management logically comes after management of the physical medium. However, as the discussions in and out of the WSIS demonstrated, key elements of the infrastructure are not global but national - the root zone files and root servers are in the hands of the U.S. Moreover, the U.S. will not give up its monopoly over the infrastructure, nor will it let its national infrastructure policed under international legislation. As far as these fundamental steps are not taken - until the Internet does not become the truly international medium what it is predestinated to be - international legislation over cyberspace will be hard to manage. **Interestingly, that means that the aggressive and excessive domination of the United States and its boycott of international democratic processes indeed preserves the liberty of cyberspace.** However, such a logic raises some serious concerns:

“Perhaps a new International Covenant is needed - possible through the United Nations - on international electric freedom of expression? This could lay down the broad principles governing freedom of expression, which are currently expressed in Article 19 of the International Covenant of Civil and Political Rights (ICCPR), and lead to the establishment of a committee which could then develop jurisprudence in this area. ... The alternative is likely to be intergovernmental agreements - concluded behind closed doors - and establishment of unaccountable global policing bodies to eavesdrop and monitor transnational communications. An inevitable corollary of the globalisation of society is the globalisation of government, just as the internationalisation of crime has led to the internationalisation of policing. The democratic deficit here is enormous and, in this sense, human rights in cyberspace concerns us all.” (Liberty 1999)

Albeit these apparent dangers, there is no plausible scenario which would explain how an international treaty on cyberspace policy could be effective, and that's especially true for free speech. The technological and cryptographic advancement of our civilisation is way ahead of its law-enforcing or self-regulating capacity. An example is discussed in the next section.

5. Recent Developments of Subcultural Answers in the Electronic Frontier - Freenet

It would be possible to survey the evolution of file-sharing from what one paper calls the “Sneaker-network” through FTP and IRC to peer-to-peer (P2P) file sharing systems, and then each generation of P2P software with an outlook on the future (Biddle et al 2002:4). However, Freenet is both an existing project and a future prospect, and it gathers into an archetypical totality both cypherpunk subcultural answers to legal repression of P2P and the mainstream features of P2P systems. Thus, it is a good focal point of Internet activity from which to survey what is possible technologically, and what may become the mainstream if the current situation escalates. First, the workings of Freenet are explained from the user's point of view, then implications for privacy and security are discussed, and finally the strategic position of Freenet in the Cyberspace war of independence is evaluated.

What is Freenet (old and new)?

Freenet follows the logic of peer-to-peer file sharing software, but it is much more and in some respects much less. It provides freedom of speech on the Internet and thus freedom of information. It is an extra cryptographic layer over the basic TCP/IP protocol of the Internet. On regular Internet, a computer on the network is either a server (for example a web server hosting the Wikipedia database) or a client (for example a library terminal with someone browsing Wikipedia). On Freenet, every computer in the system is server and client at the same time - that is how second generation P2P systems work. However, in a traditional approach everybody stores their own files on their own computers. With Freenet, the shared library - called datastore - is completely encrypted, and users have no way to find out what is on their computer. Thus, nodes in the network not only share information but they automatically exchange it. The upside of this approach is that storage place and bandwidth adds up in the whole network, and resources are allocated intelligently. The downside is that there is no search option and that unpopular material tends to “drop out” of the network. In plain English works, this means the following. On the one hand, you have as many host space as you want, and you do not have to worry about too many people requesting your page. On the other hand, webpages that nobody visits disappear. So Freenet is not directly a file sharing application, but a secretive Internet. There are various services available through this Internet - there is the equivalent of the World Wide Web with its websites and hyperlinks, available via your favourite browser, and there is Fred, a messaging board system like Usenet (Clarke et al 2002:40-49).

All that said, it has to be acknowledged that although a vast number of cybernauts use Freenet, it is still a subcultural phenomenon - which means that the average user will probably find it too tedious to bother. Upon install it is downright unusable, and it takes 48 hours to “integrate into the system”. It is highly recommended to run it on a computer which is online 24/7 (remember: every node is a server as well). Average connection speed for small files is on the level of 56k modems from the end of the 90s. Websites need to be published and republished in “editions” to avoid being swallowed down by the system. Worst of all, the existing Freenet network hosts little information that is interesting to the average user. Available content shall be discussed below, and also the reasons why that could change radically in the near future.

A new version of Freenet is due for Christmas, and it will represent a major change. The new Freenet network will hopefully be faster and more reliable, perhaps even harder to use, and certainly more secure. The most fundamental change will be the transformation into a darknet based on the small world phenomenon. The two terms are explained here in more detail. A darknet is network of trusted peers, also called a friend-to-friend network in P2P circles. This means that you only connect to people you know and trust. The downside is that you can only connect to a network if you are invited by someone who is already a member. That might seem scary and unworkable at first, but if considered in the light of the small world phenomenon, it is actually deemed workable even in a global scale (Zhang et al 2002).

The small world phenomenon is a hypothesis that everyone in the world is connected by a small number of social links. It was first described by Hungarian writer Karinthy Frigyes in a 1929 story called *Chains*. A related term is “six degrees of separation”, which implies that anyone in the world is six handshakes away from anyone else. It has had a colourful history as a mathematical problem ever since, but it was also applied to sociology and then networking (Albert & Barabási 2002). In 1967 the psychologist Stanley Milgram conducted an empirical experiment to test the theory, and the results were surprisingly favourable (Milgram 1967). His methods and conclusions has been contested since then, but subsequent experiments lead to largely the same results. On the Internet, Duncan Watts conducted a similar experiment with emails, and he found the same number - six - as the average link count (Watts 2003). Technically, existing darknets such as WASTE are limited to small networks that do not communicate with each other. However, the Ian Clarke, the father of Freenet proposed that the next version would be the first darknet to be scale-free (Clarke 2003).

Why it is unpolicable?

The primary mission of Freenet is to provide privacy, and all other issues (like being user-friendly or efficient) come second. So far, it has an absolutely clean record: nobody is reported to have been prosecuted or persecuted for using Freenet. That is why it is dealt with here: as an uncompromising effort it is an archetypical instance of cryptographic answers to censorship. However, privacy has a lot of differing interpretations. What sort of privacy does Freenet attempt to provide? In general, Freenet attempts to provide as many kinds of privacy as possible. The particular cases are explained here. First, due to the encryption between peers messages cannot be intercepted, which guards the user and the information from large-scale surveillance systems like Echelon and Carnivore. Second, the distributed and encrypted datastore concept ensures that even if the computer of a user is confiscated and computer forensic methods are used to extract information, the user can plausibly deny knowledge of ownership. (Possible enhancements in future versions will include a further trick, that only parts of files will be retained in the datastore, so that the user cannot be charged with possession of any one file whatsoever.) Third, Freenet is a data haven because it is extremely hard to censor uploaded material. Fourth, it follows from point one that it provides anonymous communication, so that your activity cannot be tracked back to you. Additionally, as a fifth feature Freenet provides options for pseudonymous communication, so that users can electronically sign information with a pseudonym, which ensures that a given bulk of information was authored by the same person. The darknet structure of the next version shall provide for a sixth privacy: if you stucked to the rules, it would be increasingly difficult to

determine that you are actually a Freenet user. In jargon, it means that Freenet will not be harvestable. Harvesting means that by monitoring traffic, the attacker compiles a list of users and then physically prevent them from running the network, for example by murdering or arresting them. Freenet will still be vulnerable to correlation attacks, malicious activity by the user's trusted peers (her immediate neighbours), although there are schemes under development to counter that as well. A report by the RAND Foundation shows that “[a]t present, like many other Chinese Internet users, most dissidents apparently fear that using encrypted e-mail would draw the attention of the security services” (Chase & Mulvenon 2002). That report justifies the development goals of freenet - developing a non-harvestable darknet.

What does it carry?

First of all, the infamous Chinese network is in fact in Chinese, and nobody has yet posted a detailed report on its contents in a mainstream European language. The Western network was once loosely surveyed by Jon Orwant at O'Reilly, but apart from that, accounts are only based on anecdotic evidence and user experience. One of the main flaws of the O'Reilly survey is that it is not aware of Fred, the messaging board, through which much of the file sharing is done. Therefore this section consciously confines itself to the World Wide Web inside Freenet, with the note that material flowing through Fred is similar in proportions of topics, only more inclined for general copyright infringing material.

The author of this document agrees with Orwant's paper in that most images are porn, but most links lead to non-porn. Freenet pages tend to be bereft of images if they are not necessary. Considering these factors, it can be plausible argue that there is as much porn on Freenet as on the Internet in general. On the other hand, there is as much political/censored content as there is porn, at least if one counts the number of pages not the number of files. The rest of the spectrum is filled up with miscellaneous copyright infringing material (Orwant 2000).

“The success of any great moral enterprise does not depend upon numbers,” however, as William Lloyd Garrison said (Lewis 2005). The quality of these material is perhaps more important than their quantity. First of all, despite all the difficulties, Freenet does acieve its goal as a data haven for material that cannot be published elsewhere. Sometimes it is child pornography, but not to the proportion expected. The papers on the Church of Scientology that were censored in the United States because of copyright reasons can also be found here, as well as 'terrorist material' relating to bomb-making. A range of anarchist content is also available from the pages of the Anarchist Black Cross (an organisation focusing on jail issues) to reports of activities. That Freenet is but a small subculture at the moment is convincingly shown by the fact that the most popular 'free speech' material is better termed 'meta free speech' material, meaning writing and programs relating to security and privacy issues. Most important, however, are not simple informational pages but more personal sites that often attempt to communicate in order to achieve a specific effect. These are the most important because these sites seem to be unique to Freenet. Perhaps they are better called confessional sites. There are 'flogs' (Freenet blogs) of child abusers talking about their experiences as a form of self-therapy, murderers revealing details of their deeds in order to save the innocently accused, and a budding satellite hacking project. Public speech admitting

a crime inevitably leads to impeachment, but not if published truly anonymously. Thus Freenet makes real a possibility of free speech protected by (for instance) the Constitution of the United States, but not actually provided for in any concrete form.

According to the U.S. Supreme Court “an author's decision to remain anonymous, like other decisions concerning omissions and additions to the content of the publication, is an aspect of the freedom of speech protected by the First Amendment” and “the anonymity of an author is not ordinarily a sufficient reason to exclude her work product from the protections of the First Amendment” (Liberty 1999:98).

Preceding sections of the present paper explored the severe difficulties which law-making and law-enforcement face in a globalised cyberspace. Traditional methods of handling extraterritories are difficult to apply, and the vast numbers of inhabitants makes effective content policing virtually impossible. Such an environment of decreased legal security and increased technological bias calls for not laws but practical solutions to its problems. As John Gilmore said on the First Conference on Computers, Freedom, and Privacy: “I want a guarantee -- with physics and mathematics, not with laws -- that we can give ourselves real privacy of personal communications” (Gilmore 1991).

What is the logic of the mainstream marketplace?

In case the current show-down on intellectual property infringers continue, more and more material will be outlawed by courts and prosecuted by authorities. If popular material is found on the black market, users will migrate there and nourish it by their activities, be that buying or sharing. The scenario can be analogous to the drug war. The development of Freenet towards the small world darknet model moves in that direction. The drug industry is also organised as a network with a global reach utilising trusted peers. Anyone in developed societies who is willing to take the energy and the slight risk is able to acquire the most common types of drugs through informal networks. It would be interesting to read research reports about testing the small world phenomena in the drug industry.

In a more sophisticated scenario, there is a possibility of the establishment and dominance of a 'white market'. That applies if the corporate actors realise their situation and start offering better services, thereby winning the game of 'competing regulations'. On one end of the spectrum - electronic financial transactions - legal solutions are already dominant, but content providers face the utmost difficulties in expanding that model. As Pierre Trudel writes:

“In some cases, people will avoid a site because it seems too controlled and the rules in force do not suit them, whereas in other situations, particularly when integrity and credibility are required, they will be inclined to visit sites applying regulations that offer optimum guarantees of integrity and reliability. In these respects, the sites are in competition with one another, which entails competing regulations” (Trudel 1998:192)

Trudel does not consider the international legal front of the battle as a significant factor in the long-term outcome, but concentrates on local regulations by entities that offer particular services, be those private sector players or civil initiatives.

6. Conclusions

All in all, it seems that while the Electronic Frontier Foundation holds back the national and corporate forces on the legal battleground, the broader subculture concentrates on technological answers. That gives two distinct fronts, one outside and one inside cyberspace. Interestingly, cutting edge developments like the Creative Commons licensing revived the ancient practice of free software licenses to apply to any content, thereby connecting the two disparate fronts.

While engagement in both fronts is becoming increasingly complex, experiences show that the law of cyberspace is still code. Consequently, prospects are that the technological front will become decisive in the battle. The good news is that the forces of cyberspace are more powerful in that particular front. What does it mean that cybernauts are fighting on home ground?

Planting the seed of marxism, Hegel describes the dialectic of the Master and the Slave in Section II. a. of the *Phenomenology of the Spirit* (1977). He claims that the individual is enslaved because he is afraid to lose his life, entrapped in the fear of confronting crude reality. However, once enslaved, the Master will force him to preserve his animal life by continual labour. In labour, the Slave is in direct contact with reality, performing the work which transforms crude reality into bliss, which is consumed by the Master. The setup results in the Master being distant from reality. More exploitation results in more distance, and more distance result in less knowledge about actual reality. While the Master is consuming the bliss, the Slave is doing the work. Meanwhile, through his work the Slave becomes familiar with primordial reality, and his fear slowly subsides. He realises that as a Slave he has the power to change reality. Through labour and his enslavement by the Master, the Slave has become the Master of reality. At that point, he becomes conscious of his powers, and the notion dawns on him that he does not need a Master. He can produce and consume bliss by working on reality, and his Master has no power over him because the Slave does not fear any more and the Master is powerless without the knowledge of reality.

Hegel's thought was unique at the time because he thought that his concepts express abstract philosophical truth about the individual and the world and actual historical developments at the same time. The Cyberspace War of Independence described in the present paper is a story that reflects Hegel's notions with surprising accuracy. Governors and other policy makers including CEOs of multinational corporations have distanced themselves from the work in cyberspace and in the process became powerless to rule over it. The inhabitants of cyberspace realised that they need not fear their worldly governors and the power of their law, because they have their own code - the power to work with the actual fabric of their unreality. Technology became their dominion - their weapon and their place of residence.

Marx reformulated and expanded Hegel's work in terms of alienation and class consciousness in the context of an antagonistic battle between the bourgeoisie and the proletariat. For the bourgeoisie, alienation is the alienation from work and thus from reality. For the proletariat, alienation means that the energy of a human being is consumed in maintaining his animal life, so that he becomes alienated from himself (Lukács 1972). As bits are easily transformed in cyberspace, the cyber-proletariat acquired the spare time to realise

itself. As cyberspace is essentially a medium of communication, global class consciousness and the tools for self-liberation spread like wildfire. However, the end of the story may be different. The overturning of the bourgeoisie in the framework of a sudden violent revolution is not necessary. After all, cyberspace runs on the hardware and distributes the content that is manufactured by the post-industrial bourgeois society.

The new theory to describe the new historical development and the novel practices to cope with it was pioneered by the Situationists. Governors need not to be overturned, merely left alone. Technology enables the masses to fight without direct confrontation - technology hides the masses and the mass black market. Freenet and other peer-to-peer networks to some extent fit in the order of the techniques of resistance. More specifically, they are techniques of disappearance. Guy Debord summarised the identity of the commoner in his 1967 book *The Society of the Spectacle*:

“Détournement is at once a technique of disappearance and reappropriation. As a technique of disappearance, it produces mobility and a multiple impersonality, meant to spread a new confusion: it is impossible to assign a forced residence to a ”dé tourneur“, he can't be forced to sign his works as one would sign a confession. Détournement is the art of a man who, as a stealer of texts and images, has nothing left to lose, especially not his reputation as artist or author. In fact, what better thing to do, when one has already committed oneself to perdition? All the more so since d tournament is also a war-technique of reappropriation of words, images and works whose poetical potential can be reactivated, if one removes them from the official channels they're caught in, thus allowing their use by all. Détournement is, theoretically, in everyone's reach. It leads to a communism of writing that shifts the meaning of writing as we know it, as was the wish of Lautréamont, who wanted poetry to be made by all, not by a happy few.” (Debord 1995)

maxigas@anargeek.net, 2005-11-05.

Document and updates available from www.maxigas.hu.

Protected by the Creative Commons Attribution 2.5 License.

List of References

Albert, R. & Barabási, A.-L. “Statistical mechanics of complex networks”, *Reviews of Modern Physics* 7J January 2002 47-97

Balsano, A.M. (1998) 'The International Dimensions of Cyberspace Law' In *Internet - which court decides? - which law applies?* Boele-Woelki, K. & Kessedjian, C. (ed.) Hague: Kluwer Law International

Banks, K. (2005) *The internet governance debate is one where civil society advocates can make a real difference* APC (Association for Progressive Communication) [online] Available at <<http://www.crisinfo.org/content/view/full/787>> [5 November 2005]

Barbrook, R. (1996) *Deregulation or Reregulation?*.

Baudrillard, J. (1993) *The Transparency of Evil: Essays on Extreme Phenomena*. In: Ctheory. [online] available from <www.ctheory.net/articles.aspx?id=32> [5 November 2005]

Biddle et al. (2002) 'The Darknet and the Future of Content Distribution' In: *Proceedings of the 2002 ACM Workshop on Digital Rights Management* Held 18 November 2002 at the Wyndham City Center Washington DC, USA. [online] Available from <<http://crypto.stanford.edu/DRM2002/prog.html>> [5 November 2005]

BLUG & Vesta Brevdueforening (2001) *The highly unofficial CPIP WG* [online] available from <<http://www.blug.linux.no/rfc1149/>> [5 November 2005]

Chase, M.S. & Mulvenon, J.C. (2002) *You've Got Dissent! Chinese Dissident Use of the Internet and Beijing's Counter-Strategies* RAND Foundation. [online] Available from <<http://www.rand.org/publications/MR/MR1543/>> [5 November 2005]

Clarke (2003) *Freenet's Next Generation Routing Protocol* [online] available from <<http://freenetproject.org/index.php?page=ngrouting>> [5 November 2005]

Clarke et al (2002) 'Protecting Free Expression Online with Freenet' *IEEE Internet Computing* [online] January-February 2002 40-49. Available from <<http://csdl2.computer.org/persagen/DLAbsToc.jsp?resourcePath=/dl/mags/ic/&toc=comp/mags/ic/2002/01/w1toc.xml&DOI=10.1109/4236.978368>> [6 November 2005]

Ctheory (2005) *Ctheory* [online] available from <<http://www.ctheory.net/>> [6 November 2005]

Debord, G. (1995) *The Society of the Spectacle* Zone Books

EFF (2005) *Our Mission* [online] available from <<http://www.eff.org/mission.php>> [5 November 2005]

Foucault, M. (1975) *Discipline and Punish: the Birth of the Prison*. New York: Random House

Gadamer, H.-G. (1990) *Wahrheit und Methode: Grundzüge einer philosophischen Hermeneutik*. 6th edition. Tübingen: Mohr

Everard, J. (2000) *Virtual States: The Internet and the Boundaries of the Nation-State* London: Routledge

Gilmore, J. (1991) 'The Private and Open Society' [online] *First Conference on Computers, Freedom, and Privacy* Held 28 March 1991. Available from <http://www.eff.org/Privacy/?f=privacy_gilmore.speech> [5 November 2005]

Hegel, G.W.F. (1977) *Phenomenology of Spirit* Translated by A.V. Miller. Oxford: Clarendon Press

Internet Society (2005) *Why join?* [online] available from <<http://www.isoc.org/isoc/membership/whyjoin/>> [5 November 2005]

ITU - International Telecommunications Union (2003) *World summit on the information society (WSIS) - Phase 1 in Geneva, 10–12 December 2003* [online] available from <www.wsisgeneva2003.org/pdf/WSIS_OFCOM_brochure-e-1006.pdf> [6 November 2005]

Lewis, J.J. (2005) *Wisdom Quotes - William Lloyd Garrison* [online] available from <<http://www.wisdomquotes.com/001973.html>> [6 November 2005]

Liberty (ed. 1999) *Liberating cyberspace : civil liberties, human rights, and the Internet* London: Pluto.

Lukács, Gy. (1972) *History and Class Consciousness* MIT

Milgram, S. (1967) "The Small World Problem" *Psychology Today* May 1967 60-67

Orwant, J. (2000) *What's on Freenet?* [online] available from <<http://www.openp2p.com/lpt/a/462>> [5 November 2005]

Peake, A. (2004) *Internet governance and the World Summit on the Information Society (WSIS)* [online] Net: APC (Association for Progressive Communication). Available from <<http://www.itu.int/wsis/documents/background.asp?lang=en&theme=ip>> [6 November 2005]

Rousseau (2005) *The Social Contract* [online] available from <http://etext.library.adelaide.edu.au/r/rousseau/jean_jacques/r864s/complete.html> [5 November 2005]

Tech Law Advisor (2005) *Grokster Decision* [online] Available from <http://techlawadvisor.com/blog/2005/06/27/grokster_decision.html> [6 November 2005]

Terret, A. (1995) 'Law and the Internet'. In *A Lawyers' Introduction to the Internet*. G. Burgess Allison (ed.) Chicago: Section of Law Practice Management, American Bar Association

Trudel, P. (1998) 'Liability in Cyberspace'. In *Internet - which court decides? - which law applies?* Boele-Woelki, K. & Kessedjian, C. (ed.) Hague: Kluwer Law International

Toner, A. (2003) 'Unzipping the World Summit on the Information Society' MetaMute [online] M26 Summer/Autumn 2003. Available from <<http://www.metamute.com/look/article.tpl?IdLanguage=1&IdPublication=1&NrIssue=26&NrSection=10&NrArticle=873>> [6 November 2005]

U.S. - United States (2005) *U.S. Principles on the Internet's Domain Name and Addressing System* Delivered by Assistant Secretary Michael Gallagher. [online] Available from <http://www.ntia.doc.gov/ntiahome/domainname/USDNSprinciples_06302005.pdf> [6 November 2005]

W3C - World Wide Web Consortium (2005) *About the W3C* [online] Available from <<http://www.w3.org/Consortium/about-w3c.html>> [6 November 2005]

Watts, D.J. (2003) *Six Degrees: The Science Of A Connected Age* N.Y.: W.W. Norton & Company

Wikipedia (2005a) *Rousseau* [online] available from <<http://en.wikipedia.org/wiki/Rousseau/>> [5 November 2005]

Wikipedia (2005b) *Cyberspace* [online] available from <http://en.wikipedia.org/wiki/Cyberspace#Nova_Convention> [5 November 2005]

Wikipedia (2005c) *Antarctica - Government* [online] available from <http://en.wikipedia.org/wiki/Government_Antarctica/> [5 November 2005]

Wikipedia (2005d) *World Wide Web Consortium/* [online] available from <<http://en.wikipedia.org/wiki/WWWC>> [5 November 2005]

Wikipedia (2005e) *RFC Editor* [online] available from <http://en.wikipedia.org/wiki/RFC_Editor> [5 November 2005]

WikiQuote (2005) *John Gilmore* [online] available from <http://en.wikiquote.org/wiki/John_Gilmore> [5 November 2005]

Zhang *et al.* (2002) 'Using the Small-World Model to Improve Freenet Performance' In: INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings vol.3 1228-1237

Notes

(1) *Northrop Frye writes in The Double Vision of Language, Nature, Time, and God// that as long as we distance ourselves from the foundations of our scientific ideas by attributing them to someone else and isolating them in quotation marks, we are assuming a bad posture. Instead, we can re-state thoughts and words as individual realisations of a truth that was identically conceived by us and the person referred.*

(2) There is a prolific academic practice (that is in decline now) of pinpointing this or that historical moment, author or work as the origins of Modernity. Despite the great wealth of these writings and the wide range of proposed origins the academic community was unable to reach any consensus on the issue, which might be an indication of the futile nature of such arguments. According to the

personal experiences of the author of the present document, these presentations are mostly cynical, and sometimes loony.

(3) “The Electronic Frontier Foundation is a group of passionate people — lawyers, technologists, volunteers, and visionaries — working in the trenches, battling to protect your rights and the rights of web surfers everywhere. The dedicated people of EFF challenge legislation that threatens to put a price on what is invaluable; to control what must remain boundless.” (EFF 2005)

(4) A (then?) member of the Hypermedia Research Centre of the University of Westminster, London.

(5) Ctheory - <http://www.ctheory.net/>, “an international peer-reviewed journal of theory, technology, and culture”, “edited by Arthur and Marilouise Kroker”. (Ctheory 2005)

(6) Of course, that applies to operations directly carried out in (cyber)space. The opposite is true for user experience in cyberspace, as everyday operations have indeed become part of the daily routine for a vast number of people. On the other hand, we still need special equipment - most notably computers - to carry on with those operations, and highly qualified technicians to maintain the system.

(7) Such a totalitarian approach to regulation is a widely accepted practice in democratic countries: it seems that democracy is considered to be a global value by its advocates, while policy makers in totalitarian countries are content to rule their own countries according to their own “community values”.

(8) These are almost exclusively nature preservation laws.

(9) Actually, nowadays an alternative protocol is also in use, called UDP (User Datagram Protocol). However, UDP is just a more lightweight implementation of TCP (Transmission Control Protocol). UDP is used for streaming (live transmission) purposes.

(10) Such as the protocols TCP/IP and UDP for communication over the network, and HTTP for the World Wide Web, FTP the File Transfer Protocol and SMTP and POP3 for email.

(11) Such as www.maxigas.hu or 195.70.43.251 for the same page.

(12) Joke RFCs are also issued at least once a year (usually April Fool's Day), for example RFC 1149 IP Datagrams on Avian Carriers described an IP-based communication protocol for carrier pigeons. (Wikipedia 2005e) This was actually implemented: (BLUG & Vesta Brevdueforening 2001).

(13) In fact such a service was available before DNS servers, but each computer had to have its own database, contained in the “hosts” file. The introduction of DNS only made the process dynamic and automated, so that information is synchronised over the network.

