Internet Regulation: Does Self-Regulation Require an Institutional Framework ?*

Éric Brousseau

University of Paris X, FORUM & ATOM

Université de Paris X, Bâtiment K, 200 avenue de la république, F-92001 Nanterre Cedex, France
Tel: (33) 01.40.97.59.22
Fax: (33) 01.40.97.59.07
E-Mail: EricBrousseau@Compuserve.com
http://atom2.univ-paris1.fr/FR/membres/eric/eric.htm

This Version : 28/07/2001

Abstract:

Is Internet an ideal model for a self-regulated economy? It seems possible to decentrally organize and render enforceable a property rights system on which inter-individual negotiations could be based. Moreover, traditional State intervention is no longer operable since Internet users can bypass the usual regulatory frameworks. At the same time, the long-term sustainability of the competitive process is not guaranteed in the digital economy, and cyber-activities generate externalities that affect the non-users of the Internet. These call for the organization of an institutional framework that would avoid the capture of self-regulations by interest groups seeking to exercise monopoly power. Delegating the management of some essential resources — especially the addressing system — to an entity responsible for the regulation in the last resort would enable the construction of such a framework.

JEL : H4, K2, L4, L5, L9

* This paper benefited from fruitful discussions with Jean-Michel Cornu (FING) and Daniel Kaplan (FING & ISOC). A draft version of the paper led Bruno Chaves (ATOM), Nicolas Curien (CNAM), Godefroy Dang N'Guyen (ENST-B), , Mhand Fares (INRA), Didier Lebrun (ISOC), Hervé Nabarette (ATOM) to make useful suggestions. I warmly thank them. Usual caveats apply.

0. A return on some common wisdom

The way the Internet is governed is increasingly considered as a model of a new regulatory regime based on decentralized and State-free regulation. At first sight, the Internet has been developing on the basis of governance mechanisms based on contractual agreements or communities' self-regulations whose enforcement is based on competition among alternative coordination mechanisms. Agents disappointed by the parties they are interacting with can easily set-up new networks or relationships thanks to the essential features of the Internet; especially because it is a global network relying on open standards. In this model, states seem to be bounded to a minimal level of intervention. They are essentially required to adapt the existing legal framework to the specific features of the Internet. For instance, they have to enlarge the range of authorized cryptographic techniques to allow Internet users to benefit from secure payment services or authentication techniques or to protect the confidentiality of their exchanges of information. Two main "technical" causes seem to lead to this minimal intervention. First, the global and decentralized nature of the network induces the ineffectiveness of traditional regulations because the users of the digital networks can bypass most state norms. Second, some dimensions of governmental intervention in information and communication networks are no longer justified, because many sources of scarcities are removed, and because digital technologies allow a very fine control over the access to and uses of information. Consequently, the cyberworld seems to be a space in which efficient self-regulation could be sustained.

However, careful observation of the actual facts lead one to qualify this simplifying view, since, while Internet is indeed a space in which regulation is highly decentralized, some functions are highly centralized. The establishment of technical standards and above all the management of the addressing system are centralized because centralization is needed to ensure the consistency of the network. States also play an essential role. The US Government is the main inventor in the Internet, which was initially primarily a network dedicated to the research community linked to the Department of Defense, before being opened to the whole research community. It was decided to open the network to commercial users and private investments, but the Department of Defense remains the owner of the addressing system — i. e. the major tool to govern the network, see appendix 1 — even though its management is delegated to non-governmental organizations. Other governments intervene as well. In particular access to Internet is heavily regulated in most countries, and many governments attempt to regulate contents.

It is true however that the way Internet is governed and regulated is innovative in several ways because self-regulation is not performed under the control — in the last resort — by a State. Moreover, the global nature of the network generates a direct and brutal confrontation among regulatory principles that are partly non-compatible.

It would be wrong to think that Internet is a satisfactory model of self-regulation. On the one hand, as pointed out above, Internet regulation is not as decentralized and private as is usually claimed. On the other hand, as will be argued in that paper, there are many inefficiencies in the present regulation of the Internet.

Relying on a detailed investigation of the governance mechanism in force in the present Internet (Cf. Brousseau & Curien [2001]), on the political and legal controversies around it, and on the advances in the economics of regulation and institutions, this paper is an attempt to

analyze the principles that should inspire an institutional framework which is well adapted to the regulation of the Internet. This will lead to an analysis of why some aspects of the coordination of activities should be centrally managed and why hierarchical principles should be implemented to organize the relationships among regulatory bodies. This will also lead to an analysis of why the new technological basis impacts on the optimal balance between the centralized vs. decentralized management of various resources.

To make these arguments clearer we will come back to some justifications for regulating the Internet (§1). We will then come back to the reasons why traditional state regulations, on the one hand, and totally decentralized private regulations, on the other, are neither efficient, nor operable. This will lead us to point out complementarities between public general regulations and private specific regulations. In addition, we will suggest an outline for an efficient regulatory framework in which a hierarchy will be organized among the various bodies involved in the regulation of the Internet (§2). For those readers who are not familiar with the technology and the present regulatory framework of the Internet, three descriptive appendixes explain the basics.

In the following pages, we will deal both with the regulation of network activities by themselves and with the content. While Internet technologies enable the separation of the management of the network services from the management of the information services, there are strong technical and economic interdependencies between the two. For instance, a specific administration of network services allows control of the access to contents. Moreover, network services have an impact on welfare because they carry the contents. Such types of interdependencies call for a simultaneous analysis of the regulation of the contents and of the uses.

Moreover, the notion of regulation also needs to be clarified. Regulation often refers to the direct intervention of the State in the management of some resources. By setting rules and commanding the players (when rules do not apply), regulatory agencies govern the allocation and uses of resources in specific domains. Here regulation is understood in a more general sense. Regulation refers to the settlement of rules that delineate and allocate the right to use economic resources to agents interacting in a common economic space. In concrete terms, regulating means setting a property rights system, a contract law, a competitive law (to fix fairness principles), and a principle to allocate and use common resources. Regulating implies four major activities: setting rules; supervising their enforcement and punishing infringers; settling conflicts, since there are always some incompletenesses in a system of rules; and commanding agents when rules do not apply. Consequently, regulating here groups several modes of intervention by an entity that is different from the players — even if, in the case of self-regulation, it emanates from the players themselves — : regulation in the usual sense, but legislation and judiciary intervention as well. In a sense, our understanding of what regulations mean is very close to what Barzel [1989] and North [1990] call a property right system[1].

[1] This is not surprising when one consider the actual work performed by regulatory agencies in deregulated industries. Their essential task is to disentangle the complex set of uses rights over the various components of the networks — i.e. to delineate property rights — and then, to allocate these rights to the various network operators. In addition, they supervise the enforcement of these various uses rights when they settle conflicts among network operators

1. Should Internet be Regulated ?

Regulating a network consists in setting a set of interoperability rules that enable its components to perform in a consistent way, and manage priorities and conflicts. Without a minimum set of common rules, there are no networks. Internet cannot escape that iron rule. Like any collective space of freedom, a myriad of rules and regulations implemented by a complex set of organizations ensures the regulation of the present Internet.

The fuzzy set that regulates the Internet draws from a recent, but rich, history during which the technical principles that govern the management of a decentralized network were progressively established by computer scientists working within US governmental agencies. This effort was then transferred to private initiatives when the Internet became commercial and open to private investments. Early and later regulation initiatives bypassed the traditional mechanisms of international standardization and regulation (Brousseau & Curien [2001]). Three main reasons explain this. First, the velocity of innovation in both digital networks and multi-media technologies was quite incompatible with the slowness or these international or intergovernmental agencies. Second, until 1998, Internet was essentially a US network, and it is still dominated by US players today (even if it is increasingly becoming global). Third, the liberal ideology of, respectively, the inventors and the entrepreneurs of the Internet, explains their mistrust of international or intergovernmental bureaucracies.

This history led to the present situation in which the Internet is *de facto* co-regulated by National Governments — that intervene however without strongly co-ordinating among themselves — by professional entities — whose competencies overlap and which are not always legitimate — and instances of technical standardization — that are very dynamic, but that lack strong institutional roots. This present institutional framework is problematic for at least two reasons: it is partly inefficient in the sense that there are incompletenesses, conflicts, and defaults in enforcement in the set of implemented rules; and the current processes used to establish these rules do not guarantee that the interests of all the stakeholders are fairly taken into account.

If the current institutional framework suffers from weaknesses, one has to investigate why the Internet should be regulated before studying how these weaknesses could be overcome. Indeed, many specialists advocate that, beyond a common minimal technical regulation — basically the publication of open standards and a transparent management of the addressing system — the Internet and its uses should be decentrally self-regulated. Indeed, the combination of an abundance of essential resources, strong competition among information and network service providers, and the ability to decentrally configure the services supported by the network according to the preferences of the users is supposed to allow the adaptation of the uses to each and everybody's preferences. Information and network services can be customized without fearing conflicting uses and the low level of barriers to entry prevent any capture (as summed up by Frishcman [2000] and Elkin-Koren & Salzberger [2000]).

These arguments have however to be discussed in more detail (§ 11). Indeed, there are scarcities (§ 111) and externalities (§ 112) in digital activities. Moreover, the long-term sustainability of the competitive process is not guaranteed (§ 113). As will be argued, these do not call systematically for regulation since decentralized solutions to these problems can be implemented (Coase [1960]). However, the capability to implement these decentralized solutions has to be addressed (§ 12).

11. Three collective problems

111. Scarcities

If a resource does not cause conflicting claims among its potential users, scarcity does not arise and there are no economic problems. As pointed out by Frischman [2000], there are scarcities in the cyberworld, even if some sources of scarcity in the real world are removed. In addition, Lemley [1999] pointed out that the solutions that were used to solve these problems in the non-commercial Internet are not necessarily legitimate and viable in the present Internet that serves a large number of heterogeneous users[2].

The first source of scarcity in the Internet is the addressing system. Because of the required standardization and of the hierarchization of the system used to identify each of the information processing devices connected to the network, there is a limited number of roots to create IP addresses. This causes a problem of allocation. One often quoted example is the University of Stanford that has the capacity to create more IP numbers than the Popular Republic of China, because when the current addressing system was created the former had the opportunity to reserve large numbers of IP prefixes. With the implementation of the Internet or third generation, a new addressing system will become available (IP v 6). This should reduce this scarcity problem[3]. The actual source of scarcity is in fact due to the Domain Name System. The numbers of available names and expressions of the natural language that can be the base of meaningful addresses is obviously bounded. Moreover, there are many potential conflicts of interests. Why should a single individual capture a family name? Who should benefit from the exclusive right to use famous names such as names of celebrities, locations, events, or trademarks. In addition to scarcities there are potential conflicts among the exclusive capture of these names over the Internet and the fact that in other spaces their uses can be already reserved (trademarks) or, on the contrary, considered as not individually appropriable (common resources). Moreover, the global character of the Internet generates conflicts among legitimate exclusive users that were previously using the same name in different spaces.

---

[2] The specific ethic of the Net-users (*Netiquette*) that was in force until 1995 was a mean to economize on some specific scarce resources such as bandwidth. This code of conduct is not any longer viable and legitimate in the present commercial Internet. Since some users are ready to pay to benefit from a prioritary access to scarce resources exploited by private operators, and since the price they pay enables to finance an increase of capacities, it is not any longer efficient and sustainable to apply a rule aimed at forcing each party to save on the uses of these resources (such has bandwidth at peak hours).

[3] It has however to be pointed out that the actual implementation of this new addressing system is still uncertain. Indeed, ISPs and hardware manufacturers tend to promote an alternative solution based on the development of independent addressing systems in each sub-network associated with the implementation of Network Address Translator (NAT). This is very similar to the solution implemented in traditional communication networks like the telephone system (see Appendix 1). This would solve the scarcity problem but would strongly decrease the transparency and the reliability of the network (because the addressing system will be composed of various layers). Indeed, end-to-end connectivity and transparency are at the core of the Internet architecture. Moreover, this would give a wide power of control to ISPs. See Internet Transparency. RFC-2775: ftp://ftp.rfc-editor.org/in-notes/rfc2775.txt / Blumenthal M. S. & Clark D.D. [2001], "Rethinking the design of the Internet: The end to end arguments vs. the brave new world", in B. Compaine & S. Greenstein, eds. *Communications Policy* in Transition: The Internet and Beyond, MIT Press, Sept. (http://www.ana.lcs.mit.edu/anaweb/PDF/Rethinking_2001.pdf)

The second source of scarcity is the available communication capacity — the bandwidth. At any moment in time, it is bounded by the capacity of the infrastructure and by the capacity of the critical nodes of the network (whether they are interconnection points or servers[4]). Two types of problem then arise. First, a criterion to allocate the available bandwidth at each period has to be established[5]. Second, the Internet operators have to be incited to invest to limit the risk of network congestion. Indeed they are not able to capture the marginal collective surplus of their investments, since the technical features of the Internet enable information packets to automatically select the available bandwidth to be routed. In the absence of correction mechanisms, Internet operators would therefore have strong incentives to behave opportunistically (Frischman [2000]).

112. Externalities

Internet activities generate a bunch of externalities. The infrastructure is becoming an essential facility to provide citizens with collective or merit[6] goods as services provided by governmental agencies, universities, non-profit organizations, etc. Citizen-to-citizen services have also to be mentioned. Generalized and global connectivity should be quoted as well. Consequently, the network and information services provided through the Internet generate a large number of externalities, as is usual for other infrastructure networks.

In the case of the Internet, these traditional problems are reinforced by the large number and the complexity of the externalities involved and which are due to the wide set of available services, and the diversity and large number of users. Moreover as pointed out by Gensollen [2000], externalities among services concern commercial activities as well. These benefit from the providing of non-commercial and free information services because free contents attract potential consumers into the cyberworld. Moreover, specific free services — such as research engines — enable consumers to identify and select their on-line merchants. Lastly, there are also strong interdependencies between network services and information services, especially because the accessibility and quality of the latter strongly depend on of the price and the quality of the former.

Such externalities can lead to an inefficient management of the network and information resources because the agents that benefit from positive externalities can under-evaluate the value of the services, and can even refuse to pay for them (if exclusion is impossible). This

[4] Odlyzko [2001] argue that the "heart" of the Internet — the backbones and the ISP's networks — are not really saturated today, and that technological evolution should decrease the potential risks of congestion. However, interconnection capabilities as well as the capacity of the content sites are potential sources of congestions. There are congestion risks on "the last kilometer" of the network as well, since the chances to have high-speed network spread till every final users is very low.

[5] In the commercial Internet, this question of priority management is essential because it influence the quality of all the services for which "real time" communication is essential : IP telephony, videoconference, TV and multimedia broadcasting, etc. (Crémer & alii [1999]). This can be of importance for some industrial and business applications.

[6] Merit goods are those goods which evaluation (their merit or demerit) do not derive from the consumer sovereignty but involves alternative norms. This concept has been defined by Mussgrave [1959] (*Theory of Public Finance*, New-York, McGraw Hill) and Head [1966] (On Merit Good, *Finanz Archiv*, New Series, 17:3, p. 1-29)

can lead their producers to under-invest as compared to what would be socially optimal (Frishman [2000]).

As will be discussed further these scarcities and externalities do not systematically call for a centralized and governmental allocation of resources. They call however for some types of collective regulation because decentralized bargaining does not systematically result in a consistent or efficient equilibrium.

113. Competition and Transparency

Two generic solutions exist when externalities and scarcities have to be managed. The first one is the direct intervention of a last resort authority — traditionally the State — that defines how economic agents are allowed to use the resources. Typically, the regulation of Public Utilities sets the content of the services provided by operators to their client and fixes the frame of the relationship among operators. The second solution consists in organizing markets through the delineation of a complete set of property rights that allows users to negotiate each and every dimension of the uses of the concerned resources. This is the coasian solution (Coase [1960]) that relies on two conditions : a complete system of property rights has to be designed and a competitive allocation of resources has to be guaranteed. The first point will be discussed in the next section. Let us argue here about the sustainability of the competition in the cyber-world.

The question of the long-term viability of the competitive process in the cyberworld is crucial for two reasons. First, because it is one of the necessary conditions of an efficient management of scarcities and externalities. Second, as in any market, it is a requisite to guarantee the long-term efficiency of the activities performed over the network, both for stati (allocative) and dynamic (innovative) reasons.

The digital network economy is often considered an economy in which competition is sustainable because the decentralized nature of digital networks and the low level of barriers to entry seem to enable any victim of the exercise of monopoly power to bypass its service provider. Put another way, contestability (Baumol et al [1982]) is supposed to be strong. Several scholars contest this oversimplistic conventional wisdom and point out that network or information service providers have some room for manoeuver to create and exploit bottlenecks. For instance Crémer et al [1999] or Tirole et al [2001] emphasise that Internet operators can strategically decrease the transportation capacity of the network. By downgrading the quality of the interconnection with smaller networks, large network operators increase the relative quality of the services provided to their subscribers (whether they are final users or information providers) as compared to the service delivered by small networks[7]. Those who operate larger networks are therefore able to attract the subscribers of smaller networks and to initiate concentration. Similar strategies can be observed on the market for content (Frishman [2000], Posner [2000]). Web-sites that benefit from the largest audiences are incited to and can develop various strategies to reduce the audience of the less famous information service providers and to expel them from the market[8].

---

[7] Indeed, the subscribers of the "small" networks have a larger probability than those of the "big" networks to send requests (request to access to content or request to send information to a correspondent) to users that are reachable through the network that is not the same that the one they subscribe to. If interconnection is of poor quality, the services they get is faded (denial of access, long delays, etc.).

[8] For instance, they can refuse to implement html links with the sites of their competitors. They can also sign

Such strategies can be harmful to the competitive process because barriers to entry exist. The required investments to develop broadband networks, for instance or the communication costs to establish a new brand are significant[9]. Due to the combination of increasing returns and positive network externalities — that are characteristic of information activities — incumbent benefit from strong protection once their market share is established. The long term viability and intensity of competition is therefore an essential challenge in the digital economy featured by strong trends toward the emergence of viable monopolies. (Cf. Shapiro & Varian [1999], Noe & Parker [2000])[10].

In that respect, it has to be pointed out that there is a strong transparency-security dilemma over the Internet. On the one hand, the long-term sustainability of the competitive process in information networks calls for a minimum level of transparency. This is essential to enable users to compare alternative supply conditions. This is also crucial if some entity is responsible for supervising potential anti-competitive behaviors. On the other hand, the protection of contents (both the privacy of information exchanges and property rights) leads to encryption. This raises complex problems, because even if it is not justified to broadcast publicly the content of all information exchanges, it is necessary to verify that information exchanges are not harmful for the collectivity as could be the case if they were aimed at settling collusive agreements, infringing intellectual property rights or performing criminal activities[11].

More generally, Elkin Koren & Salzberger [2000], Lemley [1999], or Frischmann [2000] emphasise that users of the Internet bear the risk of being overwhelmed by information flows. In the digital economy, the scarcest resource is the ability to sort and discriminate information[12]. While it is difficult to measure search costs, two stylized facts highlight the importance of these costs in the Cyberworld. Commercial strategies over the Internet are often based on the assumption that such costs are high. Because many on-line customers do not have the means to efficiently compare all the alternative suppliers' bids, they agree to being

---

exclusivity agreements with information or network service providers. Since positive network externalities arise, this type of ostracism strategy decreases the attractiveness of competing sites and reduces their visibility.

[9] After the e-crack it is now clear that the minimum investments to successfully enter markets such has backbones services or ISPs is significant and not accessible to most investors. These markets are already highly concentrated. The same is true for the markets of contents or e-commerce. With the exception of some noticeable and successful first movers, only the big players are able to perform the necessary investments or to valorize on the Internet investments in how-how and reputation that have been performed on other market places..

[10] Near 80 % of the Web traffic is dedicated to 0,5 % of the sites. The 7 more important Websites group around 20% of the whole Web supported dataflows. The ISP market is quite concentrated, as well (Cf. Gaudeul & Julien, 2001).

[11] These call for "confident third part" that should be allowed to verify that information exchanges over the network are not used to perform socially inefficient activities. Obviously, these third parts should be supervised in order to guarantee their efficiency and their neutrality. Due to the number of information exchanges, it is clear that this third part would hardly be able to analyze the on-going flow of exchanges. By keeping track of information exchanges and serving as conflict settlement jurisdictions, they could however help to dissuade potential infringers to develop too anti-competitive or too criminal strategies. However, such third part would not be sufficient to maintain the transparency of the competitive process. Indeed, if they keep the tracked information private, they do not make the public aware of the fairness and of the nature of competing bids by suppliers. The dilemma is therefore far from being solved by an agency responsible for supervising information exchanges.

[12] A link can be made with the economics of knowledge that state that in a "knowledge based society" the scarce resource is attention (Cf. Cyert & March [1963], March & Simon [1993])

captured and locked-in by their service providers, who provide a customized bundle of services to their clients, enabling them to economize on search costs (Gensollen [2001]). That counterbalances the fact that they will be finely discriminated against. The ability that the trademark owners had to impose their enforcement in the DNS is also an indicator of the high search costs over the Internet. A trademark can be considered as a bundle of information services in the sense that it provides users with a set of information over the various features of the transacted good or service. This bundled information service is provided to the customer at the expense of possible discrimination. If trademarks had not been recognized on the Web, and if standardized languages had been set up to describe the diverse dimensions of the various goods and services supplied on line, smart research engines would have been developed to compare the alternative supply according to the specific preferences of the various cyber consumers (Mueller [1999]). One can obviously question the realism of such common universal language to describe and compare alternative supply along a large number of dimensions. Nevertheless, the fact that trademarks and brands are recognized over the Internet indicates that information cost are not reduced to zero by the technology.

Because information technologies do not generate information *per se* and because there is a wide set of strategies aimed at preventing an easy comparison among alternative supply (Brousseau [2000b]) transparency is not guaranteed at all in the digital economy. This calls for the development of means aimed at guaranteeing a minimum level of transparency and preventing the definitive capture of essential resources by some players. Bounding encryption capabilities (e.g. mandatory registration of code keys to trustworthy third parties), forbidding the implementation of technical means aimed at blocking smart agents could be some of the solutions aimed at guaranteeing a minimal level of transparency. It is clear, however that these technical solutions should be combined with more institutional ones aimed at drawing these technical rules, guaranteeing their enforcement and completing the incompleteness of such rules. Whatever the solution, it is clear that competition is not self-sustainable in the Cyberworld.

12. Pre-requisite for a market

As mentioned above, externalities and scarcities can be managed decentrally through a market allocation process if a complete set of property rights is designed and if there are no transaction costs (Coase [1960]). It follows that if these specific conditions do not apply a non-market-based allocation of resources can be implemented to try to solve market failures[13].

Before discussing the problems generated by the establishment of a complete system of property rights, let us address briefly the notion of "non-market" allocation of resources. This notion is often mistaken as an equivalent of State (Public Agency of Government) based allocation of resources. Virtual communities on the Internet constitute alternative ways to manage externalities or scarcities. For instance, the specific rules that regulate the freeware communities allow the cooperation of developers involved in the production of a public good. It has to be pointed out that the self-regulation of a non-market allocation of resources is not a specific feature of the Internet. As long as the size and the nature of a community allow an efficient circulation of information among its members and the implementation of a credible threat (such has ostracism) to punish those who infringe its constitutive rules, a community is able to bound and eliminate the individual behaviors that will result in an opportunistic

[13] Unless non-market allocation of resources is worse than the inefficient market allocation.

exploitation of externalities or scarcities. Well known by historians and anthropologist (e. g. Bernstein [1992, 1996], Cooter [1994, 1996], Granovetter [1985]), these self-enforced self-regulations allow communities to avoid the "tragedy of the commons". However, the efficiency of such mechanisms decreases when communities become larger and more diverse. Indeed, each infringer is less visible because information circulates less efficiently. Moreover, each member of the community has fewer incentives to practice retaliation since it is costly and a member's individual action is also less visible (Milgrom, North; Weingast [1990]).

Nonetheless, by its ability to facilitate exchanges of information among the member of a community, Internet enables an increase in the relative efficiency of community self-regulation as compared to State driven regulations.

Another important feature of the Internet is that its technical features facilitate the enforcement of self-regulations because its technical logic makes it possible to expel infringers from virtual communities. There are two essential resources in this respect : the means of access to the network; and the list of subscribers of virtual communities. Those that control the access to the cyberworld — ISPs, but also the connection software and browser providers — can indeed screen and filter the information received by the users, forbid some types of uses, or block access to some users. This power of expulsion is obviously bounded by the ability of Internet users to access alternative means of access, and by the ability of the providers of means of access to identify the users (because the only identity that is certain over the Internet is that of the computers). This power is however real, first because switching costs to alternative means of access can be high, second because the access providers can be in a monopoly position.

- The strong trend toard the emergence of market power in activities related to information technologies has indeed to be remembered. This is partly due to network externalities among the components of information systems that oblige users willing to change a part of its system to change several of its components[14]. This is also due to the specific structure of costs, which are essentially fix. Whatever the reasons, the strong potential concentration of the supply of means of access leads to a potential control of the uses (while it also causes concern since dominant players could have discretionary use of these means to influence uses and contents).

- Lists of subscribers and address-books are also an essential means to control access to virtual communities that range from the community of the Internet users (that depends upon the DNS system) to the community of the users of this specific product. Whatever its purpose and its size, a community is defined by the list of its members. In the case of virtual communities the register that makes it possible to include or exclude users from access to the resources used to share information — whatever they are : a Website, a discussion list, a forum, etc. — allows control of entry to or expulsion from the community. Controlling it allows both to set the boundaries of the community, and to credibly threat potential infringers of the essential rules of the community. This power is bounded by the existing alternatives. If network externalities are strong within the community, if membership is costly — for instance, because a scarce resource (attention) has to be dedicated — if switching costs are not negligible, then those who control the

[14] More precisely, substitutability among alternative components is high if they belong to a common standard. it is weak if they belong to alternative standards. IT users are locked-in by the standards they adopted in the past.

access to virtual communities can exercise control and use this control to make the "law" of the community enforceable[15].

As pointed out by Berman [2000] this ability of cyberspace actors to use this power of exclusion to make their own rules enforceable by any Internet user generates a problem because these entities do not have to enforce any constitutional norms or ethical principles that would make it possible to take into account all the legitimate interests of stakeholders.

Thus, all things being equal, digital technologies allow the implementation of more easily efficient self-regulations. These regulations can help to solve problems raised by scarcities and externalities. They can solve other problems, as well; such as difficulties in transacting due to adverse selection or moral hazard. The efficiency of self-regulation is however bounded, as will be discussed later. This can explain the need to design other types of regulation.

Let us now switch back to the implementability of a complete system of property rights. On the one hand, digital technologies allow the implementation of a more complete and self-enforcing system of property rights over information goods and services. On the other hand the costs of delineating rights of use (measurement costs) and the costs of having these rights enforced (enforcement costs) are not zero.

When they support information exchanges, digital technologies facilitate the development of market based exchanges of information. Indeed any set of information that is codified in a computerized system can be either encrypted to control *ex-ante* its uses (code of access) or easily tracked to control *ex-post* how it has been used. Technical means make it possible to systematically control access or uses of contents and digital network components because these operations can be quasi-instantaneous and cheap. Following Barzel [1989] and North [1990], ICTs are therefore a means to designate a more complete system of property rights because uses rights over information can be more precisely measured and enforced.

In addition, transaction costs decrease. Moving contents across information networks costs almost nothing. Above all enforcement costs decrease because encryption and codes of access (qualified as "code" in the following) enable the cheap self-enforceability of contracts covering information exchanges (Elkin-Koren & Salzberger [2000]). Moreover, it becomes easier to customize the transferred right of uses according to the specificities of each transaction (the nature of the transactors and of the exchanged content).

There are therefore strong arguments in favor of a decentralized market allocation of resources in digital networks. other things being equal such an allocation is supposed to be more efficient because it should be consistent with the preferences of individuals, if the market is efficient. Two types of argument lead to the nuancing of this initial view. While digital technologies call for more market and decentralized allocation of resources, there are reasons why non-market intervention is not expelled from network and content industries.

First, before any market allocation of resources, a property right system has to be set up. Uses rights have to be delineated and assigned to agents[16]. This operation cannot easily be based on

[15] ISPs and portal administrators, can easily make almost invisible some content providers, and to the opposite favor the access to some services depending on the quality of those providers to be "friends" of "enemies".

[16] A property right system is nothing but the definition of various categories of exclusive uses rights over resources (while exclusive does not mean not individualized). These rights have to be delineated — the nature of

fully decentralized processes because there are no *ex-ante* legitimate exclusive rights to exchange, because there are collective choice problems and because violence and anarchy could result from a process that would not be arbitrated by some ultimate (and legitimate) court of appeal (or Leviathan)[17]. It has to be made clear that while the delineation and the allocation of exclusive uses rights can be contrasted as being different tasks, there are overlaps between the two. Indeed, the delineation of uses rights per se constrains allocation. The ability to finely discriminate among each single use and the choice to bundle or un-bundle the allocation of these distinct elementary rights of uses constrain the choices as cocernns the allocation of these rights[18]. Consequently, the two questions have to be considered simultaneously.

Precise and recognized rights of uses do not cover a wide set of the information that is circulated and managed over the Internet today. First, many contents are not eligible for legal protection. There is a wide range of information — ranging from mathematics theorems to the comparative performances of the competitive shopkeepers in a specific area — that cannot be protected through Intellectual Property tools. One can also mention personal data — ranging from identifying codes that refer to specific human beings to the information that allows the description of the various characteristics in terms of preferences, opinions, wealth, etc. — on which uses rights are very fuzzy and complex because they are contingent to various

---

the resources and of the authorized uses have to be explicit for its owner and for any third part — and made enforceable — non-authorized uses have to be credibly punished. These operations are qualified respectively as "measuring" and "enforcing" property rights; Cf. Barzel [1989], North [1990].

[17] Setting a property rights system generates two types of problem

- On the one hand, free resources have to be shared among agents (or uses rights have to be redistributed among agents). As pointed out by Libecap [2002], this has a direct influence over the distribution of wealth among individual agents (respectively it has redistribution effects). Even if various property rights regime and distribution affect collective efficiency, its choice cannot be the result of a decentralized consensual choice. This is a well-known problem of collective choice raised by Condorcet [1785] and later Arrow [1951].
- On the other hand, as pointed out by Barzel [1989] and North [1990] uses rights have to be delineated taking into account that overlapping should be avoided, and that any kind of potential uses should be taken into account. If these uses rights are decentraly delineated this can generate tremendous enforcement costs because the probability of conflict due to conflicting claims is quite high and because it will be rational for any agent to seek to permanently widen the scope of its self-claimed exclusive uses rights. Moreover, if there is no authority endowed with the monopoly of violence and in charge of making the "recognized" rights enforced in last resort by the force, conflicting claims of exclusive rights could result not only in the destruction (or un-production) of resources but also of the social community by itself. A property right system has therefore to be recognized (defined) and made enforceable by some authority in last resort.

Historically, primitive systems of property rights developed in a decentralized manner. However it was in a logic of capture and pre-emption that did not guaranteed at all neither efficiency, nor peace. In developed societies, this is the State that organize the property right regime for the new economic resources; i.e. new creations or resources that become economic resources. In that case the State arbitrate between the various interests under its jurisdiction — which does not mean that it is fair and benevolent —, because uses rights cannot be defined decentraly (impossibility of consensus) and because it will be inefficient to let a savage competition process to occur.

[18] Actual property rights generally bundle a wide set of uses rights, while this is only a social convention that can be questioned. To actually implement competition in network industries, most of the traditional property rights of network operators (that had exclusive rights over the uses of the network because they were the owners of the infrastructure) have been unbundled and reallocated among various entities (e.g. in telecommunication networks the owner of the infrastructure has a limited ability to use it according to its own preferences and its competitors have got uses right over it). The reallocation of these rights was therefore linked to a new delineation of rights that were previously bundled.

situations (as pointed out by the debates on privacy issues). One can quote as well the information that is necessary to administrate networks (IP addresses, telephone numbers, mail addresses, etc.). In each of theses cases uses rights over this information are quite incomplete. In many circumstances, no rule sets out how this information can be legitimately used[19]. Any decentralized decision process about the uses of these types of information would necessitate organizing a complete and consistent system of property rights, which could not result from a market allocation. At least some non-market allocation is needed.

Second, the question of the feasibility of a complete system of property rights arises. Indeed, a low level of transaction costs (i.e. the costs borne to establish property rights; Cf. Barzel [1989], North [1990]) does not mean that these costs are zero. First, information-processing costs are often fallaciously assimilated to data processing costs. ICTs impact less the first category than the second. Indeed, the human brain that associates various types of cognitive processes is unavoidable when complex information processing occurs. Second, the costs of a complete set of property rights are prohibitive. This is true in general as pointed out by North [1990]. A complete set of property rights means being able to *ex-ante* forecast all the possible uses of any resource and to associate rights to any of the potential uses. There are obviously many uses for which it would be too costly to perform these operations if one considers the value generated by each of the possible uses. Moreover, being able to centrally identify and make enforceable in the last resort these exclusive uses rights would mean that decision and information costs are equal to zero and that infinite computing capabilities are available. This is why property rights systems are always incomplete, generating public goods and externalities problems. In the case of information, there is an additional reason for the incompleteness of property rights. There is a tremendous number of alternative (and often non-rival) uses of the same set of information. Moreover, the ability to use a specific set of information often depends upon the access to complementary information. A complete system of uses rights should take into account the alternative possible uses of information as well as their context. Again, it would be inefficient, if it were not prohibitively costly to design such a complete set of property rights.

In sum, a fully decentralized and fully market-based allocation process to solve scarcities and externalities is not sufficient to guarantee an efficient performance of information networks since a complete property rights system over information does not exist, and since it is not sure that it could be implemented. First, there are distributive and ethical obstacles to implement a complete set of property rights. Second, it would be inefficient — and probably impossible — to implement such a complete property rights system. This does not mean that any non-market-based allocation of resources is inefficient, but it leads to the conclusion that a purely market based process would not make it possible to reach the most collectively efficient solution. This would imply restrictions in the production or use of content and some potential players would be priced out of the market[20].

[19] Taking personal data as an example, it can be pointed out that uses rights are complex to delineate and allocate because they should vary in function of the way the user initially got the information and in function of the identity of the user. Under the French Law, for instance, such differences are implemented to balance between efficiency (that consider both the utility of data-bases and the costs of punishing privacy infringements that are not too harmful) and human rights (that implies the protection of public liberties). Consequently, it is not an infringement for an individual to hold the personal address of another individual, and to communicate it to a third individual. It is however an infringement for a company to hold such an address without the consent of the person. In any case, a company is not allowed to communicate the personal data it got to any third part.

[20] Those users would not be probably priced out of the market if a really complete system of property rights could be implemented and if it would enable them to value some resources (such as their personal data) that

To conclude, there are some logical inconsistencies in assuming that a completely decentralized system of bilateral negotiation could enable us to solve the problems generated by the use of information resources over digital networks. Since a complete set of property rights cannot be implemented, some forms of alternative allocation processes have to be implemented. In that respect, devices able to implement non-market allocation process should be designed. Self-regulated communities are obviously one of the possible solutions. However, as will be discussed later, totally decentralized (and therefore un-articulated) self-regulation processes would be inefficient because the limits of totally decentralized coordination solutions among individuals (to set up a complete system of property rights) would be replicated among communities (conflicting claims without solutions). This would call, in the last resort, for some type of central coordination. Obviously, designing a more complete system of property rights can reduce the space of the non-market allocation processes. However, this would require a non-market allocation (and delineation) process as argued above.

These two logical consistency arguments about the non feasibility of a totally decentralized and market-based allocation process have to be completed by a third one. The tendency toward the emergence and exercise of market power in the digital economy, and the call for antitrust regulations.

In all these cases, implementing central and non-market regulation does not mean that traditional direct State intervention is required. The type of regulation that can apply can be based on jurisdiction that would supervise the enforcement of basic ethical, moral and efficiency — let us say, consistutional — principles. Moreover, one can imagine some new ways to set up these basic principles that will govern the regulation of the cyberworld. The important point is to design processes that would take into account the interest of the wider set of stakeholders, given the fact that Internet based activities impacts on non-users of the Internet.

2. What Institutional Framework ?

Internet is *de facto* regulated by coexisting (public and private) institutions that have very different statuses and that partly overlap. The resulting institutional framework is not satisfactory since it is both inconsistent and inefficient. To get a better understanding of how it could be amended, we will analyze why traditional modes of regulation cannot efficiently solve the problems raised by the Internet (§ 21), then analyze the major weaknesses of the institutional framework that attempts to frame information and network activities (§ 22).

21. The Boundaries of the Traditional Regulatory Framework

The libertarian or liberal ideology of the inventors of the Internet is not the only explanations of the fact that Internet is not regulated by the traditional regulating tools, that is to say National States and Inter-Governmental Organizations. Path dependency — i.e. the basic principles implemented by the technical regulatory bodies were hard to redesign ex post because of their wide diffusion and adoption — and the difficulties that most governmental

---

cannot be valorized if the property rights system is incomplete.

organizations[21] had in understanding the stakes around digital networks (Cf. Appendix 3) largely explain why governmental intervention is so weak as compared to other types of network. However, if a new institutional frame emerged, this is first and foremost because Internet has specific features that challenge the efficiency, sometimes even the legitimacy, of traditional (governmental) regulations.

211. A trans-teritorial and global network

The first and most obvious cause of governmental inefficiency is the a-territorial nature of the network. Two of the main features of the Internet are its interconnection ability — that is the basis of its ability to support the sharing of communication capabilities and contents — and its decentralization — that guarantees its reliability, its efficiency and its ability to develop. Building an Internet that would be bounded to national borders would result in great losses of positive network externalities. Moreover, it would necessitate the ability to effectively forbid any interconnection with a foreign network to avoid creating a gateway. Consequently, Internet is necessarily the support of a worldwide connectivity that overwhelms existing regulations based on territorial legitimacy. Any regulation of the content can be bypassed through the Internet because no governmental agency would be able to efficiently supervise the exchanges of information among citizens (or the organization that acts under their jurisdiction) and between them and foreign third parties that are not submitted to the same regulations. Moreover these exchanges can be faked, and the potential infringers can use a wide set of technical means to access contents whose access would be denied by some technical means operated by the state. The generalized interconnectivity as well as the possibility to break codes, and reciprocally to strongly encrypt limits the ability of Governments to control network based activities.

The basic argument here is that the Internet does not challenge the legitimacy of state intervention, but its efficiency. A massive bypass of state regulations is now possible and makes public intervention in networks and contents no longer operable. It is not the first time in history that a new technology has challenged existing regulations. Internet, however, tend to organize a direct confrontation and a brakeless competition among norms, since services and contents providers can locate their information processing devices wherever they want (i.e. in territories where the norms that are the most in accordance with their preferences apply). Competition among norms can thus result in an alignment along the lowest common denominator. That is for instance what happened with the decision to not tax electronic commerce.

Obviously, the a-territoriality of cyber-activities is bounded in some domains (for instance, when tangible resources have to be exchanged or transmitted as is the case in e-commerce). However, competition affects all the norms that apply to contents, from intellectual property rights to privacy. This destabilizes existing legal frameworks, despite the fact that international conventions could be set up to implement common legal principles. On the one hand, the example of the regulation of international flows of capital points out that the setting of restrictive inter-governmental regulations is submitted to a prisoner dilemma. In order to

[21] This remark has to be balanced with the fact that, on the one hand, the US Government has been being one of the inventor and of the main supporter of the Internet, on the other hand, many National Governments, influenced by inter-governmental organizations such as OECD and EU, strongly supported the development of digital networks and cyber activities.

stimulate their national economies there are always States that do not ratify these conventions, resulting in strongly bounding their impact. On the other hand, the capacity to agree on common norms, beyond the general principles, is quite difficult because the various legal systems result from contrasted historical and philosophical traditions, which bring us back to divergent ideologies of human nature, of social logic, or of economic activity. As illustrated by the divergences between Europeans and Americans about free speech or privacy, the probability is quite low of reaching operable international agreements about legal norms on information and public liberties.

212. A Trans-industry network

Because Internet is becoming the technological platform that will support the exchanges, the processing and the storage of all information flows, whatever their nature (voice, image, text, data) and content, the differentiation among the former regulations that were applied to telecommunications, broadcasting TV and radio programs, the press, publishing, etc. is challenged. Indeed, such a differentiation was largely linked to the contrasted economics of these contrasted technical networks that had neither common functionalities nor cost structures. Broadcasting licenses were granted because a scarce resource — the hertzian spectrum — had to be managed in some way. The contrasted regulations between audiovisual programs and printed material in terms of content was due to the technical difficulty of screening the content according to the receiver in the mass-media system. Because the present Internet is still an imperfect substitute for most traditional network services — telephony, radiobroadcasting, TV, etc. — existing regulations can be maintained because bypass possibilities are limited. However, the development of the broadband Internet, and the rise of a wide set of complementary technologies — such as e-books or printing on demand — will turn digital networks into a unified support for the diffusion and use of any type of content. Due to this technical mutation, traditional regulations will become ineffective, and partly illegitimate.

As compared to the question raised by the a-territoriality discussed above, the destabilization of the present regulatory framework does not only result from the ability to bypass it. It is also due to the fact that some constraints disappear: e.g. the impossibility to broadcast a wide number of TV channels over the air (with traditional hertzian analogic technologies) and to discriminate between television viewers ; the necessity to maintain tight distribution networks able to distribute cultural products across the whole territory; etc.

213. Self-Enforcing Mechanisms

The third profound change induced by the digital network and technologies is the ability they provide any content owner with to self-manage property rights over intangibles. A decade after the Coasian contribution (Coase [1960]) that overwhelmed the traditional approach to externalities by linking it to the setting of property rights, Calabresi & Melamed [1972] analyzed the alternative processes needed to manage these rights according to the transaction costs they imply (enforcement and adjudication costs). A property rule — i.e. a rule that implements negotiable uses rights — has to be preferred when bargaining costs are lower than the costs generated by a central agency in charge of *ex-post* assessing the damages endured by third party because of the activity of any economic agents. In the opposite case, a liability rule — whereby damages will be due to the victim in the case of losses due to the activity of a third party — is preferable. Digital technologies affect the relative costs of the alternative

solutions (Elkin-Koren & Saszverber [2000]). First, search, negotiation and contract settlement costs all decrease because it becomes possible to perform these operations on line. Second, and essentially, enforcement costs can strongly decrease thanks to encryption and access codes. Digital technologies allow us to create self-enforceable specific uses rights, because it is possible to program how any digital sequence can be used and by whom. Cyberspace is therefore more likely to be a space in which negotiable rights of uses over intangibles will be negotiated, than a world in which instances will *ex-post* organize compensation between information producers and information users on the basis of notarial and judicial assessment of welfare transfers among agents.

Referring to the transactional approach to property rights (Barzel [1989], North [1990]) and considering the costs of poor adaptation generated by general institutions — because they can provide solutions that are poorly adapted to the specific needs of users; cf. Brousseau & Fares [2000] — another argument can be made to justify a more decentralized management of property rights in the digital economy[22]. Because information goods induce high costs of measurement and enforcement and because they have essential public goods features, the traditional systems of intellectual property rights are very incomplete and leave to the users the responsibility for actually delineating and enforcing their exclusive uses rights. Indeed, this is a good way to solve the traditional production-diffusion dilemma associated with information and knowledge, since only the more valuable information goods are actually privatized by their creator, and because exclusiveness will automatically be limited by the costs of maintaining an absolute exclusivity of use. Because they bear such high costs that prevent them from efficiently capturing the benefit of their theoretically granted property rights various collective instances aimed at collectivizing the management of these rights are created in diverse circumstances — author societies in the case of copyrights, patent pools, etc. , (Bessy & Brousseau [1997, 1998]. These collective governance mechanisms benefit from economies of scale and scope and from learning effects resulting from managing a great number of similar transactions. However, the common governance of several transactions has a cost : it is not perfectly tailored to the specificities of each transaction, resulting in maladaptation costs that are opportunity costs (more customized governance would have increased welfare). For instance, copyrights licensing agreements transfer a bundle of uses rights without taking into account the actual uses that will be performed by the users or third parties (e.g. radio or TV broadcasters do not get any rights for the private copies of programs made by their audience). Digital technologies allow the transferring of each copy with a code that will fix and self-enforce the customized uses rights transferred to the buyer. Typically the problem generated by Napster and other free-music servers is due to the fact that a generic rule — the authorization of private copies — generates high opportunity costs for the music companies because it has been applied by Napster's subscribers in a new technological context in which it is no longer well adapted. Traditionally private copy was authorized because the losses borne by the producer of copyrighted material when it is (imperfectly) copied and freely spread in a low scale network were inferior to the costs of supervising and suiting infringers[23]. Indeed, it would have implied setting up agencies able to track any use of

[22] The above mentioned argument made by Elkin & Salsverber [2000] can indeed be contested, because the impact of ICTs on search costs is not systematically (and significantly) negative due to the strategic behaviors of transactors and to the strong adverse-selection problem raised by information exchanges (Brousseau [2000a], Moreover, they do not consider that the systematic and low costs trackability of any uses of information in digital networks can generate a decrease of supervision costs by a central agency that will be responsible for calculating and allocating damages ex-post.

[23] We do not discuss here the efficiency and the legitimacy of copyright. Taking into account the fact that

copyrighted material in any circumstances. Digital technologies and digital networks overwhelm the economics of many copyrighted material, and recorded music in particular, because copies are perfect, cost-less and can be spread on a very large scale. At the same time, cryptographic and tracking techniques can be used either to forbid any buyer of a copyrighted material from reproducing it (and, moreover, to set out very precisely how he is authorized to use the digital copy he has bought), or to oblige any buyer that wishes to copy and transmit a digital sequence to pay the required fees to the initial producer of the sequence. Digital technologies thus make it possible to finely tune at reasonable costs the transfer of uses rights over intangibles among economic agents and to benefit from a more efficient system of property rights management.

The role played by States in the management of intellectual property rights is therefore questioned. Digital technologies enable a customized protection of any set of digitized information and impact on the relative efficiency of the alternative institutional frameworks that govern intellectual property regimes. This does not mean, however, that the management of IPR systems can be completely decentralized and no longer require an institutional framework.

- First, a minimum transparency of information exchanges has to be maintained to allow supervision, and a repression, of possible infringements of exclusive uses rights by unauthorized third parties. Indeed, not any cryptographic system is inviolable, and code based protection is therefore imperfect. A supervision of uses implies at least a mechanism that will register claims of exclusive uses rights over information — implying a categorization of the various types of material eligible for protection — and that will check the legitimacy and the absence of overlap among these claims. Moreover, disclosure rules would have to be designed (and enforced) to enable some supervision or judicial mechanism to observe how the protected contents are actually used to detect possible infringement.

- Second, while information becomes a good whose uses are now eligible for exclusion, it remains an indivisible good. It is therefore legitimate to question the optimal property regime (i.e. the optimal level of protection) within the traditional debate that balances the advantages of strong incentives with those of a strong diffusion (Cf. Besen & Raskind [1991]). The examples of freeware or virtual communities point out that sharing information on a very large scale maximizes the benefit of disclosure. In some cases, mandatory disclosure rules — especially if disclosure rules can be tailored to different types of possible audience — would probably be collectively optimal. Such rules would imply some mechanism to guarantee their enforcement.

- Third, ICTs affect the costs of processing data sets. When it is a question of intensive-in-knowledge intangible goods; ICTs do not necessarily impact on their protection, reproduction and uses costs as is the case when it is a question of information goods that are essentially featured by a form of expression (works of art). To put it differently, the economics of the various categories of intellectual property is not impacted on in the same way by the rise of information technologies. For instance, the patent system should be less affected than the copyright system. Indeed, a patent protects an idea not the way it is

---

exclusive rights are granted to the authors of works of art, we discuss the efficiency of the enforcement of these exclusive rights of uses. Due to enforcement costs, exclusiveness is never absolute in the real world.

expressed[24], With the noticeable exception of software codes, ideas cannot be reduced to a unique data set, and are even not always fully codifiable. Expertise is needed to assess whether such technical realization constitutes an infringement of a protected idea.

To sum up, digital technologies challenge the relative efficiency of the existing alternative institutional frames of intellectual property. However, these technologies do not automatically promote the solutions that will guarantee the best collective results (it is clear that too strong, or alternatively too weak, encryption would generate sub-optimal results because it will either price out of the content many potential information users, or respectively disincite content creators). Moreover, not all the categories of information goods are influenced in the same way by digital technologies. These suggest that the present frame of intellectual property rights, that are institutional, will have to be re-engineered rather than totally replaced by technical solutions.

*

There is a last, temporary, phenomenon that challenges the traditional regulatory framework. It is the lack of capabilities of the instances in charge of supervising economic and social activities. As pointed out by Posner [2000] in the case of competitive practices, it is both a question of relying on adequate tools to observe actual practices — e.g. reliable means to assess the conditions of exchange as they are practiced on-line — and to be able to understand the link between the observed techno-economic operations (e.g. tariffs, bundling, discrimination style, mode of customization, etc.) and the anti-trust norms made enforceable by judges. In practice, because the pace of innovation is extremely rapid, because good specialists are scarce, public agencies and courts are not well placed to benefit from means that would enable them to permanently design up-to-date rules and efficiently supervise their enforcement[25].

22. The Boundaries of the Present Institutional Framework.

While the traditional regulatory framework is not well suited to efficiently ensuring the necessary regulation of the Internet, calling for the development of a new institutional framework, the one that exists today is not necessarily efficient. Two types of argument have to be made, but contrasted. On the one hand, and this is obviously temporary, the emerging institutional framework results from a not yet fully accomplished process of privatization and internationalization of the Internet. As a result, many of the necessary adaptations have not occurred and the existing framework has to be considered as provisional and transitory (§ 221). Second, and more fundamentally, the existing framework relies on a principle of "co-regulation", whose boundaries can be identified if a relevant institutional framework is not designed. Indeed, the relationship and the hierarchy among private and public, specific and generic, self-emerging or already existing institutions and communities have to be made clear and consistent (§ 222).

---

[24] More precisely, a patent protects a "mother idea" if it is associated with a technical realization and if the exclusiveness of uses is claimed for a particular field of implementation.

[25] In those activities where marginal costs are near zero, the traditional criteria of the difference between price and marginal cost cannot be a reference. Moreover, anti-competitive strategies are based on innovative and subtle practices that partly play on highly complex technical features that are not well mastered by the traditional antitrust authorities or courts.

221. A Frail and Inconsistent Institutional Framework

The existing institutional framework that *de facto* regulates the Internet is characterized by its complexity, its lack of legitimacy and its constitutional frailness.

The complexity of the institutional framework is described in Appendix 2. The consequence is that the Internet is co-regulated by a number of entities with very different statuses and imprecise competencies. This results in overlapping and potential conflicts. Since the relationships among these various entities are not well established, and since there is no recognized arbitration mechanism this conflict of competencies cannot be resolved. This generates widespread uncertainty about the hierarchy and enforceability of the various norms set up by these entities, and finally about the ability of this architecture to generate consistent and comprehensive regulations. Since the stakes are huge, uncertainty is large, because a large number of organizations and groups try to be involved in the regulation of the cyberworld. The risks of increasing inconsistency and uncertainty are therefore quite large.

The second weakness of the existing institutional framework is its lack of legitimacy. This problem is well illustrated by the Internet Corporation for Assigned Names and Numbers (ICANN) that regulates one of the essential resources of the cyberworld: the addressing system (namely the IP address system and the Domain Name System (DNS)). Initially ICANN was organized as a self-regulatory body like those which exist at the national or international level in many network industries when minimal coordination is necessary among operators (as IATA — International Air Transportation Association — does for air transportation). Such organizations provide their members with a set of means to facilitate coordination ranging from standards to services. Because Internet or information service providers could have had conflicting claims in the management of the addressing system, and because a single and unified system had to be set up to guarantee global connectivity and interoperability, these service providers were legitimately the members of ICANN. Indeed, since such an organization is designed to provide its members with coordination capabilities, only those who need such capabilities are legitimate members. However, it quickly became obvious that governments, on the one hand, and citizens, on the other, should also be associated with the management of the DNS because the use of addresses based on natural language impacts on the welfare of the individuals or communities that use these words and identifiers outside of the the cyberworld. This led to the enlargement of the representation of the various stakeholders of the Internet within ICANN, in which representatives of service providers, national governments and "netizens" co-exist today (Mueller [2000]). The problem is that the rules applied to select the representatives of these various communities are unclear[26]. Moreover, the relationships between these representatives are not precisely fixed. Consequently, a decision made by such an organization could be inconsistent and illegitimate. The decision processes do not at all guarantee that all the interests at stake are taken into account and that a clear hierachization among these interests is established. That said, ICANN is not the sole entity in which there are not guarantees that the interests of the stakeholders of the Internet are taken into account, or even that those of the weakest will be considered. In the already established or emerging entities in charge of Internet regulations, computer scientists,

[26] In particular, the 2000 election of the representatives of the "ICANN at large" — i.e. of the "netizens" — have been performed in very fuzzy conditions. Voters have been registered on line based on non-verifiable claims (and how a non-governmental organization incorporated in the US would have been able to claim the right to verify the identity of foreign citizens?). In that process, national lobbies emerged and the election was finally based on the nationality of the various candidates. See http://www.atlargestudy.org/

businesses (especially companies involved in the digital industries), and many US governmental agencies dominate. None of these categories can claim to be able or legitimate in taking into account the preferences of all the categories of Internet users, and more generally of the individuals and entities impacted on by digital networks.

The third failure of the existing institutional framework is partly linked to the two weaknesses discussed above. Its complexity and inconsistency as well as its inability to legitimately represent all the interests of all the stakeholders are partly the cause of the constitutional frailness of the existing institutional framework. Because they do not draw on a legitimate constitutional process, the governance system of the Internet result from a process in which new organizations were created within the pre-existing institutional framework to solve specific technical problems. While it was consistent when the Internet was a US network dedicated to the research community, the whole system was not reengineered when the Internet became international and open to any social activity. Several masterpieces of the present regulatory framework are incorporated within the legal framework of a specific country. Indeed ICANN, IETF and W3C are US incorporated non-governmental organizations. This means that the last resort arbitrator for their decision is a judge in California, or the Supreme Court. That obviously questions the legitimacy of the decisions made by these organizations, because while they regulate an international network, it is US law that will prevail in the last resort. This points out the boundaries of their power. In a sense, the decisions of these organizations are not legally binding outside the US. In the specific case of ICANN this frailness is even stronger since it is the US Government that delegated the management and the supervision of a resource — the addressing system of the Internet — to this organization, which is still owned by this Government and that is technically administrated by a private company (Network System Inc., NSI) that is a contractor of the US Government as well. The US Government could decide at any time to withdraw the delegation of ICANN. Moreover, the constitutionality of that delegation of the management of an essential resource is challenged by several law scholars who consider it to be un-constitutional (Fromkin [1999], Mueller [1999]).

222. Norms Legitimacy and Hierarchies among Regulating Entities

These temporary boundaries reveal more fundamental and joint questions about the way to set up legitimate norms and to organize a hierarchy among institutions for consistency and efficiency purposes.

As pointed out by Lemley [1999] the decentralized model of private norms setting on the commercial Internet questions the efficiency and the legitimacy of such norms from four points of view[27].

- First, the procedures used to design these norms do not at all guarantee that the interest of all the stakeholders will be respected. A norm is rarely neutral. It sets the conditions under which the stakeholders involved in a system can access and use resources. It therefore sets their "initial" endowment of wealth. In the case of the Internet, because one cannot refer to any historic legitimacy, this dependency of the norms on the interests of those who design

[27] The literature on private norms his also based on alternative historical experiences as the medieval "Law of Merchants" or those norms that regulate many ethnic communities; Cf. Bernstein [1992, 1996], Cooter [1994, 1996], Granovetter [1985])

them is especially obvious. In that respect, since the Internet is becoming the basis of many social interactions involving a wide range of different types of agent, there is no legitimacy to systematically adopt and enforce the norms that were designed by the first entrants, the stronger players, or the best organized lobbies. Yet, these trends exist in the present Internet. For instance the owner of commercial sites try to forbid (through bilateral reciprocal agreement, but also though threat of suits) "deep links" — i.e. html links establishing a direct link between two contents without obliging the Web user to go through the front page of the referenced site (on which the most profitable advertising banners are posted). Such a norm reflects the interest of the content editors. More precisely, it would become legitimate if Web-users had been consulted and consented to access free contents in exchange for being targeted by advertisers. However, most of the existing private norms on the Internet apply to people that never accepted, nor even discussed them. Berman [2000] discusses this issue by pointing out that cyber-norms settlers do not have to enforce any constitutional principle resulting in legitimacy problems because norms do not guarantee that the fundamental rights of the various stakeholders of the Internet are enforced.

- Second, no mechanisms are implemented to solve conflicts among norms. The common wisdom denying the usefulness of such a mechanism is that if two groups of users want to apply contrasted norms, it is easy for them to create two different virtual communities. This argument relies on the assumptions that no Internet-user needs to get in touch with members of both communities, and that the members of these two communities do not bear any welfare losses by belonging to different communities resulting in a low-intensive interconnection among them. Because there are huge positive network externalities in Internet based activities, this is a strong assumption. In addition, even if a competitive process applies to conflicting norms, nothing can guarantee that the most efficient one will be selected. This is a well known result of the literature on the competition among technical standards (David [1985], Arthur [1989], Cowan [1990]).

- Third, norms that would apply to the cyber-world and that would result from processes ratified by the community of cyber-citizens could be legitimate if they would not produce any externalities for non-users of the Internet. Such externalities are numerous. For instance, if systems that allow large scale barter of private copies of digital contents (e.g. Napster) develop, the revenues of the creators of content will be affected, unless taxpayers are asked to compensate for their losses by contributing more to the funding of the production of works of art and contents. In both cases, it is clear that the norm of free exchange applied by the members of a given community affects the welfare of members of other communities. An efficient and fair distribution of resources requires processes and instances able to manage these externalities between the cyberworld and the real world.

- Fourth, the norms that arise within virtual communities are not so strongly enforceable. A good example is given by the code of conduct — the *Netiquette*[28] — that was in force before 1995 and that prohibited commercial practices over the Internet. This self-sustained norm disappeared within a matter of months because it became no longer operable with the enlargement of the community of Internet users. Indeed the enforcement mechanism

[28] To get details see Shea V., [1994], Core Rules of Netiquette, Educom Review, 29:5, September/October (http://www.educause.edu/pub/er/review/reviewArticles/29558.html), and Rinaldi A., [1998], The Net: User Guidelines and Netiquette, (http://www.fau.edu/netiquette/net/)

was based upon ostracism and this mechanism did not apply any longer when the members of the Internet community became too diverse. Post-1995 adopters had very different preferences from the early developers and adopters, and they did not support the enforcement of this pre-commercial code of ethics. As pointed out by Lemley [1999], when ostracism does not apply, norms have to be enforced by external coercion mechanisms that can exercise some power of last resort over those who are supposed to enforce these norms. This is also the result raised by Milgrom et al [1990] studying mercantilism in medieval Europe.

Thus, the decentralized and unorganized process of production of self-legitimated norms does not at all guarantee that the resulting norms will be efficient. Nor does it solve the problems raised by conflicting norms. Moreover, it does not provide the users with a coordination framework that would be secure and that would guarantee the long-term enforcement of norms. All these call for the organization of an institutional framework that will enable these weaknesses to be overcome.

Indeed decentralized and private norms have strong advantages that partly balance these weaknesses. They enable groups to create norms that are well tailored to their specific needs. They allow firms to innovate more easily in norms, resulting in an institutional framework that is more innovative and dynamic than when innovation processes are centralized. In particular self-legitimated norms that are particularly efficient would be able to emerge and be adopted by the members of an emerging community even if there is no social consensus about it. In a sense this is what happened with the norms that govern freeware communities.

The recent literature on the efficient design of institutional frameworks[29] (North [1990], Levy & Spiller [1994], Brousseau [2000a] Brousseau & Fares [2000], Ménard & Shirley [2001]) states that complementarities have to be taken into account and that a hierarchy has to be implemented among the various components of any institutional framework.

Complementarities occur because rules and norms that are set up at a very general level (because they apply to all the agents and to many contrasted situations) are necessarily incomplete in the sense that they do not state precisely the required behaviors in specific situations. Consequently, it can be efficient to design norms that apply to sets of more specific situations. These enable users to benefit from collective solutions that generate economies of scale, scope and learning as compared to cases where the coordination among agents would rely on bilateral contracting and inter-individual decision that would require the dedication resources to decision-making and of ensuring their enforcement. This is why private and specific norms (or regulations) are created. They are complementary to generic and public norms (regulation) insofar as they partially complete them[30].

Hierarchy plays a role because decentrally set up norms have to be made consistent both among themselves and with the more general norms that take a wider range of interests into consideration. At the top of the hierarchy, one and *only* one last resort institutional

[29] An institutional framework is made of norms (or rules) and organizations — qualified as institutional organizations — that set up, make enforceable and complete norms by prescribing behaviors to agents when norms do not apply (Brousseau [2000a]).

[30] Indeed, collective norms cannot fit to every details of any transaction, and bilateral agreements have always to be implemented. However, collective norms enable to simplify the design of these agreements since norms provide contracting parties with guidelines to negotiate, and interactions rules that do not need to be negotiated.

organization has to ensure the resolution of such conflicts, much as a Supreme Court does in a constitutional State. Logically this institution of last resort has to take into account the interests of all the components of the community that is *de facto* under its jurisdiction. This leads to the idea that this last resort regulatory body has to verify that private and local norms are not captured by some groups to create and exercise monopoly power. In turn, establishing a hierarchy among institutions is a way to reinforce the enforceability of self and local regulations. Indeed, since these local regulations can be considered as components that participate in the general efficiency provided by the institutional framework, it is legitimate to reinforce the enforceability of these self-regulations when necessary. Following the above discussion, if a last resort organizational institution gets some power of constraint over agents, it can use it to credibly threat infringers of self-regulations. In fact, this is quite a common practice in the real world. Self-regulations are often created to govern professions and industries, and the State can decide to make such self-regulations mandatory if it considers that they are efficient. In this case the violence monopoly of the State becomes the guarantor of the enforceability of self-elaborated norms, that would be weaker without this contribution of this last resort power. In turn, the State often applies antitrust policies to these self-regulations to ensure that they are not set-up to exercise monopoly power.

To conclude, one of the necessary conditions to benefit from an efficient institutional framework is to implement a unique and legitimate institutional organization of last resort regulation — legitimate in the sense that it would be able to take into account the interests of the wide set of Internet stakeholders. It would have to design and make enforceable constitutional principles aimed at guaranteeing some fundamental rights of Internet users, and would be aimed at solving conflicts among decentralized regulations set-up by communities and second-rank institutional organizations. Indeed self-regulations based on specialized norms and private institutional organizations enable agents to benefit from coordination frames that are well adapted to their specific needs and preferences. The last resort institution overlooking private and specific institutions is essential to maintain the consistency of specific regulations, to ensure their enforceability and to avoid their capture by individual interests. This calls for a federal institutional model enforcing a subsidiarity principle. The central and last resort institution is there to guarantee the efficiency of a decentralized mode of self-regulation, not to directly regulate users.

It is obvious that such an institutional framework that would be the guarantor of the general interest and that would be able to regulate the self and local regulations is missing in the existing Internet framework. This is why the logic of decentralized self-regulation seems to be prominent in the mode of regulation that is experienced today. Since it is an unsatisfactory solution, does it call for a co-regulation between States and private interests as is advocated in many instances ? Since co-regulation is a fuzzy concept, it is difficult to answer without being more precise about the institutional design behind it. However, two points can be made:

- First, if co-regulation means that national States on the one hand, and interest groups and large companies on the other co-operate in regulatory processes in which they are considered as equally legitimate (as happens within ICANN), it would not be efficient because such a process would not organize a hierarchization of the regulation designers according to the breadth of the diversity of the interests they are able to take into account due to their nature.

- Second, traditional national States are not likely to federate in order to create an entity that would be able to regulate the Internet in the last resort. It is clear that many national states are not able to legitimately represent the interest of their populations. Moreover, many

bureaucracies, either national or international, are simply not efficient at regulating. Lastly, as mentioned above, inter-governmental agreements are difficult to reach in many situations.

At the same time, a last resort mechanism of regulation able to take into account the interests of the various parties whose welfare is impacted on by the Internet and which will ensure the efficiency and the long term sustainability of decentralized regulations is unavoidable. Institutional innovations are therefore necessary.

This last resort regulation device should be submitted to democratic control and responsible for enforcing a basic constitution aimed at preventing capture and protecting essential natural rights. It should act more as a jurisdiction than as a government. However, it has to be made clear that, as a regulator — indeed, it will be the regulator of the (self) regulators — it will both settle conflicts and set the basic rules that will constitute the constitution.

3. Toward a Cyber Institutional Framework.

Internet challenges the traditional regulatory frames of network and information activities that are based upon State intervention. First, some of the justifications of public intervention are removed with the rise of digital networks and technologies: some sources of scarcities dry up, and the relative costs of centrally or decentrally managing uses rights over informational resources are reversed. Second the convergence of many activities toward a common technological platform removes the boundaries among activities that were previously featured by highly contrasted technological logic and economics. Traditional regulations have to be adapted to the new platform, and inconsistencies among former regulations have to be removed. Third, the a-territoriality of the network makes traditional state regulations inoperable. Moreover, the direct competition of legal norms in the cyberworld does not facilitate efficient harmonization.

Because Internet based activities generate a lot of externalities both within and without the cyberworld, because a minimal technical and economic regulation of the Internet is needed, and because there are strong risks of monopolization of key resources in the digital world, regulation of Internet based activities seems to be unavoidable. Such a regulation cannot be entirely based on self-regulation for at least three reasons First, the parties that self-proclaim themselves regulators would not necessarily be able to take into account the interests all of the of economic and social agents affected by Internet based activities. Moreover, they would be able in some cases to capture the regulatory process to implement regulations that would serve their interests, or worse enable them to exercise monopoly power. Second, private and self regulations are not automatically self-enforceable, because self-enforcement necessitates homogeneous communities whose members share common values and are incited to protect the norms that structure the community. Third, decentrally set-up regulations can be inconsistent.

Consequently a hierarchized institutional framework should be designed, on the one hand, to organize a clear distribution of sovereignty in terms of regulation (by settling conflicts among norms), and on the other hand, to guarantee that the interests of the various stakeholders — whether they are or are not Internet users — are taken into account. Such a mechanism has to be of a supra-national and democratic nature. Obviously designing and implementing such a regulatory entity will be quite difficult in practice because it implies that national states give up a part of their sovereignty.

Beyond its logical justification, the implementation of a principle of regulation of the Internet in the last resort is made possible by the necessity to centrally manage the addressing system. The mastering of the management of the addressing system by the entity that would be responsible for the regulation of the Internet in the last resort will allow this entity to dispose of the means of its assignment. Indeed, it would enable it to dispose of a credible last resort of excluding agents from the access to the cyber world[31] that it could use to have its decisions and regulations respected. In turn, only a well designed and democratically controlled entity should be allowed to control the system of inclusion/expulsion form the Internet.

Such a last resort entity does not contradict the principle of self and decentralized regulations developed within communities. One of the interests of the Internet is precisely its ability to structure communities emancipated from geographical constraints. The decrease in enforcement costs allows the building of self-enforceable regulations on a larger scale than before, whose sole boundaries are the minimal consistency of these communities (whose members should share values and preferences). The second main advantage of Internet and related digital technologies is that codes allow a strong customization of the management of uses rights. Last but not least, the ability of individuals and communities to self-organize and to design innovating coordination processes is a strong source of technical, organizational and institutional innovation. By self proclaiming themselves as coordinators and regulators, individuals are able to submit new principles to the test of users and to the competitive selection process without needing to benefit from an a-priori legitimacy (that would be granted by their past reputation, labels or qualifications, or delegation provided by pre-existing authorities). A supervision of these innovating practices is nevertheless unavoidable to be able to guarantee the long-term viability of the competitive process and the openness of the network.

More broadly, the problems raised by the regulation of the Internet are very similar to those raised by Global Governance[32]. They are not specific to network or digital industries. The perspective adopted in this paper could therefore be deepened, applied and tested in to deal with other issues. By assimilating regulation — in the broad understanding adopted here — with the design of a property right system, I pointed out that several features of the design of an Institutional Framework could be analyzed in a common analytical perspective. By not

---

[31] As pointed out in note 3, the necessity of having a unique and uniform addressing system is however challenged by the technical research today. It is true for the IP addressing system. It is also true for the DNS that is in a sense only a peripheral application of the Internet. Technical solutions enable to create independent "naming spaces". One can even imagine systems that would locate the right server by combining tools — in fact, B-trees and distributed data bases — able identify the contents of the servers thanks to combinations of indices.

At the same time, if end-to-end connectivity and transparency would be maintained, the IP numbering system would remain a central resource. Moreover, if the network numbering system would be de facto decentralized (see note 3), it would become possible to disconnect sub-networks infringing basic rules.

[32] There is a growing literature on the necessity to better articulate and regulate activities that generate international externalities. This includes the management of environmental resources, security, etc. The notion of Global Public Good has been especially developed to address these issues. See for instance : Faysse N., [2001], Que dit la théorie économique sur la gestion des ressources en bien commun ? Les différents outils et les avancées récentes Miméo INRA, (http://www.ensam.inra.fr/ESR/mabel/articles/faysse_RBC2.pdf) ; Kaul I., Grunberg I., and Stern M.A., (eds), [1999], Global Public Goods : International Cooperation in the XXIth Century, Oxford University Press ; Ostrom, E., Gardner, R., Walker, J., 1994. Rules, Games and Common Pool Re-sources. University of Michigan Press ; Tubiana L., [2000], Environnement et développement :l'enjeu pour la France, Paris, La Documentation Française (http://www.ladocfrancaise.gouv.fr/html/0040005.36/html/0000.htm);

considering private and public order complementary, by recognizing that the pooling of resources management can be made though very different types of organizational arrangements — ranging to bureaucracies to self-regulated communities —, etc., I tried to point out that the design of a regulatory framework can be think, first, in terms of trade-off between the efficiency/costs of establishing general rules or negotiating inter-individual agreements, second, in terms of delineation of the impact of these rules on the individual welfare of each of the stakeholder in the system. Indeed, the fully decentralized delineation of (individual or collective) uses rights over resources can generate problems of incompleteness, overlapping, capture, etc. Moreover, full decentralization can be inefficient in terms of enforcement. Measurement and enforcement costs can therefore be brought down by designing of institutional frameworks that mix inter-individual contracting, communities self-regulations, and global regulations. In that perspective, such notions as legitimacy or hierarchy can be theoretically grounded from an economic point of view (by taking into account the notion of externalities and property rights settlement costs). The advances made by Ronald Coase and Douglas North prove again their fruitfulness in analyzing issues at the frontier of law, economics, politics and ethic.

Appendix 1:
The Technical Principle of the Internet and the Key Resources to Govern it

Internet is not a network *per se*, but a network of networks that relies on common standards and a decentralized network administration. Standardization and decentralization principles are at the core of its reliability and ability to evolve, since new functionalities (services) can be incorporated into the network only by plugging in information processing devices (or implementing new software) that perform specific information handling processes.

From a logical point of view, Internet relies on two basic principles:

- Each information-processing device (IPD) that is connected to the network plays two roles simultaneously : processing information and operating the network. In a digital network, there is no technical discrimination between the resources dedicated to the administration of the network and the terminals that process the information carried, as is usual in traditional communication (e.g. telephone) or distribution (e.g. TV broadcasting) networks. In the latter, the network operator is responsible for managing transportation and switching capabilities to ensure the exchange of information among "terminals" that do not interfere in the administration of the network. In a digital network each IPD is a switch that receives information from the other IPDs and routes it to the targeted IPD. Even though, in practice, some IPDs are specialized in the management of data flows, each IPD connected to the Internet has some routing capacities. This is the key to the decentralized administration of the network

- All the services provided by the Internet rely on Client-Server architecture. Any IPD on the Internet can become a client that sends requests to another IPD — that then becomes a Serve — to provide him with information processing or service[33].

The combination of these two principles makes it possible to generate any communication or information services provided by the Internet, and the development of new services relies on the adjunction of new information processing capabilities (IPDs or software) that enrich the collection of basic services that can be combined to produce the various available ready to use services.

To have a digital network performing, two types of essential resources are needed. A single *addressing system* should enable any IPD to identify the other IPDs to route the requests and the replies from the right client to the right server, and vice versa. In addition, *standardized languages* have to be spoken by the IPDs to manage both communication among them and co-operative information handling processes.

On the Internet, the *addressing system* is made of two layers. First, a numerical address is allocated to each of the IPDs connected to the network : the *Internet Protocol Number*. *IP*

[33] This is the case for the two main applications of the Internet : e-mail and the Web. Sending a mail consist in asking the server (the recipient) if he accept to receive an information. If he agrees, the client (sender) sends the information. In practice, these operations are performed by mail servers that are permanently connected to the network, facilitating the management of data flows. Consulting a Web-site corresponds to a case in which the visitor sends request to a computer in which information is stocked. The information server send back to the client html codes that enable the computer to re-build pages on the client's screen.

Numbers are machine only readable addresses that are the basis of the dialogue among the devices connected to the network. It is essential to avoid any duplication of IP addresses within the Internet, because it would prevent the clients from identifying the servers, and more generally disturb the routing of information packets among machines. Second, a "user-friendly" addressing system — the *Domain Name System* (DNS) — is implemented to allow Internet users to express their request in a language that is close to "human" language. The prefixes of the form www.identifier.com are indeed easier to manage than IP numbers for boundedly rational human beings. Moreover, this is a flexible system since the manager of a Domain Name (DN) can dedicate several IPDs (and therefore IP numbers) to a single DN. The nucleus of the DNS is a root file that establishes a single link between any DN and IP number. This allows any computer connected to the Internet to interpret requests expressed in html language.

The second type of essential resource is a set of common languages — standards — that enables IPDs to communicate with each other and process information. Internet is based on the use of two types of standards. The *Internet Protocol* (IP) is the common communication protocol that makes it possible to manage data flows among IPDs. It is the heart of the interoperability of the components or the networks that require a broad set of common rules (to organize information in data packets, to route data-packets within the network, to manage priorities, etc.). *HyperText Markup Language* (html) is the multimedia language of the Internet that enables any IPD to transform any kind of information (data, sound, image, etc.) into codes that can be "understood" by any other IPD. This is a common programming language that allows heterogeneous devices to inter-operate when processing information.

There is therefore some of centralization and hierarchy within the Internet[34]. The management of a decentralized network of networks implies an entity that sets a single addressing system and a set of common languages in the last resort. Since the number of required addresses and standards is enormous in global multimedia networks, it is essential to decentrally allocate addresses, and set standards. However, to avoid overlapping and conflicts, a hierarchy has to cover the decentralized entities and committees to guarantee the consistency of the system. While it can be a federative institutional framework, a single entity responsible for ultimate decisions and last resort conflict settlements has to oversee the whole institutional framework.

[34] It is important to point out, however, that some of the main inventors of the Internet (e.g. David Clark) really tried to develop a network that cannot be centrally controlled in order to avoid its capture by any type of interests (and not only for security reasons as often argued). Today, researches are performed — e.g. within the Advanced Network Architecture Group at MIT (Laboratory for Computer Science) in order to withdraw all the elements of centralization in the concept and in the architecture of the Internet for the same reasons. See : Vannevar Bush [1945], "As We May Think", *The Atlantic Monthly*, July, http://www.ps.uni-sb.de/~duchier/pub/vbush/vbush-all.shtml / David Clark: http://www.ana.lcs.mit.edu/

Appendix 2:
The Present Institutional Framework that Regulates the Internet

Today the "technical" regulation of the Internet is performed by three main organizations:

- ICANN (*Internet Corporation for Assigned Names and Numbers*; http://www.icann.com/), is a non-profit organization incorporated in the US that was set up in 1998. Under a delegation contract with the US Government (*Department of Commerce*), ICANN is responsible for distributing IP numbers and Domain Names. In both cases, the addressing system is a hierarchical one in which a limited number of roots (e.g. .com, .org or .net) enable the creation of a bounded number of addresses. This hierarchy makes it possible to delegate the concrete distribution of addresses among entities that manage portfolios of addresses according to their own rules. ICANN is therefore a supervisor in the last resort of:

  - the distribution of IP numbers that is ensured by the administrators of the subscriber networks (the Internet Services Providers; ISP) who are endowed by territorial authorities with the right to manage a set of IP prefixes.

  - the distribution of Domain Names, by setting the features of the available roots (first order domains, or suffixes, such as .com, .fr, etc.) on the one hand, and by selecting and supervising the organizations in charge of collecting and registering the claims of the users on the other hand[35].

ICANN's power derives from its ability to command the entity responsible for the technical management of the *Root Computer* of the DNS : the private companies *Network Solution Inc*.[36]. Indeed ICANN is endowed with the right to withdraw from this root server the Domain Names operated by entities that would not enforce the rules designed by ICANN. That is why ICANN is one of the possible roots of a non-technical governance system of the Internet. It already plays such a "non technical" role when it deals with claims that interfere with registered trademarks.

- IETF (*Internet Engineering Task Force* ; http://www.ietf.org/) is *de facto* the entity responsible for the standardization of the communication protocols : the IP system. It has no legal status, and is only a working group of the *Internet Society* (ISOC), a non-profit scientific organization aimed at promoting the development of an open and efficient network. While IETF is not endowed with any status or power to design enforceable standards, it *de facto* sets the rules that ensure the inter-operability of the components of the Internet[37].

---

[35] In 1992, the *National Science Foundation* (NSF) delegated the management and the distribution of non-governmental domain names (.com, .org and .net) to a private (for-profit) company (*Network Solution Inc*.; NSI) that did provided that service on a monopoly basis for five years. In 1997, that "market" was liberalized, and 46 companies are now competing. On the other hand, national suffixes (such as .fr, .uk, etc.) are managed by national entities that distribute domain name following discretionary or market processes.

[36] Neither ICANN, nor NSI own this root database of the DNS that is the property of the US Government that delegated its management to both organizations on a contractual basis.

[37] IETF does not really design standards, but open source software. Moreover, there are no certification bodies responsible for supervising the enforcement of these "standards". In fact, they are made enforceable by the necessity to maintain interoperability among the components of the network. This technical self-enforceability of

· W3C (*World Wide Web Consortium* ; http://www.w3.org/) is responsible for the development of the HyperText Markup Language (html). It is a kind of club where access is reserved to those organizations that can afford the relatively high membership fee.

These three organizations *de facto* regulate the Internet today. They are however not really regulating bodies

· First, none of these organizations is really endowed with the right to set rules and supervise their enforcement for fear of sanctions. ICANN's legitimacy is low. IETF's and W3C's standards are not mandatory.

· Second, the legal statuses of these organizations are unclear. Since their membership rules and their decision rules do not guarantee any legitimacy of their decisions, the status of the rules they set and of the sanctions they decide is questionable (see § 22).

· Third, the scope of the competencies of each of these organizations is fuzzy. In principle, they are responsible only for the technical regulation of the Internet. However, in many cases, the technical standards, or the "technical" decision to manage the addressing system according to a given logic, affects the economic and social features of the services and contents. Moreover, as pointed out by Leiner et al [2000], there is a strong tradition in the Internet community to set ethical, social and economic norms in addition to technical rules (a good example of this is given by Berleur et al [2001] who survey 70 self-regulations developed over the Internet).

Beside these three main components, other organizations play a role in the design of the standards and norms in use on the Web:

· First, informal structure — such as free software communities, or the profession concerned with the management of sounds or images — develops specific standards tailored to, respectively, designing operating systems for Web servers or processing photos or sound

· Second, more formal structures, such as the multiple governmental agencies and intergovernmental organizations that traditionally set up standards in the field of telecommunications (ITU), software, etc.

Indeed, because they are rooted in a strong pragmatic school of thought, Engineers rely on existing technical standards when they are considered satisfactory.

---

standards is both the strength and the weakness of the Internet standardization system. Frailness occurs because the upgrading of standards necessitate both a consensus and a strong coordination among the great number of participants in the networks. If consensus would not occur, some players could try to organize a competition among standards, resulting in potential losses of connectivity (and therefore of positive network externalities) and in potential capture of standards by some interest groups.

Appendix 3:
A Path Dependent Institutional Framework

ICANN, IETF and W3C draw from the specific history of the Internet. These organizations are the daughter of the inventors of the Internet who have been working within the US research system since the late 1960's.

Until 1985, the Internet did not really exist. Various specialized digital networks had been developed by the various US research programs and agencies (ARPANet (defense), SPAN (space), CSNet (computer sciences), etc.). Launched in 1969, ARPANet was however the main laboratory of the future Internet in which most of the principles in use today were invented (Leiner et al [2000]). When the NSF decided in 1985 to favor the development of a network open to the whole US scientific community, ARPANet therefore became the main component of the NSFNet, which turned into the Internet when NSF decided in 1988 to inter-connect it to private networks.

NSF's policy of the "open" Internet was not limited to inter-connection. In 1985, it initiated a policy of active transfer of Internet related technologies to the industry. NSF's policy was aimed at stimulating the development of both the network and digital technologies. Logically, the responsibility for the management of Internet policy was transferred from the NSF to the Department of Commerce in 1998.

This history of progressive enlargement and openness of the Internet explains why the organizations responsible for the management of the present Internet draws from pre-existing, often informal organizations that were progressively transformed to take into account the introduction of new stakeholders and the explosion of users and uses.

- The computer scientists that were exchanging memos stating the advances in their work in progress — the *Request for Comments* (RFC), whose earliest drafts date from 1969 —organized a formal process to elaborate and publish them on-line. With the multiplication of the topics, the elaboration of the various RFCs was progressively coordinated under the authority of Jonathan Postel from the *Information Science Institute at the University of Southern California* (USC-ISI). The IETF then emerged to act as a scientific committee of a scientific journal (cf. above).

- Various committees were set up to manage the development of the network within DARPA. In 1983 they were reorganized and their presidents (including the president of the IETF) became members of the *Internet Architecture Board* (IAB). However, due to the enlargement of ARPANet to the Internet, the IAB became inappropriate as early as 1985, leading to the idea of creating an organization responsible for coordinating the various functions necessary to operate the Internet.

- By the beginning of the 1970's the management of the addressing systems was delegated to the USC-ISI by the US Government. By the beginning 1990's this Department was no longer able to perform this task because the invention of the Web and the opening of the network led to an explosion of the demand for Domain Names (that rose from 300 to 45 000 per month between 1992 and 1995). The NSF thus decided to delegate this task to a private company — *Network Solution Inc.* (NSI). This decision to privatize and monopolize the management of the DNS to a weakly controlled for-profit organization was strongly criticized. At the end of the 5 year contract (1993-1998) between NSI and

the NSF, the monopoly of the distribution of domain names by NSI was suppressed and the regulation of the addressing system was separated from its technical management. This led to the creation of ICANN.

Taking into account the enlargement of the Internet, the scientists that greatly contributed to its design and development — especially Vint Cerf and Robert Kahn — funded the *Internet Society* (ISOC) in 1992. This non-profit organization aimed at managing the Internet by taking into account the interests of all its stakeholders. The IETF and the IAB thus became components of ISOC. Initially ISOC was supposed to manage both the standards and the addressing system of the Internet. However, policy makers and industry lobbies denied any legitimacy of this new organization to manage the DNS. Because ISOC was supposed to be controlled by US computer scientists, these circles estimated that it was not able to take into account either the interests of non-US citizens and foreign Governments, or those of industry, especially the owners of industrial title deeds (especially trademarks and brands). This led to the foundation of ICANN.

ICANN draws from a tumultuous process (Mueller [1999]). The development of the commercial Internet raised potential conflicts between the owners of domain names and those of trademarks. The internationalization of the Internet led national communities to claim for sovereignty in the management of domain names associated with each country. Moreover, the allocation of scarce resources — such as IP numbers and non-governmental domain names — became an international and not only governmental problem. Numerous interest groups pushed therefore for the emergence of an organization that would involve all the stakeholders of the Internet.

ICANN's members can be either public or private organizations involved in the development of the uses of the Internet, government representatives, and individuals ("netizens"). Ad hoc committees group these various communities. The main weaknesses of the present ICANN are:

- First, the legitimacy of each member is not at all guaranteed by any accreditation process. Moreover, the relationships (and the hierarchy) among the various types of members are unclear. This results in an organization that does not guarantee that the interests of the various stakeholders are taken into account and hierarchized, nor that its decision will be consistent, nor that it can even make decision.

- Second, it is not autonomous since ICANN is a contractor of the US Government Moreover the contract between the US Government and ICANN is only transitory, and the technical management of the DNS is ensured by another contractor of the US Government : NSI. As a result, ICANN is neither an independent organization, nor a strong one. It is presently not autonomous and the institutions responsible for the enforcement of ICANN's rules in the last resort (the US courts and the US Government) cannot be considered as fully legitimate and powerful. On the one hand, since their purpose is to protect the interests of US citizens and people, they cannot impartially protect the interests of all the stakeholders of the Internet. On the other hand, their formal power is bounded by the boundaries of their jurisdiction: the US territory.

The IETF does not have any specific legal status. It is an ISOC working group aimed at developing new solutions to enhance the Internet. It functions as free software communities

work, rather than like traditional standardization committees[38]. The individuals — essentially academics or engineers employed by the major companies in the field — who want to develop a set of technical solutions can create a working group. The only constraints are, first, that the purpose of the group does not overlap with the topics addressed by already existing and recognized working groups; second, that the groups include a minimum number of participants; and third, that it provides workable solutions within a limited period of time. On this basis, the members of the group elaborate RFCs. An RFC is "published" if no counter-proposal is made by the members of the group (the principle of the "rough consensus") and if three independent tests of implementation have been successful. When published, an RFC becomes a *de facto* standard since it is open software that will be used by all the Internet developers and network operators. Two committees are responsible for the enforcement of these rules. Their power derives from the fact that they can withdraw from the IETF's servers the technical documentation and the RFC of the groups that would not enforce the procedure.

The W3C was founded by Tim Berners-Lee the inventor of the html language. This is a non-profit organization incorporated in the US. Since subscription fees are relatively high, only organizations are members of the consortium. Tim Berners-Lee decided to create an organization in addition to the IETF because he was dissatisfied with the way IETF performs due to its shortage of funding. The W3C budget is 20-30% higher than that of ISOC.

[38] For more information about the procedures of the IETF, see : http://www.ietf.cnri.reston.va.us/structure.html ; Best Current Practices: http://www.ietf.org/rfc/rfc1818.txt; The Internet Standards Process: http://www.ietf.org/rfc/rfc2026.txt

References

Arrow K.J., 1951, "Alternative Approaches to the Theory of Choice in Risk-Taking Situation", *Econometrica*, 17, p. 404-437

Arthur B. W., 1989, "Competing Technologies, Increasing Returns and Lock-in by Historical Events", *Economic Journal*, 99, 116-131

Barzel Y., 1989, *Economic Analysis of Property Rights*, Cambridge, Cambridge University Press

Baumol W.J., Panzar J.C. & Willig R.D., [1982], *Contestable markets and the theory of industry structure*, Harcourt Brace Jovanovich, San Diego

Benkler Y., 2000, "Net Regulation: Taking Stock and Looking Forward", *University of Colorado Law Reveiw*, 7:4, Fall, p. 1203-1261

Berleur J. & alii, 2001, Documents d'autorégulation — Classification — Un premier inventaire, Mimeo, CITA-CRID, Université de Namur & International Federation for Information Processing (IFIP-SIG9.22.)

Berman P. S., 2000, "Cyberspace and the State Action Debate : The Cultural Value of Applying Constitutional Norms to "Private" Regulation", *University of Colorado Law Review*, 7:4, Fall, p. 1263-1310.

Bernstein L, 1992, "Opting out of the Legal System : Extra Legal Contractual Relations in the Diamond Industry", *Journal of Legal Studies*, 21, p.115,

Berstein L., 1996, "Merchant Law in a Merchant Court: Rethinking the Code's Search for Immanent Business Norms, *University Pennsylvania. Law Review*,, p. 1765.

Besen S. & Raskind L., 1991, "An introduction to the Law and Economics of Intellectual Property", *Journal of Economic Perspectives*, 5, 3-27.

Bessy C. & Brousseau E., 1997, "The Governance of Intellectual Property Rights: Patents and Copyrights in France and in the US", Inaugural Conference for The International Society for New Institutional Economics, *The Present and Future of the New Institutional Economics*, September 19-21, 1997, Washington University, St. Louis, Missouri, USA

Bessy C. and Brousseau E. [1998], "Technology Licensing Contracts: Features and Diversity", *International Review of Law and Economics*, vol. 18, pp. 451-489.

Brousseau E., 2000a, "What Institutions to Organize Electronic Commerce ? Private Institutions and the Organization of Markets", *Economics of Innovation and New Technology*, 9:3, July-September, pp. 245-273

Brousseau E., 2000b, "Commerce Electronique: Ce que disent les chiffres et ce qu'il faudrait savoir", *Economie et Statistiques*, 339-340, 2000-9/10, p. 147-170

Brousseau E. & Curien N. (eds), 2001, Economie de l'Internet, *Revue Economique*, October, *forthcomming*.

Brousseau E. & Fares M., 2000, "The Incomplete Contract Theory and the New-Institutional Economics Approaches to Contracts: Substitutes or Complements ?", in Ménard C., (ed.), *Institutions, Contracts, Organizations, Perspectives from New-Institutional Economics*, Edward Elgar Pub., p. 399-421

Calabresi G. et Melamed D., 1972, "Property Rules, Liability Rules and Inalienability : One View of the Cathedral", *Harvard Law Review*, 85, p. 1089-1129.

Coase R., 1960, "The Problem of the Social Cost", *Journal of Law and Economics*, 3, pp. 1-42.

Condorcet, 1785, *Essai sur l'application de l'analyse à la probabilité des décisions rendues à la majortié des voix*

Cooter R. D., 1994, "Structural Adjudication and the New Law Merchant : a Model of Decentralized Law", *International Review of Law and Economics*,, 14, p. 215-231.

Cooter, R. D., 1996, "Decentralized Law for a Complex Economy : The Structural Approach to Adjudicating for the New Law Merchant", University *of Pennsylvania. Law Review*, p. 1643

Cowan R., 1990,, "Nuclear power reactors: a study in technological lock-in", *The Journal of Economic History*, 3

Cremer J., Rey P., Tirole J., 1999, "Connectivity in the Commercial Internet", *Working Paper*, IDEI Toulouse

Cyert R. & March J. G., 1963, *A behavioral Theory of the Firm*, Englewood Cliffs (NJ), Prentice Hall

David P. A.,1985, "Clio and the Economics of QWERTY", *American Economic Review*, 75:2, May, 332-7

Deffains B. & Fenoglio P., 2001, "Economie et ordre juridique de l'espace virtuel", in Brousseau E. & Curien N. [2001]

Du Marais B., 2000, "Réglementation ou autodiscipline: quelle régulation pour l'Internet ?", in *L'internet, Les Cahiers Français*, n° 295, La Documentation Française, Paris, mars – avril, p.65-73

Elkin-Koren N. et Salzberger E.M., 19, "The Economic Analysis of Cyberspace :Challenges Posed by Cyberspace to Legal Theory and Legal Rules", *International Review of Law and Economics*, 19, pp. 553-582.

Engel C. 2001, "A Constitutional Framework for Private Governance", Mimeo Max Planck Institute, Bonn

Frischmann B., 2000, "Privatization and Commercialization of the Internet: Rethinking Market Intervention into Government and Government Intervention into the Market", *Mimeo*, Wilmer, Cutler & Pickering, November

Fromkin M.A. 1999, "Wrong Turn in Cyberspace: Using ICANN to Route Around the APA and the Constitution", *Duke Law Journal*, 50, p. 17-184

Gaudeul A. & Julien B., [2001], "E-Commerce, quelques éléments d'économie industrielle", in Brousseau & Curien [2001]

Gensollen M. (1999), "La création de valeur sur Internet", *Réseaux*, 17 (97), novembre, p.15-76.

Gensollen M. (2001), "Internet : marché électronique ou réseaux commerciaux ?", in Brousseau E. & Curien N. [2001]

Granovetter M., 1985, "Economic Action and Social Structure: the Problem of Embeddedness", *American J. of Sociology*, 91:3, November, p. 481-510

Halpern M. & Mehrotra A. K., 2001, "From International Treaties to Internet Norms: the Evolution of International Trademark Disputes in The Internet Age", *University of Pennsylvania Journal of International Economic Law*, forthcoming

Hetcher S., 2000, "The FTC as Internet Privacy Norm Entrepreneur", *Vanderbilt Law Review*, Vol. 53, Forthcoming, http://papers.ssrn.com/paper.taf?abstract_id= 253317

Leiner B.M., Cerf V.G., Clark D.D., Kahn R.E., Kleinrock L., Lynch D. C., Postel J., Roberts L. G., Wolff S., 2000, "A Brief History of the Internet", http://www.isoc.org/internet/history/brief.html

Lemley M., 1999, "The Law and Economics of Internet Norms", *Working Paper*, University of California at Berkeley

Levy, B. and P. T. Spiller (1994). "The Institutional Foundations of Regulatory Commitment: A Comparative Analysis of Telecommunications Regulation". *Journal of Law, Economics and Organization* 10(2): 201-246

Libecap G. D., 2002, "A Transactions Costs Approach to the Analysis of Property Rights", in

Brousseau E. & Glachant J.-M., eds., *The Economics of Contracts: Theories and Applications*, Cambridge, Cambridge University Press, forthcoming

March J.G., Simon H., 1993, "Organizations revisited", *Industrial and Corporate Change*, 2, 3, 299-316.

Menard C. & Shirley M., 2001, “Reforming Public Utilities: Lessons from Urban Water System in Six Developing Countries” *Working Paper*, The World Bank

Milgrom P., North D., Weingast B., 1990, "The Role of Institutions in the Revival of Trade: The Law Merchant, Private Judges, and the Champagne Fairs", *Economics-and-Politics*, 2(1), March, 1-23.

Mueller M., 1999, "ICANN and Internet Governance Sorting Through The Debris of ‘Self-Regulation’", *info*, Vol 1, No 6, December, http://www.camfordpublishing.com

Noe T.H., Parker G., 2000, "Winner Take All: Competition, Strategy, and the Structure of Returns in the Internet Economy", *Mimeo*, Tulane University, November

North D. C., 1990, *Institutions, institutional change and economic performance*, Cambridge University Press

Odlyzko A., 2001, "Internet growth: Is there a "Moore's Law" for data traffic?", in K. G. Coffman & A. M. Odlyzko. *Handbook of Massive Data Sets*, J. Abello, P. M. Pardalos, and M. G. C. Resende, eds., Kluwer, 2001.(http://www.research.att.com/~amo/doc)

Piazolo D., 2001, "The New Economy and the International Regulatory Framework", Mimeo, Kiel Institute of World Economics

Polischhuck L. & Savvateev A., 2001, "Spontaneous (Non) Emergence of Property Rights", Mimeo U. of Maryland & New Economic School (Moscow)

Posner R. A., 2000, "Antitrust in the New Economy", *John M. Olin Law & Economics Working Paper*, 106, Law School, University of Chicago, November http://www.law.uchicago.edu/Publications/Working/

Samuelson P., 2000, "Five Challenges for Regulating the Global Information Society", *Working Paper*, University of California at Berkeley

Shapiro C. et Varian H. R., 1999, *Information and Rules*, Cambridge, Harvard Business School Press.

Thornburg E.G., 2000, "Going Private: Technology, Due Process, and Internet Dispute Resolution", *Working Paper*, Southern Methodist University

Tirole J., Laffont J.J. Marcus S., Rey P, 2001 "Internet Interconnection and the Off-Net-Cost Pricing Principle", *Working Paper*, IDEI Toulouse

Weinberg J., 2000, "ICANN and the Problem of Legitimacy", *Duke Law Journal*, Vol. 50, pp. 187-260