



20 Property rights in the digital space

*Eric Brousseau**

Internet, a global and integrated information space

Digital technologies overwhelm the economics of information, knowledge and networks. First, they increase the fixed-costs nature of these resources, turning them into less rival goods than before (Shapiro and Varian 1999). Second, the digital codification of information allows the separation of the management of containers from the management of contents, leading to ‘universal’ platforms able to manage any kind of information independent of its nature (whether it is information, codified or tacit knowledge), its form (voice, image, data and so on), or its semantics (whatever ‘language’ is used to establish links between things, concepts and form of perceptible expression). When compatible technical solutions are implemented across groups of users, the platform becomes global. It enables any agent to transmit any information to any third party or to access contents. Third, the rules that govern the use of information can be implemented in the software that manages the hardware. This provides the opportunity to implement self-enforcing rules about the possible use of the technology and the information (Lessig 1999).

Of course, none of these characteristics is perfect in the digital world. Variable costs are not equal to zero. Technical standards are competing and imperfect. Hackers constantly break codes. Moreover, these characteristics do not free economic agents of all constraints. Solutions have to be implemented to cover fixed costs and to stimulate agents to contribute to the production of public goods. Coordination mechanisms have to (be) develop(ed) to ensure the development (and enforcement) of compatible and efficient technical standards. Rules have to be designed and selected to enhance the efficiency of the information and knowledge-based economy. At the same time, digital technologies give rise to many economic and institutional questions, and their specific characteristics lead one to wonder what the optimal way to organize the institutional frameworks of the digital space would be.

The property right (PR) system is one of the essential components of an institutional frame. As pointed out by Barzel (1989) and North (1990), by establishing how agents can use and exchange rights to make decisions about the use of resources, a PR system affects the way an economic system performs. In this chapter, we shall point out how digital technologies call for the emergence of *ad hoc* frameworks to organize the production and the use of information and knowledge on digital networks.



We shall focus on the Internet since it is not only the current most famous communication and information-sharing network, but also, and essentially, the integration platform of digital technologies. Indeed, the Internet is not a network but a set of standards (and an addressing system) that enables heterogeneous information processing devices (IPDs) – either computers or any system able to code/decode, store/retrieve, receive/transmit or process information – to exchange information and to process it cooperatively. Many of the limits of the present Internet – low speed (it is unable to transmit high definition moving images efficiently), unreliability (some exchanges of information cannot be completed when the network is crowded), security risks (information can be captured when transiting through the network, disk contents can be accessed by third parties (hackers) and so on) – should be removed in the future, thanks to the development of the technology and the institutional framework that will set up rules to manage networks and information. The Internet will then become the principal platform for the production, circulation and consumption of knowledge and information.

Stakes are indeed huge. Technology provides new opportunities to organize an institutional environment able to fully benefit from the capability to manage information and knowledge more efficiently. In addition, the Internet is challenging the current institutional frameworks. There are, however, multiple options to build the new one. There are at least two highly controversial issues. First, should the new institutions come from the existing national states – on the model of intergovernmental organizations – or should they be based on self-regulation? Second, should the new institutions maintain the current legal segmentation following the nature and the form of information (for example, copyright versus patents, contrasts with regard to legislation of the press and of entertainment activities, differences in the protection of music and movies and so on), or should they be homogeneous? Indeed, once digitized, any type of information can be managed the same ways on digital networks. These issues are too broad to be discussed in just one chapter. Here we shall therefore limit our focus to the economics of intellectual property rights (IPRs) on the Internet.

We shall argue that, while digital technologies make it possible to establish a decentralized IPR system based on self-regulation and the self-implementation of exclusive rights of use over information, a total decentralization would not be optimal. On the one hand, decentralization would enable agents to benefit from coordination frameworks well adapted to their specific needs and preferences. On the other hand, full decentralization of the settlement of IPRs would result in inefficiencies. While becoming subject to exclusion, most information remains a non-divisible good. Individuals and groups could succeed in establishing monopolies that would deter further entries into ‘privatized’ information spaces. In addition, despite the capabilities of the



440 *Current issues from a property rights perspective*

technology, it remains individually and collectively costly to enforce exclusive rights of use. Full decentralization could therefore lead to prohibitive transaction costs. Several elements are therefore calling for a coordination of self-regulatory efforts to settle IPRs. This coordination should be organized by a central entity in charge of promoting the collective interest by reinforcing the ability of individuals and community to self-organize, by preventing regulatory overlaps and inconsistencies, by maintaining the sustainability of competition in the long run and by taking into account the specificity of non-rival goods. This central entity should be of a federal nature, and should coordinate the efforts of the various self-regulators (whether groups or individuals) to ensure the consistency and the efficiency of the global digital space.

First, we shall explain how the PR approach developed by Barzel (1989) and North (1990) makes it possible to analyse the organization of the institutional framework within which agents can use and exchange economic resources. We shall then illustrate how and why digital technologies and networks challenge the 'traditional' institutional frameworks that organize access and use of information goods. The problems raised by the management of rival and non-rival information goods will then be examined. These will lead us to explain the case for a federal system to coordinate self-regulatory entities, so as to ensure the consistency and efficiency of the exchange of digital goods.

The transactional approach to property rights

According to Barzel (1989) and North (1990) a PR system is a set of rules and mechanisms that delineates rights over economic resources and allocates them to decision makers so as to enable them to take economic actions.¹ It is based on a definition of these rights, consisting in setting the frontiers among different ways of using resources and among regimes for appropriating the output of these uses, and on a process of allocation of these rights, which are granted to individuals or groups. These operations are qualified as 'measurement' by Barzel and they generate measurement costs. Enforcement mechanisms implement these rights of use by excluding every unentitled agent from access to the protected resources, or from capturing the benefits. This implies controlling access, supervising uses, granting authorizations for uses and punishing unauthorized uses (either to obtain compensation for damage or to deter potential infringers), and generates enforcement costs.

In a given group –say, a nation – measuring and enforcement of property rights can be performed either centrally by an authority of last resort – generally the state, which exercises the monopoly of legitimate violence – or by the agents. In the former case, the government defines for each set of economic resources the rights associated to them (for example, *usus, fructus*



and *abusus*) and maintains a registry where each of these rights is attributed to individuals or groups. Then the government sets up and operates an enforcement mechanism to expel any unentitled agents from the protected use of these resources. It can be an *ex ante* mechanism, for example, a guard or an encryption mechanism that forbids access, or an *ex post* mechanism that assesses violation and punishes infringers. The alternative is to have the property rights self-delineated and self-enforced by agents. In this latter case, individuals (or groups) claim exclusive usage, and they apply all the available means (and in the last resort violence) to have their claims enforced by third parties.

The advantages of centralization are threefold (Barzel 1989; North 1990; Bessy and Brousseau 1998; Brousseau and Fares 2000). First, it allows economies of scale and scope, as well as learning effects in the measurement and enforcement of operations. Indeed, the centralized establishment of rights avoids duplication of efforts and enables individuals to specialize. Second, it reduces the level of conflict since agents are less likely to adopt predatory strategies.² On the one hand, if a central authority defines and allocates rights of uses, individual agents cannot unilaterally expand the boundaries of their rights to the detriment of others. On the other hand, if a central authority enforces the existing rights, incentives to infringe them are reduced since it is either *ex ante* or *ex post* costly to do so. Third, the central authority can limit the room for manoeuvre of agents and thus reach a better collective outcome. Decentralized implementation processes could indeed lead to collective inefficiencies when externalities occur.³ In the case of non-rival goods, the central authority could bind the agents' ability to capture them, so as to maximize their spread or their use.⁴ More generally, when a monopoly position generates inefficient capture,⁵ it can be optimal to have an authority that prevents such inefficiencies. Lastly, a last resort intervention can be efficient in the case of negative externalities. Think for instance of the enforcement of exclusive rights of use. The existence of a last resort authority prevents agents both from overequipping themselves in attack and defence capabilities (since decentralized enforcement would lead to an 'arms race' to be always able to exercise credible threats among others, while being non-subject to extortion by stronger players), and from expending resources in destructive conflicts. Of course, what has been said depends upon the assumption that the central authority is both efficient and benevolent.

The cost of centralization is twofold. First, it leads to inefficiencies due to inadequate adaptation of central uniform solutions to local diversified needs and preferences. Even if the centrally designed rule can be optional, it is obvious that it cannot take into account all the possible options. This would require unbounded computing capabilities and unlimited access to information by the central authority (for example, it would be able to access the set of



442 *Current issues from a property rights perspective*

preferences of each individual). Moreover, if it were feasible, the benefit of centralization would be lost since economies of scale and learning effects would be dissipated in the design of rules adapted to any specific individual and to any particular situation. Second, centralization leads to inefficiencies, since it induces distortion between the marginal cost of delimiting rights over the various uses of a resource and the marginal benefits of doing it. Indeed, delimiting and enforcing property rights have a cost. Since the central authority benefits from economies of scale, scope and learning, it cannot charge any individual benefiting from a right to use a resource according to the marginal benefit he/she gets from it. Moreover it would be tremendously costly to try to evaluate the marginal cost of any protection and the marginal individual benefit. Public and centralized PR systems are therefore financed by taxes (or fixed fees). These taxes (and fees) are distortive by themselves. They are also distortive since the government could dedicate a lot of resources to delineate exclusive rights of uses of little economic value; while at the same time it would underprotect access to other more valuable uses of resources.

The advantages of decentralization are the opposite. Decentralization allows a finely adapted definition of property rights to the preferences of economic agents, and ensures that only the use of resources that generate a utility whose valuation is over the cost of protection will be protected. This guarantees, first, that effort will not be dedicated to design and enforce property rights of poor economic value, and second, that certain uses of some resources will remain freely available, which can raise efficiency if these resources are indivisible and renewable. The costs are also the opposite. Decentralization is costly for the agents because they have to bear the direct costs of measuring and enforcing the exclusive rights they claim (without benefiting from economies of scale, scope and learning). Moreover, decentralization is the cause of many and permanent conflicts since there is no last resort authority to stop them. There can be both conflicting claims and conflicting enforcement of these (never recognized) exclusive rights of use. Agents will therefore overinvest in attack and defence capabilities and the high level of risk will prevent part of the uses and the trade from happening (because insurance premiums would be too high).

Decentralization also has a dynamic advantage. It facilitates individual innovation with regard to norms design, resulting in an institutional framework that is more dynamic and more able to adapt than when innovation is centralized. In particular, local norms that are particularly efficient would be locally settled by individuals and progressively adopted by the members of an emerging community even if there is no social consensus about them. In a sense this is what happened with the norms that govern open-source communities. The boundaries of that decentralized innovation process are obvious. First they can result in inconsistencies. Second, since competition can be



biased, efficient norms do not systematically prevail or survive (as pointed out by the literature on technology diffusion; for example, David 1985).

In practice, setting up a PR system, either centrally or decentrally, would be inefficient in the sense that the costs of setting up a complete PR system⁶ would be too high as compared to the benefit agents would get from being able to use resources, investing in production capabilities, and organizing trade.

Any PR system results therefore from a trade-off between the advantages of centralization and those of decentralization. The central authority designs an incomplete PR system, and the agents decentrally complete it (or vice versa). From a normative⁷ point of view, this trade-off should make it possible to maximize the 'collective welfare/transaction costs' ratio; the latter notions encompassing the cost of resources dedicated to trading and setting up the PR system (either centrally or decentrally). It would then be dependent on three main factors: the nature of the resources (which are subject or not to many different uses by many different agents), the heterogeneity of preferences of agents, and the capabilities of the central institutions. This is why the organization of PR systems differs across space and time, given the nature of the resources. This trade-off results in a level of transaction costs (at the macro level), and a distribution of them (at the micro level), and impacts on the capability of a system to generate wealth.

The Internet as a challenge to traditional institutional frameworks

A global information infrastructure overwhelming the economics of information goods

Digital technologies raise essential issues with regard to IPRs since these technologies affect goods that (often) have a public nature, and whose circulation can be organized on a global basis, while new institutional frameworks can be imagined since the technology allows the design of self-enforcing rules. More precisely:

- The Internet will become the principal infrastructure for exchanging and sharing information and knowledge. It can be information and knowledge that is exchanged *per se*, or which are themselves components of modular goods and services that mix tangible and intangible components, or even information that is necessary to organize a transaction. Part of this information is clearly a public good. Part of it is private, since it is submitted to rival uses. Given the nature of information, the optimal way of organizing rights of access and rights of use differs, resulting in complex institutional frameworks.
- The Internet is organizing a global connectivity that is both one of its ends and one of the means of benefiting from a reliable and evolving



444 *Current issues from a property rights perspective*

network infrastructure (since new functionalities can be incorporated into the network only by implementing new IPDs or new software). This connectivity is provided by universal technical standards that manage interoperability among network components.⁸ Interface standards enable any device connected to the Internet to exchange and cooperatively process information with another device implementing the same standards. The strength of the Internet standards relies in their width, openness and public nature. They are wide in the sense that they organize interfaces among a very wide set of technologies and software. They are open in the sense that they are modular and are permanently enhanced to ensure interoperability among most of the available information technologies worldwide. They are public in the sense that they have been produced on the open-source software model and are available for free to any user or developer. Due to these characteristics, they have been able to generate high positive externalities of adoption. They ended in creating a global network that is overwhelming most pre-existing information gaps between individuals and professionals, between large and small firms, among economics agents involved in different industries, among citizens in different countries and so on.

- The Internet is based on a decentralized architecture, qualified as ‘end to end’.⁹ The IPDs connected to the network can get in touch directly with the other machines without depending upon any central capability that would manage the network. This decentralization of the network administration allows any user of the Internet to freely organize information space by establishing technical rules designing how a set of machines can interoperate to share or to exchange information or processing capabilities. This can be done freely because end to end imposes no constraint on how to do it and because there are no means of preventing users from organizing such spaces. This provides the Internet users with the ability to decentrally set up the rules that will govern their information spaces.

Digital technologies provide new opportunities to settle rules about the uses of information resources, while the traditional institutional frameworks organizing the management of these resources – the national IPR systems, but also most national regulations on contents – are both outflanked and severely questioned by the rise of a transnational and universal infrastructure. In particular, digital technologies make it possible to implement self-regulations at a low cost, which can provide the members of communities (characterized by common preferences, or common interests) with rules that better fit their needs than when general rules are designed to govern heterogeneous communities.



Code and controlled information spaces as means of self-regulation

The combination of the code and end-to-end connectivity makes it possible to implement a decentralized process of self-enforcing regulations in the cyber-world.

As pointed out by Lessig (1999), writing digital codes is equivalent to writing rules. Two techniques are at the heart of this feature. First, software codes implement routines on how a set of information will be handled. Second, encryption capabilities allow the control of access both to information and to software. By combining encryption and software coding an agent is able to control access and use of digitized information goods and services. He/she is therefore able to delineate rights of access and rights of uses on information goods and services – and also on network components – and to grant them to any third party.

These rights are self-enforceable since the simple fact that it is written in code makes it mandatory to use the information the way it is authorized or imposed by the code. Of course there are limits to this self-enforcement since a code can be cracked. However, cracking a code requires expertise and time. It is a costly activity. Most of the individuals or groups able to crack codes perform, even informally, a cost–benefit analysis to determine whether or not it is relevant to bear the fixed costs of code cracking. The result of the analysis will depend upon the benefits that are a function, on the one hand, of the conditions of access to the coded contents (both depending on the tariffs and the restrictions imposed by the writer of the code), and on the other hand, of the rewards the cracker can get either by selling or by disclosing for free the ‘uncoded’ material (which itself is dependent upon what the hacker can get – payment, reputation and so on – and the size of the community). The possibility of cracking codes makes the self-enforcement of rules implemented in digital codes imperfect. The ability to control the uses of information thanks to digital technologies is nevertheless quite strong for at least three reasons. First, a code has to be written to manage hardware in any case. Cracking *per se* is useless if no code is written to replace the cracked code. Many codes are not cracked simply because nobody wants to pay for writing a new one. Second, due to their network nature, information technologies perform in a system and compatible codes have to be adopted. Third, the new technological base enables the control of uses not only *ex ante*, but also *ex post*. Thanks to the low cost of handling and storing information, and since any operation requires the execution of codes, a systematic tracking of information handling operations is performed by most digital information systems. Infringements to rules can easily be tracked and then retaliations can possibly be implemented. This ability to design (almost) self-enforceable rules about the way information can be used, strongly reduce the usefulness of having such rules designed and enforced by a third party of last resort, such as the state.¹⁰



446 *Current issues from a property rights perspective*

The end-to-end connectivity also plays a central role, in enabling the agents to design and enforce rules without the intervention of a third party. Indeed, it enables agents to organize the information space, whose frontiers can be controlled. Thanks to end to end, agents can control who (or which machine) can access or not a virtual space within which the participants can communicate, share information, perform cooperative information handling processes and so on. In concrete terms these virtual spaces can be websites with controlled access, intranets or extranets, mailing lists and so on. This ability to control inclusion in/exclusion from virtual space allows, first, the setting of frontiers within which common rules are to apply, second, having these rules enforced, since the ability to exclude provides the agent(s) in charge of managing the virtual space with means of retaliation. The credibility of these retaliations is obviously bounded by the (implicit) cost-benefit analysis made by agents accessing an information space. On the one hand, access provides various possible advantages: lower transaction costs among members of the community (see Milgrom et al. 1990), free access to shared information and more generally to a club-good and so on. On the other hand, it can be costly to be excluded, especially if sunk investments were requested to join. The higher the advantages, the higher the sunk costs, the fewer alternatives to the considered information spaces, the higher the credibility of potential retaliations. While enforcement capabilities are partly bounded, the end-to-end connectivity provides the agents with the ability to implement self-regulations in the digital world. Indeed, they can create information spaces with clear boundaries and decide that the infringers of common rules, whether they are unilaterally or consensually identified, will be expelled from the space, and therefore from the virtual community it creates.

This is typically what happens in many 'virtual' communities on the Internet, among which those of open-source software developers are the most famous. When joining a 'project' – like Linux, Apache, Mozilla and so on – developers gain access to a source code (which is hidden in commercial software). The source code enables the user to understand how the software operates. It then allows the user either to enhance it, or to add new functionalities to the software. The GNU licences that are at the core of these virtual communities stipulate that in exchange for free access to the code, developers have to disclose their own lines of source code. Several retaliation means can be implemented if there are infringements to these rules. In particular, the opportunistic developer can be prevented from further access to the source code, can be subject to ostracism and even to retaliations (spam, viruses). The same applies in many forums, discussion lists, chat rooms and so on. These apparent anecdotal practices of techno-alcoholics are also used by many business organizations to structure information sharing within their Intranet. It is also a basis of the organization of markets.



Thus, digital technologies provide individuals or groups with an accessible tool to design rules and to have them enforced. These rules can be individually settled and concern the way information and knowledge¹¹ can be used. Individual agents are able to implement at a relatively low cost – the cost of writing a digital sequence to manage authorization of access, plus (possibly) the costs of tracking uses – rights of access and uses. Moreover, these rights can be traded since they are implemented in the set of digits that is potentially transmitted among information processing devices. When a rights holder transmits a digital sequence to a third party, he/she can implement in the sequence the contractual conditions in which the receiver can access and use the content. This contract is self-enforceable since the code controls *ex ante* the future uses. A system of tradable rights of uses can therefore be implemented without any recourse to a central institution. In addition, individuals and groups have the possibility of creating information spaces in which they settle rules that have to be enforced by the members of the community. These rules cover the use and access to information and knowledge, but they could be even more general since, for instance, an information space can be the ‘information infrastructure’ of a market. In that case, the rules that will organize a community do not create rights of uses only on information goods.

The discrepancy between the global and generic information infrastructure and traditional regulatory frameworks

Traditional institutional frameworks are therefore challenged by digital technologies. Individuals and groups can indeed create and implement *ex nihilo* property rights, contracts and exchange rules, and regulations bounding the extent of these property rights. Moreover, digital technologies weaken these traditional institutional frameworks, since they enable agents to bypass them.

The Internet is a-territorial by nature, while public legal systems are implemented on a territorial basis. The Internet’s generalized interconnection and decentralized management provides individuals with the ability to easily manipulate information at a low cost and to use it according to specific rules in information spaces that do not fit the territories of jurisdiction, and/or that can escape the sovereignty of enforcement authorities. These information spaces defined by on-line communities are generally international. Conflicting legal principles should therefore often apply. Moreover, digital networks can support uses that are hybrid as compared to the pre-existing categorization of uses. Think, for instances of chats, forums and discussion lists that correspond neither to program broadcasting, nor to pure interpersonal communication. This is another reason for the existence of potential conflicting legislation. The discrepancy among legal spaces and information spaces makes it difficult to apply legal rules.



448 *Current issues from a property rights perspective*

First, it is often difficult to determine which law should apply. In many cases conflicting laws could legitimately apply, and there is no pre-existing international convention to solve potential conflicts among laws. Moreover, digital technologies make it possible to distribute the processing of information through the network. A well-designed information service might locate the various components of an information handling process in computers under different jurisdiction, which could perform illegal information handling processes according to a national law, without formally breaking laws. Lastly, in many cases, existing legal rules have not been translated to be applicable to the new media, leaving open wide spaces free of law.

Second, enforcement authorities are often unable to act since authors of legal infringements are difficult to identify and beyond the reach of the authorities' power of sanction:¹²

- Infringements and infringers are not so easy to identify. It would be complex for a governmental agency to efficiently supervise the exchanges of information among citizens (or the organization that acts under their jurisdiction) and between them and foreign third parties to guarantee the enforcement of existing laws. Moreover, such a systematic supervision of exchanges among citizens would represent a threat for civil liberties and would be considered as unconstitutional and not acceptable in many countries. In addition, the transterritoriality of the network would lead a foreign government to supervise information exchanges by individuals or organizations that do not act under their jurisdiction. Again it would be considered as unacceptable by many.
- More generally, private information spaces can be impenetrable for traditional enforcement authorities. Thanks to the ability to code information and to manage information spaces on a decentralized basis, individuals or groups can close information spaces. Moreover, these third parties would hardly identify anyone responsible in the last resort of potential legal rule-breaking. Indeed, the way information is managed in these information spaces can be faked, and the various operations can be distributed throughout the whole network, opening escape doors to the infringers who would easily be able to relocate their activities in the event of lawsuits in a particular jurisdiction area, being able at the same time to continue their activities. The users of Napsters switched to new systems like KaZaA and Gnutella, when major music companies sued the too centralized former system.

In order to have national laws enforced on the Internet, national governments should create a 'national Internet' with clear boundaries and the ability to control the exchanges (through gateways) with other national Internet



systems. Such architecture would, however, result in wide losses of positive network externalities, since it would *de facto* result in a bounded interconnectivity. Moreover, it would necessitate both the ability to effectively forbid any uncontrolled interconnection with a foreign network, and the ability to really control the exchanges of information of citizens and organizations with foreign counterparts. This would be costly, hard to legitimate, and would probably lead many users or potential users to switch to alternative information infrastructures. In other words, while it is technically possible to organize digital networks under the traditional hierarchical model controlled by national governments, such architecture would result in efficiency losses. First, users would no longer benefit from the generalized connectivity that enables them to finely organize information spaces according to their needs and preferences, without any territorial restrictions. Second, this decreasing quality of service would prevent the Internet from becoming a single and unified information infrastructure. It would maintain the existing information gaps due to the coexistence of heterogeneous information infrastructures, and would decrease the share of information activities benefiting from the efficiency gains brought by the use of digital technologies (agents being less incited to digitize their information activities, since the absence of a universal network would reduce the scale and scope effects of digitization).

Traditional institutional frameworks are also challenged in the digital economy because their logic and their legitimacy can be questioned. Of course, the legitimacy of organizing the delimitation and the allocation of uses over information on a territorial basis when a global network is available comes first. Before the rise of digital networks, it was relevant to do this since information flows were more intense within national boundaries than between them, and because the government was the only entity actually able to enforce exclusive rights of use. In a global information society, the legitimacy of such an organization is less convincing. Information goods can easily circulate worldwide, and a consistent system of right of use would increase efficiency by reducing the transaction costs over digital contents. Indeed the coexisting IPR systems force rights holders to claim for exclusiveness of use in many jurisdictions, to potentially sue infringers in these different jurisdictions and to manage complex contracts when transferring the right of uses to business partners or users that could manage operations in different countries. Redundancy is costly, but the cost of managing various IPR systems can become even higher when there are discrepancies among national laws.

The Internet is not only a-territorial (or transterritorial), it is also the heart of a global information infrastructure that supports the exchanges, the processing and the storage of all information flows, whatever their nature (voice,



450 *Current issues from a property rights perspective*

image, text, data) and content. In the past, information networks were implemented on different and largely incompatible infrastructures, which were dedicated to specialized uses and which were made available only to users belonging to a same pre-existing community: an industry, a category of customers, companies of a certain type and so on. In many cases, specific regulations – a regulation being a way to implement or bound rights of uses – were implemented for each of these specialized networks because they were characterized by contrasted economics, technical capabilities and purpose. For instance, broadcasting licences were publicly granted because a scarce resource – the radio spectrum – had to be allocated in some way among conflicting uses and different operators. The restrictive regulations about contents in the public broadcasting of audio and video programmes (much tougher than for printed material) were justified by the technical difficulty of screening the various categories of audiences in the mass-media networks. Many of the justifications for the limitations of the rights to produce or communicate information over information networks are weakened or removed by the development of the Internet. Moreover, many of these past regulations of contents (and the various categories of intellectual property rights) can implement conflicting principles, which are impossible to manage in a unified information space. For instance, privacy is traditionally strongly protected in telecommunications networks. The content of an exchange, and even the existence of an exchange of information between two correspondents, cannot be screened and tracked by any third party, unless the judicial system provides authorization to document a case. On the other hand, the notion of privacy is meaningless in a broadcasting network. In the case of the Internet, what principle should be applied to information flows? Should a government or any entity be authorized to screen and track information exchanges? Should this principle be applied only to one-to-many communication? In the last case, what is the threshold? Is it really possible to identify the hidden one-to-many exchanges and so on? Clearly, many regulations of the past are no longer relevant.¹³

Moreover, the new technological context impacts on the efficiency of the former rules. For instance, copying copyrighted material for private purposes has been authorized in most IPR laws. This *de facto* restriction on the rights of IPR owners to control the use of their material was justified because copying did not really harm their capabilities of getting revenues. Private copy was limited in scale due to the cost and the low quality of copies. Today, the ability of digital technologies to make for free perfect copies that can be distributed on a very large scale could cut most of the revenues of copyright owners. If we admit that they have to get a return on their investments to create the intangibles, then this formerly justified restriction of copyright turns out to be totally inefficient.



Thus, traditional institutional frameworks in charge of organizing the use and the circulation of digital goods are challenged by the rise of global digital networks. On the one hand, digital technologies provide the producers and the users with tools to cheaply implement rules about their uses. On the other hand, the rules designed by traditional frameworks become less relevant than before (and can even generate major inefficiencies), while their enforceability is decreasing.

Many discussions about the required institutional frameworks to organize the cyber-world are fuzzy since there are two different sets of problems raised by the development of the global digital information infrastructure. First, the Internet is in itself a new economic space – a new frontier – in which rights of uses over resources are not yet totally and clearly established. A process has to be run to establish how rights of uses have to be delimited and allocated. Second, the Internet is the infrastructure on which a specific category of goods – information goods – is going to be produced and exchanged. When it comes to IPRs, we are considering intangibles only, we should therefore essentially focus on the second problem: the optimal design of a PR system for non-rival goods. However, while information goods are generally considered as non-rival, there are rival information goods. We shall start by discussing the case of this latter category of resources that are created in the new economics space before considering non-rival information goods.

Cyber-world: a new frontier

In the case of rival goods, the analysis of the optimal organization of a PR system on the Internet is close to the analysis of the optimal organization of a PR system in general, as developed by Barzel (1989), North (1990) and many others since most economists focus on the analysis of rival goods. There are in fact two main categories of rival resources on the Internet: addresses and signals of quality.¹⁴ Before discussing how the management of these resources could and should be organized by the institutional framework, it is useful to return to some technical aspects of the Internet.

Addresses and signals as rival information goods

As stated above, the Internet is not a network *per se* but a set of principles and standards that enable any information processing device connected to a network implementing these principles and standards to be able to communicate and interoperate with any other IPDs connected to other networks relying on the same principles and standards. In addition to common, standardized interface languages, the performance of the resulting virtually unified network relies on a single ‘addressing system’, which allows any IPD to identify the other IPDs necessary to route the requests and the replies from the right client to the right server (see note 9), and vice versa.



452 *Current issues from a property rights perspective*

On the Internet, the addressing system comprises two layers. First, a numerical address is allocated to each of the IPDs connected to the network: the the Internet protocol (IP) number. IP 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 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 bounded 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 numbers. This allows any computer connected to the Internet to interpret requests expressed in HTML language (see note 8).

In fact IP addresses and DNs are different resources. An IP address can be considered as a mandatory registration to be included in the Internet system. Without IP, an IPD cannot operate on the Internet. The other machines connected to the network simply do not recognize it. A DN is not a mandatory resource to get access to the Internet as a consumer of contents (a 'client' in technical terms). For producers of contents, however, it is a means to facilitate access to their services. DNs free users to identify the IP numbers of the machines where information goods and services are localized. By decreasing considerably the search costs associated with the localization of contents, DNs are closer to signals of quality such as brand names, logos and labels than to addresses.¹⁵

IP numbers and DNs are rival resources since two different users cannot use them at the same time. Common IP numbers will simply lead to forbidding access to the Internet to the second party attempting to log on to the network. It could also hinder the performance of the network, resulting in a poorer service for the other users participating in the network. DNs are rival since if a party invests in the development of various capabilities to guarantee a level of service to its customers, and if this party invests in addition in communication to establish a direct link in the mind of the public between a symbol and this guaranteed level of quality, then the use of the same (or even a similar) signal by another player who would not guarantee its customers the same level of quality, will destroy the credibility, and therefore the usefulness and the value of the signal. Consumers will no longer benefit from the economies of search and inspection costs provided by a credible signal. Providers will lose the value of the investment they made in building a reputation. This might result in lower incentives to provide (both horizontally



and vertically) differentiated supply, while differentiation is an efficient reply to consumers' heterogeneous preferences.

These resources are not only rival, they are even scarce. Because of the required standardization and hierarchization of the system used to identify each of the IPDs connected to the network, there are a limited number of roots to create IP addresses. This causes a problem of allocation. One often quoted example is the University of Stanford which has the capacity to create more IP numbers than the People's 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. However, the actual source of scarcity is in the DNS. The number of available names and expressions of the natural language that can be the base of meaningful addresses is obviously bounded.

Centralization as a guarantee for decentralized network operations

Thus the Internet *per se* is a new economic space where at least two categories of rival and intangible resources have to be managed: IP addresses and DNs. In each of these cases exclusive rights of use have to be delimited and allocated to users, both to simply enable the system to perform and to allow trade among them should the initial distribution of these rights be enhanced to better fit agents' preferences. There are in each of these cases two extreme ways to organize the delineation and allocation of these exclusive rights of use. The decentralized solution is when the final users or the decentralized network operators – for example, the Internet service providers (ISPs), whether they are providing access on a commercial basis or not – self-claim exclusive rights of use. The centralized solution is when an authority of last resort is endowed with the right to make sovereign decisions in granting exclusive rights of use to claimants.

The advantages of centralization and decentralization will be discussed below. Before that, it has to be pointed out that any claim for exclusive rights of use is not self-enforceable in the specific case of IP addresses and DNs. In a fully decentralized system, and technically the Internet is fully decentralized,¹⁶ anybody can claim for exclusivity on addresses, while nobody can force the other participants to recognize these exclusive rights of use. In particular, a new entrant could decide to use an already used IP or DN. In a fully decentralized system, the initial claim will not systematically be enforced, and the new claim might either disrupt the system or supplant the initial claim. A central register has therefore to establish the list of all the IP addresses to be recognized by the IPDs connected to the network, and to establish a one-to-one relationship between any DN and the related IP num-



454 *Current issues from a property rights perspective*

bers. This central register must be acknowledged (and its contents enforced) by all the users of the system.¹⁷ Since self-enforcement of claims cannot occur, a minimum level of centralization is thus needed to ensure the absence of conflicting claims.

We shall now discuss more generally the advantages of centralization and decentralization, the impossibility of fully decentralizing the design of the addressing system being taken into account.

In the case of IP addresses, a decentralization of the concrete allocation of addresses to the users by ISPs is the simplest way to concretely manage the allocation process. However, two very different decentralizations could be implemented. On the one hand, the ISPs can be endowed with an ability to distribute a pre-established list of addresses by the entity in charge of managing in the last resort the register of network addresses. On the other hand, the ISP can be allowed to develop its own addressing system to distribute as many addresses as it wants. It is therefore responsible for establishing a gateway between its own addressing system and other ISP addressing systems. The former solution does not allow for removing the intrinsic scarcity of available addresses. Moreover, it reduces the competition among ISPs since the number of granted addresses bounds their market share. This bounded competition could result in a lower quality of service and an inefficient allocation of addresses. The development of independent addressing systems in each subnetwork associated with the implementation of network address translator (NAT) resembles the current practice in traditional communication networks like the telephone system. It would solve the scarcity problem but would strongly decrease the transparency and the reliability of the network (because the addressing system would be composed of various layers). In addition, this solution would give a wide power of control to ISPs because the network would no longer be an end-to-end network.¹⁸ ISPs would manage gateways between their networks and the other networks and would become therefore able to control what their users are doing. That could raise problems for two reasons.

First, it would allow ISPs to become private norm settlers, while they would not have to enforce any basic constitutional principles guaranteeing the protection of some fundamental rights to the users of the Internet – privacy, protection against arbitrary decision to remove rights of use, guarantees that in the case of infringement of its own rights of use, the last resort authority will ensure their enforcement and so on – since they are operating on a global market where such rights do not exist (Lemley 1999; Shiff Berman 2000) and since the competitive pressure can be weak (see Box 20.1). Moreover, for the same reasons, these private norm settlers can ignore the interests of the non-users of the Internet, while there are externalities,¹⁹ resulting in potential capture of welfare to the detriment of these non-users.



Second, digital and network activities are characterized by the combination of fixed costs and increasing returns of adoption that make monopolies sustainable (see Box 20.1). The private norm settlers might therefore be freed from taking into account their customer's preferences when establishing their own norms. Moreover, their control over the addressing system would be a tool to establish market power since, with the collapse of end to end, network operators would become able to control the information service provision on their networks, and therefore to adopt strategies aimed at decreasing the competitive advantages of their competitors (in particular, by providing exclusive services on their own network). Not only would such strategies lead in the long run to the emergence of uncontestable monopolies, but they would also lead in the short term to a decreasing ability of ISPs to market their services on the global digital market (with unavoidable consequences on the diversity and on the price benefiting the final users, since providers will have to write off the fixed cost of the service provision on a reduced audience).

For these reasons, the former solution is intrinsically superior to the latter: it preserves the end-to-end character of the network that is at the heart of its reliability and flexibility. It is, however, sustainable in the long run if and only if the IPV6 numbering plan can be implemented. In that case, the spectre of an actual scarcity of IP addresses would be removed, and the long-term sustainability of competition among ISPs guaranteed.

BOX 20.1 THE LONG-TERM STABILITY OF MONOPOLIES ON DIGITAL NETWORKS

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. In other words, 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 manoeuvre to create and exploit bottlenecks. For instance Crémer et al. (1999) or Tirole et al. (2001) emphasize 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.¹ 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 (Frischmann 2001; Posner 2000). Websites that benefit from the largest audiences are induced to develop various strategies to reduce the audience of the less-well-known ISPs and to expel them from the market. For instance, they can refuse to implement html links with the sites of their competitors. They can also sign exclusivity agreements with information or network service providers. Since positive network externalities arise, this type of ostracist strategy decreases the attractiveness of competing sites and reduces their visibility.

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 (and these markets are already quite concentrated²). Due to the combination of increasing returns and positive network externalities – which are characteristic of information activities – incumbents 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 characterized by strong trends towards the emergence of viable monopolies (see Shapiro and Varian 1999; Noe and Parker 2000).

Notes

1. Indeed, subscribers of the 'small' networks have a larger probability than those of the 'big' networks of sending requests (request to access content or request to send information to a correspondent) to users that are reachable through a network that is not the same as the one they subscribe to. If interconnection is of poor quality, the service they receive is deteriorated (denial of access, long delays and so on).
2. Nearly 80 per cent of the Web traffic is dedicated to 0.5 per cent of the sites. The seven most important websites group around 20 per cent of the whole Web-supported data flows. The ISP market is also quite concentrated (see Gaudeul and Julien 2001).

In the case of DNS, decentralization is also the only way to concretely allocate addresses to users. The entity in charge of maintaining the root file of the DNS (that is, the source that establishes a link between each individual DN and Ips, and which is managed by ICANN in the present system) has to delegate to other entities (the registrars in the present system) the right to grant DNS to users, the essential problem being avoiding the allocation of the same DN to two users. However, in the case of DNS the problem is more complex than in the case of IP numbers. Indeed, DNS are not neutral since



they are used by ISPs (whoever they are and whatever their motivations are) as signals. DN ‘owners’ want therefore to avoid confusion. In particular, if two DNs differ only by one or two letters, or only by a suffix, externalities could occur between the two owners. Moreover, DN claimants can consider that names and expressions are not insignificant. Meaningful expressions are scarce. Names with a specific reputation are also scarce. Lastly, exclusive rights of use can already be granted in the non-digital world (brand names, but also denomination of origin, family names and so on). Three types of conflict can then occur. First, claimants can have conflicting claims both because they want to be the single user of an exclusive DN and because they want to exclude other claimants from similar names. Second, registrars could also compete by distributing the more ‘valuable’ names. Third, the individuals and groups benefiting from the exclusive use of names outside the Internet can be harmed by the fact that alternative claimants would capture this exclusivity within the digital world, and would potentially either capture the investments made by the former to build reputation, or even decrease the value of this reputation. The problem is even more complex as the pre-existing rights of use of names can be conflicting since they were recognized in fragmented spaces (within national boundaries and often in even more local communities) resulting in the existence of several legitimate users of the same name.²⁰ Moreover, claims might target the private capture of names – such as names of celebrities, locations, events – and expressions that are considered as not individually appropriable (and therefore are common resources) outside of the Internet. In addition, the rules that apply to the usage of names can differ among jurisdictions.

The delineation and allocation of property rights over the DNS leads to the same problems as those raised in general when implementing a property system over a free but rival resource. Dividing the generic right to use a resource freely in a set of exclusive rights of use and distributing them among agents has a direct influence over the distribution of wealth among them. A decentralized process of negotiation – that is, a negotiation without any last resort arbitrator – can therefore hardly result in an agreement on the way the right to use the resource has to be divided and distributed, even if setting exclusive rights of use will increase collective efficiency (Libecap 2002). This is the well-known problem of collective choice raised by Condorcet (1785) and later by Arrow (1951). Note, moreover, that such an agreement not only covers the distribution of rights. Agents have to agree on the delimitation of these rights as well. For instance, should a right to use a DN cover a single suffix (like .com or .fr), or should it cover all the suffixes? Should the exclusive rights be permanent or temporary? Should these rights be extended to keywords? How do these rights overlap with other exclusive rights of using names such as brand names? Endless conflicts could result from such a



458 *Current issues from a property rights perspective*

negotiation and agreeing on a conflict settlement procedure of last resort is essential to maintain the consistency and the operability of the DNS.

As in the case of IP addresses, a decentralized system of name distribution could be organized with different registrars (either on a commercial or on a geopolitical basis; see note 20) distributing freely their own DNSs, and organizing, or not, gateways among their networks. This would result, however, in the coexistence of various Internets, since end to end and general connectivity would no longer be maintained. The various DNSs would *de facto* create independent networks. While this fragmentation of the network would be in that case weaker than if it were based on the management of alternative IP addressing systems, the fragmentation would be effective for most of the users and network externalities would be weaker. Moreover, because they will be granted a *de facto* exclusion right, the registrars would be able to implement their private norms, without caring about any essential constitutional principles protecting the individual users (as would be the case for network operators if the allocation of IP addresses were fully decentralized). For all these reasons, it would be costly to not implement a system guaranteeing in the last resort the consistency and the unity of the DNS, and more generally of the addressing system at the heart of the Internet.

Arbitrating among conflicting interests

Historically, primitive systems of property rights developed in a decentralized manner. However, it was in a logic of capture and pre-emption that in no way guaranteed either efficiency, or peace. As pointed out by North (1990), economic history shows that path dependency and rent seeking can prevent economic systems from evolving towards more efficient PR systems. In that context, the state often played a central role in arbitrating among the various interests under its jurisdiction – which does not mean that it is fair, benevolent and efficient – to help to implement PRs allowing either the reduction of transaction costs or the sustaining of growth. This is consistent with Libecap (2002) who suggests that a central entity might be useful in enabling the players to solve the redistribution problem – by implementing compensation – which hinders the privatization of a formerly free resource.

The procedures used to set up PRs in the present Internet in no way guarantee that the interest of all the stakeholders will be respected. Most of the existing norms result from a ‘first-come, first-served’ process. Inventors and early adopters were able to capture most resources. However, 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 adopting and enforcing the norms that have been designed by the first entrants, the stronger players, or the best-organized lobbies (Lemley 1999; Shiff Berman 2000).



Moreover, since there are interdependencies between the cyber-world and the actual one, even if norms were to result from a consensus ratified by the community of cyber-citizens, nothing would guarantee their efficiency, in the sense that the interest of every stakeholder would be taken into account (Lemley 1999). An efficient and fair distribution of resources requires processes and instances able to manage these externalities between the cyber and the real worlds.

To sum up, while the Internet allows a decentralized creation of PR, several elements call for some centralization in so far as it concerns rival resources. First, the addressing system of the Internet cannot be decentrally enforced, a last resort authority responsible for maintaining a central register or claim of exclusive use of addresses has to be managed to maintain the consistency and the unity of the addressing system that is at the heart of the end-to-end character of the network. Second, the measurement – that is, the delimitation and the allocation – of individual exclusive rights of use can be technically decentralized, but a central authority has to be in charge of granting these rights in the last resort. This is the only way to solve potential endless conflicting and overlapping claims, to avoid the infringements of exclusive rights granted outside the Internet, and above all to guarantee the end-to-end architecture of the network whose collapse could result both in reduced network externalities due to the fragmentation of the network and in monopolistic capture (without any ability to really limit because of the sustainability of monopolies in the digital economy).

The latter set of problems does not systematically occur for each of the two essential rival resources that are specific to the Internet (see Table 20.1). However, the combination of enforcement and measurement problems calls for some centralization and hierarchy within the Internet. The management of a decentralized network of networks implies an entity that sets the fundamental rights of the users, and that therefore bounds the ability of potential

Table 20.1 Potential problems raised by full decentralization of PR settlement

	IP addresses	DNs
Inconsistencies (overlapping claims/ unreachable agreement)	X	X
Infringements of existing rights		X
Private norm settlement without constitutional guarantees	X	X
Risk of monopoly capture	X	



460 *Current issues from a property rights perspective*

private norm settlers to implement these norms without any limit. In addition, this entity of last resort should avoid inconsistencies in the delimitation and the allocation of these rights. However, given the size of the system and its complexity, it would be inefficient to manage it centrally. It is therefore essential to combine a decentralized management of the PR system with a principle of hierarchy and authority of last resort responsible for guaranteeing the unity of the system and at the same time some essential right of its users.

IPRs and non-rival goods on the Internet

The necessary decentralization of an IPR system

While some specific categories of information are rival, most of information and knowledge is of a public good nature. First, its consumption is indivisible. It is therefore worthy to have it as widely diffused as possible, while it is costly to produce it. This results in the well-known protection/diffusion dilemma. Second, it is 'naturally' complex (and costly) to exclude a third party from the use of information or knowledge since once revealed it is quite impossible to (voluntarily) remove it from the brain which stored it, and since reproduction costs, which are much lower than production costs, strongly decrease with the development of reproduction technologies, making it easy to multiply copies, whose circulation is complex to control.

Due to the latter characteristic, only agents who can physically constrain individuals can really control the circulation and use of information. Due to the former, it is generally acknowledged that the access and use of intangibles will be restricted in some way to enable their creators and potential investors to obtain a return on their investments and efforts, while it is recognized that this protection should be limited so as to favour diffusion ultimately (Besen and Raskind 1991).

This partly explains the organization of the traditional IPR systems (Bessy and Brousseau 1997, 1998). On the one hand, the intervention of the state is required, since its power of constraint in the last resort is necessary to prevent individuals from using information or knowledge even if they could easily access it. It is recognized at the same time that too strong a protection by the state would be inefficient since it would prevent diffusion. The traditional central (governmental) systems that 'measure' and enforce IPRs are therefore very incomplete, in the sense that they leave to the owners the responsibility for actually delineating and enforcing their rights of exclusive use. The producers of information or knowledge have to delineate the piece of information or the idea on which they claim exclusivity. The government only maintains a list (*cadastre*) where it registers claims for exclusiveness of usage. IPR owners are then responsible for detecting possible infringement and bringing



infringers to court to ensure that illegal use is stopped or damages and royalties are paid. Since IPR owners bear the cost of having their rights registered and enforced, the production–diffusion dilemma is partly solved, since only the more valuable uses of information goods are actually privatized by their creators, and because the search for exclusiveness is limited by the costs of claiming and maintaining exclusivity.

From a collective point of view, this is also a way of keeping the costs of the PR system at a reasonable level. Indeed, information and knowledge can be consumed in very different ways, and can be used as inputs to produce new information goods or services. Consider a piece of recorded music, for instance. It can be listened to by an individual, broadcast to a wide audience, played in a public space, used in a motion picture, be an input into a new piece of music and so on. Centrally measuring and enforcing exclusive rights for each of the possible uses of a piece of music would mean that a central public agency – unable to value the net outcome of protection for each possible use of each piece – would manage a cadastral database (registering all the rights' owners of each of these potential uses), and would check any audio-visual production and any use of music to assess whether exclusive rights of uses are infringed. Since defence of exclusive rights of uses is costly, agents *de facto* bound their claims for exclusiveness when protection is decentralized. This results in a less complete, but less costly, IPR system.

These pre-existing justifications for a substantial decentralization of IPR institutions is reinforced by the capabilities of self-regulation provided by digital technologies.

A central agency to ensure enforcement and prevent capture

While strong arguments call for a decentralized settlement of IPRs in the digital world, other arguments lead to the mitigation of this initial view. Three questions have to be addressed. First, whether self-claim and decentralized negotiation among claimants of exclusive rights of use would lead to inconsistencies. Second, would the self-enforcement of IPRs lead to a consistent and workable institutional environment? Third, would a decentralized IPR system result in delineation and allocation of rights of uses guaranteeing the best possible collective outcome?

First, as mentioned in the case of rival goods, in an economic space in which there are no *ex ante* legitimate exclusive rights of uses, a full decentralization of the delineation and claims of exclusive rights of uses could result in overlaps (conflicting claims on the same resource) and inconsistencies (no claim for some exclusive rights of use of some resources, resulting *ex post* in potential conflicts or lack of investment to develop and maintain these free resources).

Would that be a problem for non-rival goods? In fact, everything depends upon the centralization of the enforcement mechanism. If it is centralized –



462 *Current issues from a property rights perspective*

that is, if an authority²¹ recognizes and makes enforceable the claims for exclusive use – then exclusion actually applies and one comes back to the reasoning given above about rival goods. If there is no such central authority to enforce these claims, and agents therefore spend resources locally to exclude others (for example, by encrypting their contents), then conflicting claims are not an issue, since they result in competition on the supply of twice-claimed exclusive rights of use. Since information is not a rival good, claims for exclusive uses compete but do not conflict. The decentralization of claims – of the ‘measurement’ of IPRs – is therefore neutral as long as the enforcement is decentralized.²²

Second, is the complete decentralization of IPR enforcement sustainable? As mentioned above, the enforcement of PRs relies generally on owners’ efforts together with the intervention of a last resort authority that benefits from lower costs and extended ability and credibility in punishing infringers. At least two reasons justify the intervention of such a mechanism of enforcement in the last resort. First, no cryptographic system is inviolable. Code-based protection is therefore imperfect.²³ Second, the enforceability of collective norms founding virtual communities is also in question. The self-enforceability of norms governing virtual communities is bounded by the ability of Internet users to access alternative communities, providing them with the same type of service, and by the ability of the supervision mechanisms of these communities to identify rule breakers and to actually expel them from the community. Indeed, Internet users can hide their behaviours, and the only identity that is certain over the Internet is that of each computer. Put another way, a code cannot guarantee *ex ante* the enforcement of rules (in general, including therefore the rules concerning the rights to use information sequences) and communities are bounded in their ability to supervise behaviours and retaliate in the case of rule infringement.²⁴

These call for a central mechanism granted with the power of constraint aimed at guaranteeing a minimum transparency so as to control how the protected contents are actually used. Indeed, virtual communities could be organized to hide the sharing of decrypted digital contents without the consent of owners. A mechanism limiting faking capacities would enable the owners of exclusive rights to enhance their supervision capabilities. In addition, and more fundamentally, there is a need for some exercise of constraint in the last resort. Indeed even if a self- or local regulatory mechanism can rely on capabilities to harm infringers, its credibility is bounded by the cost borne by the infringers in the case of exclusion (and by the costs borne by the entity exercising retaliations). If this cost is inferior to the benefit the infringers can make by violating the local regulation, the self-enforcement mechanism will be unable to prevent (major) infringements. A last resort enforcement device, which would be able to increase the costs of violating the local



regulation by implementing additional retaliation, would reinforce the enforceability of local regulation (see Milgrom et al. 1990; Brousseau and Fares 2000).

Behind the argument that a complete system of PRs could be entirely decentrally established thanks to information and communication technologies (ICTs), there is the assumption that PR settlements would cost nothing with the use of the technology. This assumption, which is implicit, could also lead to the opposite conclusion that a complete IPR system could be centrally created. In fact, lower costs of PR settlement do not mean that these costs are zero.²⁵ Encrypting digital information does not result therefore in a perfect control over its uses. Additional means have to be used to complete the incompleteness of these PRs. A central (traditional) PR institutional system could for instance back up the technological self-implemented protection (as in the music industry today). Economic agents could also try to decentrally reinforce technological locks by settling interindividual agreements. However, these contracts would necessitate an authority of last resort to guarantee their enforcement. Some centralization would therefore be necessary anyway. Positive measurement and enforcement costs unavoidably involves agents in having to mix centralization and decentralization to reduce these costs.

Third, beyond the question of the capability of a process based on self-claim and self-enforcement to generate consistent and workable PRs, the ability of such a decentralized process to generate efficiency has to be questioned, as well. If we admit that alternative institutional frameworks have contrasting impacts in terms of collective efficiency and distribution of wealth, some mechanisms to aggregate individual preferences have to be designed to select (even arbitrarily and imperfectly) a collective regulatory framework that would seek to result in the best collective outcome. Indeed, if one admits that various stakeholders have various interests and do not have the same ability to influence the decentralized settlement of IPRs, either because they have contrasting endowment or because they enter in the game at different periods while there are path-dependent phenomena (such as pre-emption), then decentralization does not guarantee that the delineation and allocation of PRs would be fair – by considering equally the various individual (and efficient) interests by allocating use rights so as to reach the best possible use of resources from a collective point of view. If one admits that stakeholders can have conflicting interests, one should admit that some type of centralization is needed to compare the various possible PR systems in terms of collective efficiency so as to choose the most efficient one, whatever the efficiency criteria is. The important point here is to design a process in which the interests of the wider set of stakeholders would be taken into account.

In the specific case of information and knowledge, a PR system based on self-claims and self-enforcement could in particular lead to excessive and



464 *Current issues from a property rights perspective*

indefinite private capture of these public goods. It would lead to distortive capture of monopoly rents, and to the hindering of the efficient diffusion of that information. Indeed, while information becomes a good whose uses are now eligible for technical exclusion, it remains a non-rival and indivisible good. It is therefore legitimate to question the optimal level of protection within the traditional debate that balances the advantages of strong incentives to create intangibles with those of a wide diffusion (see Besen and Raskind 1991). The example of freeware shows that sharing information on a very large scale maximizes the benefits of disclosure. In some cases, mandatory disclosure rules – especially if disclosure rules could be tailored to different audiences; for example, free access to published material to students and teachers in low-income countries – would be collectively optimal. Such rules could spontaneously emerge, as happened in the open-source software communities. However, there are also many situations in which it is doubtful that they would. Since investors in the creation of digital sequences could fear they would not get any return if they disclosed them, and since they can cheaply control access to them, it should result in an IPR system that would overprotect resources; in the sense that the collectivity would be deprived from the potential positive externalities of open access (externalities of diffusion, spillovers and so on). This calls for some centrality, both to select the collectively optimal system, and to compensate those who are harmed by a system in which PRs are bounded as compared to what they would get if a system of unlimited rights to control uses prevailed.

There is an additional reason for bounded PRs. The ability to use specific information or knowledge often depends upon the access to complementary information. A central system guaranteeing some fundamental rights of access to information should be able to guarantee the exploitation of these externalities.

The limitation of exclusive rights of use over information and knowledge should combine disclosure rules and the limitation of encryption capabilities. Indeed, the combination of the capability to encrypt with the long-term viability of monopolies leads to the possibility of controlling and preventing the free diffusion of information. This capability could be used in particular to reinforce barriers to entry, so as to allow endless capture of rents and the blocking of innovation and creation in the long run (by forbidding access and use of existing creations of the human mind). Such threats should lead to the bounding of agents' encryption capabilities (for example, mandatory registration of code keys to trustworthy third parties) so as to maintain a minimal level of transparency aimed at allowing supervision by some last resort authority in charge of preventing monopolistic capture. Moreover, reducing encryption capabilities would limit *de facto* the levels of barriers to entry, and therefore the strength of monopoly power.



The self-enforcement of PRs would therefore have to be supervised by some last resort authority ensuring that encryption and self-regulation are not combined to develop and exercise monopoly power, and to maintain competition in the long run. Indeed, competition is the best solution to provide agents and communities with incentives to implement efficient technical and organizational solutions in terms of knowledge production, use and sharing.

It has to be pointed out that bounding encryption capabilities would not be enough *per se* to ensure efficiency in the long run. Supervision of behaviour by a third party is essential since it would dissuade people from taking anticompetitive action, without forcing agents to be totally transparent about their behaviours and information exchanges. The protection of contents (both the privacy of information exchanges and property rights) leads to encryption, and it is not justified to broadcast publicly all information exchanges. It is, however, necessary to verify that information exchanges are not harmful for the collectivity as could be the case if they were aimed at setting up collusive agreements, infringing IPR or performing criminal activities. An independent and neutral third party in charge of supervision is therefore a good solution to deter indefinite monopolistic capture, while enabling the agents to preserve privacy and to protect access to their informational contents.

To conclude, since the code and the lists of subscribers (to a virtual community) are not perfect enforcement tools, and since information remains a non-rival good, a decentralized IPR system on the Internet could lead to inefficiencies. On the one hand, agents may have to dedicate too many resources to the enforcement of their claimed exclusive rights of use. On the other hand, information could be overprotected, both because the optimal level of diffusion would not be reached and because some players would use information protection to establish monopoly power. A last resort authority, in charge of guaranteeing the enforcement of rules established by local regulators, while guaranteeing that these rules result in a desirable level of diffusion, and that encryption cannot be used to hide contents and behaviours endlessly, would therefore be useful to guarantee a more efficient outcome of a decentralized process of IPR settlement.

Organizing a PR system on the Internet

Digital technologies challenge the relative efficiency of the existing alternative institutional frameworks. However, the decentralized and unorganized process of production of self-legitimated norms does not guarantee that the resulting norms will be either workable, or efficient. All these call for the organization of an institutional framework that will enable these weaknesses to be overcome. Stakes are huge since the Internet, as an infrastructure, is becoming an essential facility on which economic activity takes place, on



which individuals communicate and share information and knowledge, and through which collective goods are provided to citizens.

The decentralized process of PR settlement based on self-claims and self-enforcement that is made possible by the use of digital technologies has to be combined with central coordination aimed at avoiding the inefficiencies and weaknesses of self-regulation, and at implementing the most efficient solutions by taking into account the interests of the widest possible set of stakeholders, the public nature of information and the risks of having digital technologies used to deter competition and capture rents without time, or scale, or scope limits. It would therefore be worthwhile to set up a last resort authority, which would have to design and make enforceable constitutional principles aimed at guaranteeing some fundamental rights both for contents producers and for users. While decentralized systems of IPR settlement would enable agents to benefit from coordination frameworks well adapted to their specific needs and preferences, the last resort institution would maintain the consistency of the resulting systems of private norms, would ensure the enforceability of these self-regulations,²⁶ and would prevent capture of public wealth by individuals or groups. 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 uses.

This last resort regulation device should be submitted to democratic control and be 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 it will both settle conflicts and design the constitutional rules.

Beyond its logical justification, the implementation of a regulator of last resort is made possible on the Internet by the necessity of managing the addressing system centrally. The mastering of the management of the addressing system by the entity that would be responsible for the regulation 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 threat – excluding agents from access to the cyber-world by depriving them of IP addresses – 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 in or expulsion from the Internet.

Notes

- * This chapter was written when the author was a fellow at the International Centre for Economic Research (ICER, Turin), which is thanked for its support. It benefited from comments of participants in workshops held at the University of Turin, Statistic Norway, and the University of Paris I (ATOM). An earlier and broader version ('Internet regulation: does self-regulation require an institutional framework?') elicited useful suggestions



from Bruno Chaves (ATOM), Nicolas Curien (CNAM), Godefroy Dang N'Guyen (ENST-B), Mhand Fares (INRA), Didier Lebrun (ISOC), Hervé Nabarette (ATOM), Lee Davis (CBS) and Birgitte Andersen (Birkbeck, University of London). I warmly thank them all. Usual caveats apply.

1. This very fundamental understanding of property rights clearly differs from the legal notion of property rights, but the latter is included in the former. Barzel's and North's analyses aim at synthesizing how an institutional framework results in economic properties through the allocation of decision rights to agents and through their ability to be exchanged (to arrive at a more efficient use of resources). Their definition of property rights encompasses what we usually call property rights, but also the regulations that bound economic agents' decision rights, the law that establishes boundaries to the free will of agents, and the informal rules (such as social customs) that mitigate and frame individual freedom of decision, and contracts since they allow agents to delineate the rights of use transferred to other agents.
2. It can also be said in a more positive way: the central authority can ensure *ex ante* the absence of conflicting claims *ex post*, since it is able to design a system avoiding inconsistencies – mainly overlaps – among claimed rights of use.
3. When externalities occur, the price system does not reflect all the constraints of the economy. Going back to Coase (1960), we acknowledge and agree that 'externalities' are not natural characteristics, but the consequences of the incompleteness of the PR systems. However, if we agree that in any case, setting up a PR systems is costly, then we must recognize that any PR system is incomplete (since the marginal pay-off of delimitating and enforcing exclusive rights of use falls beyond the marginal costs of doing so at some point). Whether it is set up centrally or decentrally, an incomplete PR system generates externalities.
4. Of course, since the producers of these resources should get a return on their investments, the central authority can decide either to subsidize them in exchange for producing free goods (as in the 'public science' model), or to grant them with temporary and bounded exclusive rights of uses (as in the patent-copyright system).
5. Monopoly capture is inefficient in particular when it generates an underoptimal use of available resources, or when it hinders the dynamics of investment and innovation. As soon as the use of a resource is in some way not totally rival, a profit-maximizing monopoly will deprive some of the potential users from access, resulting in inefficiencies (especially if discrimination is costly and therefore imperfect). When networks effects (and in particular, increasing return of adoption) occur, a monopoly can block either the innovation process or the adoption of alternative solutions. Monopoly capture is then dynamically inefficient.
6. Completeness of property rights corresponds to an ideal. It would mean that any potential use of any resources would be identified and associated with a right granted to either an individual or a group. A complete PR system would enable almost costless transactions since agents would only have to bear the cost of meeting and agreeing on the terms of the exchange. Transaction would not be free, however, because the costs of the PR system would have to be taken into account.
7. Indeed, in a positive perspective one should admit that selection processes are not perfect, and that public institutions are subject to capture by private interests (whether they are bureaucrats, politicians or groups of interests). Both can prevent an efficient institutional design from emerging.
8. The 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 information processing devices (IPDs). It is the heart of the interoperability of the components or the various networks involved. The hypertext markup language (HTML) is the multimedia language of the Internet that enables any IPD to transform any kind of information (data, sound, image and so on) into codes that can be 'understood' by any other IPD. This is a common programming language that allows heterogeneous devices to interoperate when processing information.
9. From a logical point of view, the Internet relies on two basic principles. First, each IPD



468 *Current issues from a property rights perspective*

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 (for example, telephone) or distribution (for example, 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. Second, 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 – which then becomes a server – to provide the former with information processing or service. 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 addition of new IPDs (or software) that enrich the collection of basic services that can be combined to produce the various available services.

10. This is typically what happens today in the music industry. Major music companies try to code the recorded music they sell to avoid the duplication of their digital files. Generally, for instance, they make recorded songs available on the Internet to enable potential customers to listen. However, these digital files are coded either to reduce the quality of copies or to prevent copies from being made. Especially for most famous artists, hackers attempt to break these coded protections to display the music for free. In response, music companies develop tools to harm hackers' information systems. For instance, in case of infringement, viruses that attack the hacker's system can be implemented in the code. Music companies are also suspected of employing former hackers to track the hackers and attack their systems.
11. Indeed, software literally 'embodies' knowledge and makes it operable, since it implements routines to solve all kinds of problems. However, knowledge is also 'embodied' in databases, in text or audio-files explaining theories or ways to operate and so on.
12. It is often claimed that this is only true for small players, because governments are unable to detect and bring to court all the small infringements made by individuals and small and medium-sized enterprises. Moreover, if these individuals and small businesses do not have any assets located in the country where they infringe the law, the local government cannot retaliate. On the other hand, large companies should comply with most existing legal constraints since their behaviour is 'visible', and since they have in any case some form of tangible anchoring in all the countries where they have operations. Moreover, governments could try to deter them from breaking the law by threatening to harm their commercial reputation. Such arguments are weakened since large firms could conceal information-handling processes, and it can be costly for governments to prove that the law was broken. Moreover even if only small infringers are able to break the law with *de facto* impunity, billions of them could overwhelm traditional frameworks. This is typically what is happening today in the music industry.
13. Because the present Internet is still an imperfect substitute for most traditional network services – telephony, radio broadcasting, TV and so on – existing regulations can be maintained because bypass possibilities are limited. However, the development of broadband Internet, and the rise of a wide set of complementary technologies – such as e-books or printing on demand – will transform digital networks into a unified support for the diffusion and use of any type of content that will inevitably turn former regulations into illegitimate ones.
14. The communication capacity – the bandwidth – is the third rival resource on the Internet. That said, the Internet relies on principles that make the competition for bandwidth less acute in the Internet than in any other network. The end-to-end connectivity makes the totality of the remaining bandwidth available for marginal communication. Despite this principle, however, bandwidth remains a scarce resource. 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). Two types of problem then arise. First, a criterion to allocate the available bandwidth at each period has to be established. Second, the Internet operators must be encouraged to invest to limit the risks of network congestion (Frischmann 2001). While bandwidth is clearly a rival resource and raises PR delineation and allocation problems, it cannot be considered as an IPR problems. However, the analysis developed hereafter could be applied to the optimal design of a system to manage rights of use over bandwidth.

15. That has been *de facto* recognized by the users of the Internet and by those in charge of the management of the addressing system since the end of the 1990s. ICANN (see note 17) – in close cooperation with the World Intellectual Property Organization (WIPO) – progressively set up processes to recognize brand names and trademarks within the DNS. While in the early days of the commercial Internet, any user was allowed to register for exclusiveness in using any type of identifier as a DN – leading to the emergence of cybersquatting, a practice consisting in capturing famous names in order to resell them later to those who had made them famous or in order to develop services aimed at capturing customers valuing the reputation associated to this name – procedures have progressively been defined to enable owners of brand names to benefit from priority in getting exclusive rights to use these names in the DNS.
16. In fact, this is true from a logical, but not from an operational point of view. The Internet could be fully decentralized, but it is simpler and more efficient to maintain some elements of centralization. Network servers are intermediaries among the IPDs connected to the network. They take charge (both on the client and server sides) of the management of communication. This ranking of the network simplifies its topography and facilitates the routing of information among IPDs, but it is not mandatory to rank an end-to-end network. The key element of centralization, however, is the root server of the DNS. The nucleus of the DNS is a root file that establishes a single link between any DN and IP numbers. This root file is duplicated in several root servers that are themselves used by the IPDs connected to the network to address their communication to the right IPD. Having a limited number of copies of the root file facilitates the maintenance of the system. However, the root file could logically be copied in any IPD connected to the network to suppress any kind of technical centralization.
17. ICANN (Internet Corporation for Assigned Names and Numbers; www.icann.org) is the organization currently in charge of ‘governing’ the addressing system of the Internet. It is responsible for distributing IP numbers and DNs. It is a non-profit organization incorporated in the United States and set up in 1998. It operates under a delegation contract with the US government (Department of Commerce).
18. See the Internet Transparency, RFC-2775: <ftp://ftp.rfc-editor.org/in-notes/rfc2775.txt>; Blumenthal and Clark (2001).
19. For instance, if systems that allow large-scale barter of private copies of digital contents (for example, Napster or Gnutella) develop, the revenues of the creators of content will be affected, unless taxpayers are asked to compensate by contributing more to the funding of the production of works of art. In both cases, it is clear that the norm of free exchange applied by the members of an on-line community affects the welfare of members of off-line communities.
20. In a sense, this problem has been being addressed with the development of the numbers of ‘domains’. ICANN promoted the development of national domains (country code top level domains – ccTLDs – corresponding to the suffixes .fr, .uk, .cn and so on for each of the countries recognized by the United Nations) and of additional generic domains (global top level domains – GTLDs – corresponding to the suffixes .com, .org, .info, supposed to correspond to the type of organization that claim for exclusive uses rights [respectively, for the suffixes quoted above: commercial corporations, not-for-profit organizations, information providers]). However, there is clearly a conflict between the logic of the ccTLDs – which *de facto* endorses the existing geographical fragmentation of ‘property rights’ on names – and the logic of GTLDs – which tends to establish global property rights on names. Moreover, the ‘reputation’ of the various top level domains is unequal – .com being, for



470 *Current issues from a property rights perspective*

instance, the symbol of the Internet because it is understood as 'communication' rather than as 'commercial' by the public – creating a *de facto* hierarchy among the TLDs. The 'game' is also complicated by the fact that some countries with a specific suffix try to turn their ccTLDs into GTLDs – like the Tuvalu Islands attempting to grant any television channel in the world a domain name with the suffix .tv – and that there are many attempts to multiply the number of TLDs in order to create new 'labelized' information spaces: for example, .eu to be applied to any type of organization within the European Union, or .kids to be applied to sites targeting children with controlled contents. The resulting fuzziness leads clearly to a *de facto* globalization of property rights on names, in particular of brand names. Many owners of DNs, tend to register the same name with all the possible (and available) suffixes, whether they are GTLDs or ccTLDs. Indeed, famous brands want to avoid the new form of cyber-squatting that could develop with the multiplication of suffixes.

21. The authority can be a government, an intergovernmental agency, or a business alliance that would be able to deny access to contents to unentitled third parties. Think, for instance, of an alliance among major music companies.
22. If it were not, it would become a problem. However, decentralized claims are inconsistent with centralized enforcement. Indeed, in the latter case, the central supervision of uses would imply at least a mechanism that will centrally register claims of exclusive rights of use, which would have to check for the legitimacy and the absence of overlap among these claims.
23. This is typically the reason why the United States passed the Digital Millennium Copyright Act (DMCA) in 1998 to protect the code that protected contents, by severely punishing techniques and practices aimed at cracking codes. However, the DMCA did not take into account the necessity to guarantee openness in exchange of stronger institutional protection. See the end of this section.
24. The literature on private norms often refers to historical experiences (such as the medieval 'Law of Merchants') or to those norms that regulate many ethnic communities to point out the efficiency of decentralized self-regulation (see Granovetter 1985; Bernstein 1992, 1996; Cooter 1994, 1996). However, some papers also point out the limitations of self-regulation (see Milgrom et al. 1990). We pursue here such types of analysis. Indeed, and 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.
25. First, data processing costs are not zero and encrypting information is costly (for example, it takes time, generates failures and so on). Second, information-processing costs are often fallaciously assimilated in data processing costs. ICTs impact less on the first category than on the second. Indeed, to manage complex information management processes, it is necessary to benefit from the ability of the human brain to combine heterogeneous cognitive processes.
26. 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 their enforceability when necessary. The authority responsible in the last resort for the regulation of the system has therefore to use its credible threats to punish infringers of self-regulations. This is a common practice in the real world when the state becomes the guarantor of the enforceability of self-elaborated norms, like professional codes of conducts, by making them legally binding (see Bessy and Brousseau 1998; Brousseau and Fares 2000).

References

- Arrow, K.J. (1951), 'Alternative approaches to the theory of choice in risk-taking situation', *Econometrica*, **17**, 404–37.
- Barzel, Yoram (1989), *Economic Analysis of Property Rights*, Cambridge: Cambridge University Press.
- Baumol, William J., John C. Panzar and Robert D. Willig (1982), *Contestable Markets and the Theory of Industry Structure*, San Diego, CA: Harcourt Brace Jovanovich.



Property rights in the digital space 471

- Bernstein, L. (1992), 'Opting out of the legal system: extra legal contractual relations in the diamond industry', *Journal of Legal Studies*, **21**, 115–57.
- Bernstein, L. (1996), 'Merchant law in a merchant court: rethinking the code's search for immanent business norms', *University of Pennsylvania Law Review*, **144** (5), 1765–821.
- Besen, S.M. and L.J. Raskind (1991), 'An introduction to the law and economics of intellectual property', *Journal of Economic Perspectives*, **5**, 3–27.
- Bessy, Ch. and E. Brousseau (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', 19–21 September, Washington University, St. Louis, MO.
- Bessy, Ch. and E. Brousseau (1998), 'Technology licensing contracts: features and diversity', *International Review of Law and Economics*, **18**, 451–89.
- Blumenthal, M.S. and D.D. Clark (2001), 'Rethinking the design of the Internet: the end-to-end arguments vs. the brave new world', in B. Compaine and S. Greenstein (eds), *Communications Policy in Transition: The Internet and Beyond*, Cambridge, MA: MIT Press, http://www.ana.lcs.mit.edu/anaweb/PDF/Rethinking_2001.pdf, September.
- Brousseau, E. and M. Fares (2000), 'The incomplete contract theory and the new institutional economics approaches to contracts: substitutes or complements?', in C. Ménard (ed.), *Institutions, Contracts and Organizations: Perspectives from New Institutional Economics*, Cheltenham, UK and Northampton, MA, USA: Edward Elgar, pp. 399–421.
- Coase, R. (1960), 'The problem of social cost', *Journal of Law and Economics*, **3**, 1–42.
- Condorcet, Marie Jean Antoine Nicolas Caritat (Marquis de) (1785), *Essai sur l'application de l'analyse à la probabilité des décisions rendues à la pluralité des voix* [Essay on the Application of Analysis to the Probability of Majority Decisions], Electronic edition (1995), <http://gallica.bnf.fr/scripts/ConsultationTout.exe?E=0&O=N041718>, accessed 2002.
- Cooter, R.D. (1994), 'Structural adjudication and the new law merchant: a model of decentralized law', *International Review of Law and Economics*, **14**, 215–31.
- 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*, **144** (5), 1643–96.
- Crémer, J., P. Rey and J. Tirole (1999), 'Connectivity in the commercial Internet', Working Paper, Institut d'Économie Industrielle (IDEI), Toulouse.
- David, P.A. (1985), 'Clio and the economics of QWERTY', *American Economic Review*, **75** (2), May, 332–7.
- Frischmann, B.M. (2001), 'Privatization and commercialization of the Internet: rethinking market intervention into government and government intervention into the market', *Columbia Science and Technology Law Review*, vol. II (2000–2001), <http://www.stlr.org/html/archive/>, accessed 2002.
- Gaudeul, A. and B. Julien (2001), 'E-commerce, vers une analyse économique' [E-Commerce: Some Elements of Industrial Organization], *Revue Économique*, special issue, 'Économie de l'Internet', edited by E. Brousseau and N. Curien, **52** (HS), October, 97–118.
- Granovetter, M. (1985), 'Economic action and social structure: the problem of embeddedness', *American Journal of Sociology*, **91** (3), November, 481–510.
- Lemley, M.A. (1999), 'The law and economics of the internet norms', Working Paper, University of California at Berkeley.
- Lessig, Lawrence (1999), *Code and other Laws of Cyberspace*, New York: Basic Books.
- Libecap, G.D. (2002), 'A transactions costs approach to the analysis of property rights', in E. Brousseau and J.M. Glachant (eds), *The Economics of Contracts: Theories and Applications*, Cambridge: Cambridge University Press, pp. 140–56.
- Milgrom, P., D.C. North and B. Weingast (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.
- Noe, Th. H. and G. Parker (2000), 'Winner take all: competition, strategy, and the structure of returns in the Internet economy', Mimeo, Tulane University, November.
- North, Douglass C. (1990), *Institutions, Institutional Change and Economic Performance*, Cambridge: Cambridge University Press.



472 *Current issues from a property rights perspective*

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/>, accessed 2001.

Shapiro, Carl and Hal R. Varian (1999), *Information and Rules*, Cambridge, MA: Harvard Business School Press.

Shiff Berman, P. (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, 1263–310.

Tirole, J., J.-J. Laffont, S. Marcus and P. Rey (2001), 'Internet interconnection and the off-net-cost pricing principle', Working Paper, IDEI, Toulouse.

