Carving up the Internet : Jurisdiction, Legal Orders, and the Private/Public International Law Interface

Schultz, Thomas

How to cite

SCHULTZ, Thomas. Carving up the Internet : Jurisdiction, Legal Orders, and the Private/Public International Law Interface. In: European journal of international law, 2008, vol. 19, n° 4, p. 799–839. doi: 10.1093/ejil/chn040

This publication URL: https://archive-ouverte.unige.ch/unige:168238
Publication DOI: 10.1093/ejil/chn040

Carving up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface

Thomas Schultz*

Abstract

The Internet is caught between old forces of local territorialism and new forces characteristic of global economies. As a result, this article maintains that it may end up being carved or fragmented into discrete legal spheres. This development contradicts with the hitherto traditional vision of the Internet as a paradigmatic example of a borderless world of global transnationalism. This fragmentation is taking two forms: one vertical which reflects concerns of public policy and the protection of local values, the other horizontal which is driven by the rationale of commercial efficiency. The former (vertical), if not understood and handled properly, may lead to an informational impoverishment of the Internet. One response to this risk resides in new configurations of the appropriate jurisdictional bases for assertions of state power. I argue in favour of a double standard of jurisdiction for the regulation of Internet content: one, based on the principle of targeting, used to sanction behaviour, the other, an incarnation of the effects doctrine, used to prevent actions and fulfil the cathartic function of law. The latter (horizontal) form of fragmentation should lead us to rethink certain aspects of the concept of law, in particular with regard to legal pluralism, and to discover new places where law is to be found.

Introduction

The Internet is caught between old forces of local territorialism and new forces characteristic of global economies. As a result, it may end up being carved up or fragmented

* *Maître d'enseignement et de recherche* (Senior Lecturer), University of Geneva. This article was written during a post-doctoral research stay at the Lauterpacht Research Centre for International Law, Cambridge University, 2005–2006. The Swiss National Science Foundation and the Holcim Foundation for the Advancement of Academic Work provided support for this research. I owe the following people thanks for useful comments on an earlier draft: James Fry, Dan Joyce, Gil Limon, Kate Parlett, Sandy Sivakumaran, and Mehmet Toral.

EJIL (2008), Vol. 19 No. 4, 799–839 doi: 10.1093/ejil/chn040

into discrete legal spheres – a development which contradicts the hitherto traditional vision of the Internet as a paradigmatic example of a borderless world of global transnationalism.

The fragmentation is taking two forms. The first may be represented as vertical in nature; led by the forces of territorialism, it reflects concerns of public policy and the protection of local values. The second, which may be considered horizontal, is driven by the rationale of commercial efficiency.

The former (vertical), if not understood and handled properly, creates the risk of an informational impoverishment of the Internet. One response to this risk seems to reside in new configurations of the appropriate jurisdictional bases for assertions of state power. This form of fragmentation is indeed primarily a consequence of the current determinations of jurisdictional scopes, which tend to disregard the externalities which jurisdictional assertions create. Answers to this issue, so I contend, may be found in the reconsideration of private international law standards in the light of public international law standards of jurisdiction. On this basis, I argue in favour of a double standard of jurisdiction for the regulation of Internet content: one, based on the principle of targeting, used to sanction behaviour; the other, an incarnation of the effects doctrine, used to prevent actions and fulfil the cathartic function of law.

The latter (horizontal) form of fragmentation, which is of more academic interest, translates as the emergence, in certain specific and mainly commercial contexts, of anational and often cross-border normative orders which, at least sometimes, deserve the label of juridicity. The development of such private legal orders should lead us to rethink certain aspects of the concept of law, in particular with regard to legal pluralism, and to discover new places where law is to be found.

These two forms of evolution, the reasons behind them, their consequences, as well as likely responses, drive the narrative and argument of this article.

These developments are meaningful not only for the Internet in and of itself. They also matter for our more general understanding of law on the global plane. To understand why, one needs briefly to travel to Westphalia, in the 17th century. It was there, in the Westphalian cities of Münster and Osnabrück, that treaties were negotiated to end the Thirty Years' War and the Dutch Revolt. Out of these negotiations and the resulting treaties emerged principles of the sovereignty and equality of states, as well as of non-intervention in the affairs of another state. They contributed to the firm establishment of the principle of territoriality, understood in the sense of a political repartition of power and spheres of influence, an instantiation of each state's right to political self-determination.[1] From that time on, and for the better part of the last 300 years, law and governing were dominantly represented as strongly rooted in territory. But today this dominant mode of representing law and governing seems to be shifting[2] to the view that law on the international level is increasingly, in the words of Bruno Simma and

[1] M.N. Shaw, *International Law* (5th edn, 2003), at 21, 25.

[2] Roberts, 'After Government? On Representing Law Without the State', 68 *MLR* (2005) 1, at 3.

Dirk Pulkowski, 'a spread-out web of normativity'.[3] States are shown as inexorably losing ground. Juxtaposed pyramidal arrangements of state law are increasingly being replaced by more or less confused and overlapping networks of normativity, arranged in tangled hierarchies[4] – even though many residues of the former model stay unperturbed.[5] From the point of view of territoriality, transnationalism is replacing internationalism. This now fashionable view is marked by a number of paradigms, some of which are commonly shared prime examples embodying with particular clarity the characteristics which found the general view.[6] As was already briefly mentioned, our general understanding of the Internet forms one of the paradigms which underlie the general view of deterritorialization, transnationalism, state decline, and the replacement of national pyramids of normativity by global networks of spread-out normativity.[7] The Internet is commonly used as a landmark, a spearhead, a paradigmatic illustration of the transnationalist movement. Now, could it be that this general understanding of the Internet and its governance is a mere conventional wisdom, an idea that is 'simple, convenient, comfortable and comforting'?[8] There certainly exist tendencies towards transnationalism on the Internet, though not in its borderless and global guise, which is usually presumed. One may observe evolutions towards the constitution of legal systems which are transnational and largely autonomous with regard to the state – legal systems the juridicity of which may be affirmed on the basis of a solid, not wishy-washy, acceptance of law. This is the horizontal form of fragmentation mentioned above. Nonetheless, one can also discern evolutions that herald a return to some degree of nationalism, understood in the sense of a greater assertion of state power and a greater control over national territories as far as information flows are concerned. This is the vertical form of fragmentation.

The Internet and its regulation cannot be seen as a single phenomenon: if, on the one hand, commercial transnationalism undeniably takes place (though not in a borderless and global fashion), on the other hand, the protection of local values pushes for a return to a more Westphalian system. Given as much, the 'residues of the former model' mentioned earlier seem to be growing rather than receding, at least in this particular area. This article seeks to describe both of these trends and, in doing so, challenge the conventional wisdom that the Internet is inexorably global. The first part of the article considers, as an illustration, the evolution of another such conventional wisdom about the Internet – its 'unregulability' – that had been strongly anchored

[3] Simma and Pulkowski, 'Of Planets and the Universe: Self-contained Regimes in International Law', 17 *EJIL* (2006) 529, at 529. See also J.M. Kelly, *A Short History of Western Legal Theory* (Repr. edn, 1993), at 158ff, 175.

[4] On the concept of tangled hierarchies see D.R. Hofstadter, *Gödel, Escher, Bach: An Eternal Golden Braid* (1989), at 10; as applied to law see F. Ost and M. van de Kerchove, *Jalons pour une théorie critique du droit* (1987), at 213, F. Ost and M. van de Kerchove, *De la pyramide au réseau? Pour une théorie dialectique du droit* (2002), at 49–124.

[5] *Ibid.*, 14.

[6] On the concept of a paradigm see T.S. Kuhn, *The Structure of Scientific Revolutions* (1962).

[7] J. Goldsmith and T. Wu, *Who Controls the Internet? Illusions of a Borderless World* (2006), at 179, 181–183. See also Y. Benkler, *The Wealth of Networks* (2006).

[8] S.D. Levitt and S.J. Dubner, *Freakonomics* (2006), at 90, relying on the definition of conventional wisdom coined by J.K. Galbraith, *The Affluent Society* (1958).

in our general understanding but was shown to be patently wrong. The second part then introduces the two trends just mentioned, which will subsequently be treated separately and in detail in parts 3 and 4.

1 Conventional Wisdom about the Internet

The Internet used to be conceived of as a place that was free from regulation. It was thought that everything on the Internet would be free. Free not in the sense of obtaining something for free,[9] but in the sense of being unrestricted. To use Lawrence Lessig's words, it was not '"free" as in "free beer"', 'but "free" as in "free speech," "free markets," "free trade," "free enterprise," "free will," and "free elections".'[10] It was thought that this inability to regulate was an inherent characteristic of the online world. The famous *Declaration of the Independence of Cyberspace*, comes to mind:

> Governments of the Industrial World … You have no sovereignty where we gather… . I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us… . Cyberspace does not lie within your borders. Do not think that you can build it … It is an act of nature.[11]

Today those words sound odd, but they were taken very seriously for many years. If they were shocking at the time, it was because people believed they were shown this new creature, this realm of freedom that would challenge the social and political order that the modern nation-state had achieved. The spectre of the state of nature was looming.[12] But the words of the *Declaration* did not shock people in the sense that what it said was shockingly wrong. This inherent liberty on the Internet was taken for granted; it was used as a postulate until it was clearly demonstrated that what we can do on the Internet depends on the laws of technology just as our non-electronic actions depend on the laws of nature.[13] Technology allows us to do or prevents us from doing all the things we can or cannot do on the Internet, and technology can be shaped so as to enshrine values of liberty or values of control.[14] The proof of concept had been established. It had been shown that the Internet could be a place of exquisite control just as it used to be a place of exquisite liberty. Thus, the first 'inherent characteristic' claim had been repealed.

But another claim largely remained, and is still very much prevalent today. It is the idea that the Internet is necessarily global. The word 'cyberspace' at least partly sprang from there, and it shaped a great part of the meaning it subsequently acquired. The entire *lex*

[9] There were, of course, a good deal of those kinds of claims as well.

[10] L. Lessig, *Free Culture* (2004), at p. xiv.

[11] Barlow, 'A Declaration of the Independence of Cyberspace' (1996), available at: www.eff.org/~barlow/Declaration-Final.html.

[12] This understanding is described in Ost, 'Mondialisation, globalisation, universalisation: s'arracher, encore et toujours, à l'état de nature', in C.-A. Morand (ed.), *Le droit saisi par la mondialisation* (2001).

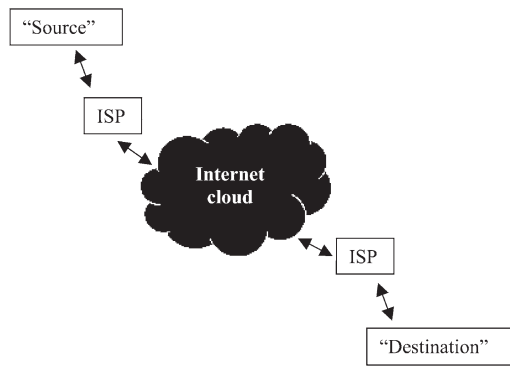
[13] Most famously demonstrated by L. Lessig, *Code and Other Laws of Cyberspace* (1999), at 89 and Reidenberg, 'States and Internet Enforcement', 1 *U Ottawa L & Technology J* (2003–2004) 213.

[14] This is the main argument in Lessig, *supra* note 13.

electronica movement is built on that assumption.[15] Most writings on the regulation of the Internet insist on the idea that what marks it as different is that it is global. Such 'illusions of a borderless world'[16] remain very strongly anchored in our collective imagination. But the reality appears to be that the Internet is being carved up into discrete legal spheres.

2 Two Forms of Internet Segmentation

It is probably correct to argue that we 'used to speak accurately of *the* Internet'.[17] It used to be sensible to reduce the Internet to a single network of computers and people behind most of those computers, hosting and using information always only a few clicks away, regardless of how near or far in physical space. This was precisely the intent of the creators of the Internet; they connected different, smaller networks together; they taught all those networks to speak a single common language (the Internet Protocol language); they integrated all those lesser networks into a global whole. And they embedded the characteristic of decentralization into the very foundational technical architecture of the Internet: the Internet has no centre or central authority through which all communications would travel and which could regulate all those communications.[18] This is what we call the Internet 'cloud', which symbolizes the unpredictability of the path that communications will take from one point to another. To borrow from Jonathan Zittrain, it may be represented in the following form:[19]



[15] The *lex electronica* is the idea of a development of a sort of *lex mercatoria* for electronic transactions on the Internet. See, for instance, Hardy, 'The Proper Legal Regime for "Cyberspace"', 55 *U Pittsburgh L Rev* (1994) 993, at 1021; Johnson and Post, 'Law and Borders: The Rise of Law in Cyberspace', 48 *Stanford L Rev* (1996) 1367, at 1389; V. Gautrais, *Le contrat électronique international. Encadrement juridique* (2002); Trakman, 'From the Medieval Law Merchant to E-Merchant Law', 53 *U Toronto LJ* (2003) 265; Farrell, 'Hybrid Institutions and the Law: Outlaw Arrangements or Interface Solutions', 23 *Zeitschrift für Rechtssoziologie* (2002) 25.

[16] See Goldsmith and Wu, *supra* note 7.

[17] Zittrain, 'Be Careful What You Ask For: Reconciling a Global Internet and Local Law', in A. Thierer and C.W. Crews (eds), *Who Rules the Net? Internet Governance and Jurisdiction* (2003), at 13.

[18] *Ibid.*

[19] Zittrain, 'Internet Points of Control', 44 *Boston College L Rev* (2003) 653, at 656.

This technical characteristic of the Internet led inevitably to the assumption that there is only one cyberspace. And this characteristic of the Internet made people marvel at the fact that, for most purposes of Internet activities, they could forget about the geographical distance which separates them from those they wanted to trade bits with. Web entrepreneurs were jubilant about the idea that they could broadcast to the entire world with minimal investment, that setting up a single website would offer its contents to everyone connected to the network, wherever they may be found in real space.[20] Internet users were amazed that they could remotely access the same information on the web that local users could. All this was thought to be good and desirable. 'Netizens' of the 'Global Village' were painting the town red.

But then the tide reversed. Then came libel originating in distant countries, stock manipulation from afar, worldwide domain name cybersquatting, sales tax circumvention by citizens purchasing faraway goods, hate speech websites located in countries protecting this kind of expression, online casinos based within the territory of states encouraging this business as it would almost exclusively affect foreign people in foreign countries while generating tax revenues, and worse.[21] The dark side of the Web manifested itself, and it triggered a movement for cultural and nationalistic withdrawal. People started to say that they did not want outlandish foreigners to do the equivalent of standing in the garden in front of their house doing things that are regarded with outright repugnance in their community. The French were anxious at the thought of there being, just around the corner, defiant Americans believing it is their fundamental right to say whatever they want to say, even if it involves an apology for Nazism.[22] In the United States, people were incensed about lax foreign governments not cracking down on online casinos, which were intruding into American homes and offices, computers, and mobile phones, to fuel compulsive gambling.[23] Many countries became concerned about incitements to terrorism and appeals to fund terrorist organizations flowing into their country simply by dint of being globally accessible. Some governments began to consider blocking by technical means local residents' access to foreign Internet sources that glorify terrorism.[24] Other governments grew increasingly apprehensive about the West spreading its culture and values throughout the world by a mere information transfer into territories which were previously exposed mainly to local information. Suddenly, the free and global character of the Internet started to be considered an evil. The global Internet community started to think that, after all, it did not want to be a single community, but several, and that each community should be allowed to live according to its internal

[20] Zittrain, *supra* note 17, at 13ff.

[21] *Ibid.*, at 13–14.

[22] See the landmark example of the Yahoo case, *infra* notes 54ff and accompanying text.

[23] See the various studies reported in Swiss Institute of Comparative Law, *Cross-border Gambling on the Internet: Challenging National and International Law* (2004) and Reidenberg, *supra* note 13, 219–220.

[24] See, for instance, Edwards, 'From Child Porn to China, in One Cleanfeed', 3 *SCRIPT-ed* (2006) 174, at 175. More generally see Goldsmith and Wu, *supra* note 7, at 153. See also Reidenberg, 'Yahoo and Democracy on the Internet', 42 *Jurimetrics J* (2002) 261, at 275.

fundamental values, according to its own choices of public policy (in the sense of *ordre public*), which partake of the expression of each nation's *Volksgeist*.[25] The Internet should be free, most agreed, but only insofar as this freedom stopped short of violating the fundamental principles underlying the operation of each state's legal system. The 'ancient principles governing law and politics within nations'[26] were being challenged. The forces behind them were not about to be pushed around and came back to re-establish the 'older and stronger order whose relevance remains inescapable'.[27]

A somewhat similar phenomenon started to take shape in another context. As e-commerce developed, people started to shop increasingly abroad, and frequently for small amounts. Small cross-border transactions burgeoned. Again, it was considered to be a remarkable achievement to be just a click away from well-stocked bookshops in the United States and retailers of cheap electronic equipment in Hong Kong. But in this context, the issue that quickly emerged was the resolution of disputes arising out of such transactions. It is nonsensical to start a court action against a foreign business, for instance, over a few books or a laptop computer. Something had to be created on the Internet that made it feel 'local', predictable, and with easily accessible legal remedies.

The way that the form of regulation is starting to change as a reaction to these concerns is in my view a transformation which will profoundly mark the evolution of the Internet. Under the pressure of public policy protection and commercial efficiency, the Internet will increasingly be carved up into distinct spheres or virtual spaces governed by different rule-sets. My contention is that this evolution will follow two main avenues. On the one hand, states will develop increasingly efficacious and legitimate processes of juridical and technological control in order to safeguard local values.[28] On the other hand, online communities of various kinds, albeit primarily of a commercial nature, will further the development of their social norms into private legal systems. The following two sections explore these two avenues, but before that one may summarize these evolutions with the following chart:

THE TWO FORMS OF 'CARVING UP'	*The 'billiard balls' process*	*The 'layers' process*
Bases	Territorial delimitation	Delimitation by 'slice of life' or activity; non-territorial
Techniques	States building electronic fences to block incoming traffic	Electronic marketplaces creating their own normative orders

[25] See generally C. Engel and K.H. Keller, *Global Networks and Local Values. A Comparative Look at Germany and the United States* (2002), at 46ff.

[26] Goldsmith and Wu, *supra* note 7, at p. ix.

[27] *Ibid.*, also at 183.

[28] For a similar though in its implementation significantly different argument, see *ibid.*, at 149–150.

Driving forces	Public policy/local values (no reason why we should not protect online the values we protect offline)	Commercial efficiency (simplification of applicable rules and dispute resolution)
Community basis	Proximity	Selective ties
Primary subject-matters concerned	Torts and criminal offences	Contracts
Situations	'Public policy' situations	'*Lex mercatoria*' situations
Instrumentalities	International law and technology	Online 'life' or identity
Values involved	Geography-dependent moral and social values	Geography-independent moral and social values
Forms	Public legal systems	Private legal systems
Lessons	Inherent global character of the Internet is as wrong as John Perry Barlow's unregulability claim was: technologies start to develop which allow geographic zoning of the Internet.	Public legal systems may not be adapted for the regulation of certain forms of e-commerce, just as they are not for certain forms of international commerce (arbitration and *lex mercatoria*).

3 The Billiard Balls Evolution

Safeguarding local values is one of the foundational roles of the state, part of the national (as opposed to universal) social contract.[29] As Hegel argued, the state embodies and expresses the *Volksgeist;* it is the vehicle of the fulfilment of the collective will (and thereby of the individual will) and must consequently protect the fundamental axiological references of its population.[30] It is further a role inherent in the nature of modern nation-states. Originally, nation-states had to subject smaller feudal, religious, and customary communities in order to impose a unified and centralized political structure. The separatism underlying personal relations in feudalism had to be marshalled by a unifying territorial relationship.[31] From above, as it were, the powers of the Papacy and the Holy Roman Empire also had to be warded off.[32] An important means used in the struggle against separatism and regional or global affiliations was to 'transcend ethnic, religious and other cleavages in a political construction'.[33]

[29] As applied to the regulation of the Internet: Reidenberg, *supra* note 13, at 216ff.

[30] G.W.F. Hegel, *Elements of the Philosophy of Right* (ed. A.W. Wood, 1991 [1821]), at 275.

[31] Yntema, 'The Historic Bases of Private International Law', 2 *Am J Comp L* (1953) 297, at 305; Mills, 'The Private History of International Law', 55 *ICLQ* (2006) 1, at 11–13, with further references.

[32] *Ibid.*, at 16, Kelly, *supra* note 3, at 200.

[33] Ost and van de Kerchove, *De la pyramide au réseau?, supra* note 4, at 128.

Smaller discrete communities had to be superseded by the one overarching 'imagined community' which is the nation.[34] And the development and subsequent safeguarding of fundamental shared values are foundational for the creation and sustaining of this community. The modern nation-state is in this sense merely the equation of an imagined community and 'imagined geographies',[35] namely the territory of the state. To protect such values is to protect the imagined community that is the nation.

The protection of such local values lies at the heart of modern conceptions of political sovereignty, as they originated from the Peace of Westphalia and the works of Machiavelli, Bodin, and Hobbes.[36] At this time, sovereignty took on the exclusively defining dimension of territoriality (and the concept of territorial sovereignty emerged), marking the rise of the territorial state.[37] This historical and legal theoretical development ascribed two attributes to territorial sovereignty: one internal, founding the state's increasing power and prominence over local communities, the other external, establishing the states' equality and independence. It might be enlightening to conceive of this relationship between states in terms of a co-ordination game governed by the agreed rule of the international Westphalian repartition.[38] This co-ordination game may be seen (somewhat anachronistically) as forming the groundwork of Savigny's approach based on the 'community of law among independent states'.[39] In opposition to the positivist theory of international law or state voluntarism,[40] it is the idea of a natural law approach to private international law that derives rules of private international law 'from the nature of the subject itself', as expressed by von Bar writing in Savigny's wake.[41] It is a conception of private international law where the international community of law 'restricts all territorial laws, and defines their competency',[42] an approach that, in more fashionable terms, takes into account the interface between

[34] B.R. Anderson, *Imagined Communities: Reflections on the Origins and Spread of Nationalism* (1983). On the nation as a product of modernity see E. Gellner *Nations and Nationalism* (1983). See also Gupta and Ferguson, 'Beyond "Culture": Space, Identity, and the Politics of Difference', in A. Gupta and J. Ferguson (eds), *Culture, Power, Place: Explorations in Critical Anthropology* (1997) and Rée, 'Cosmopolitanism and the Experience of Nationality', in P. Cheah and B. Robbins (eds), *Cosmopolitics: Thinking and Feeling Beyond the Nation* (1998).

[35] E.W. Said, *Orientalism* (1978). See also A. Giddens, *The Nation-State and Violence* (1985), at 125.

[36] N. Machiavelli *The Prince* (transl. G. Bull, 1999 [1513]); J. Bodin, *Les six livres de la République* (ed. C. Frémont, M.-D. Couzinet, and H. Rochais, 1986 [1576]); T. Hobbes, *Leviathan* (2005 [1651]). For commentaries on these authors and on modern conceptions of sovereignty see Shaw, *supra* note 1, at 21, 25; L. von Bar, *The Theory and Practice of Private International Law* (2nd edn, 1892), at 29; Yntema, *supra* note 31, at 305.

[37] Mills, *supra* note 31, at 13–14.

[38] Gillroy, 'Justice-as-Sovereignty: An Application of David Hume's Philosophical-Politics to the Origins of International Law', (2006) ExpressO Preprint Series Working Paper 1494, available at: http://law.bepress.com/expresso/eps/1494, e.g., at 30.

[39] F.C. von Savigny, *A Treatise on the Conflict of Laws and the Limits of their Operation in Respect of Place and Time* (1880), at 71.

[40] The positive theory of international law sees international law as a pure product of the will of the states: see P. Allott, *The Health of Nations* (2002), at 331 and Mills, *supra* note 31, at 15ff.

[41] von Bar, *supra* note 36, at 77.

[42] *Ibid.*, at 56. See further Mills, *supra* note 31, at 33–37.

private and public international law.[43] The protection of local values should stop short of disrupting the Westphalian co-ordination equilibrium,[44] which is what the various incarnations of the concept of jurisdiction seek to achieve. The avoidance of undue encroachment on other territories is a fundamental principle of jurisdiction as a co-ordination game. Put in more traditional terms, it is the idea that 'a state is, as a general matter, *prima facie* free to legislate or regulate with respect to persons or events beyond its territory, as long as doing so does not interfere with the same right of states that may have a closer connection to those persons or events'.[45] This non-intervention in the affairs of other states, Ian Brownlie explains, is a corollary of the independence and equality of states.[46] At a foundational level, the principle also permeates constructions of private international law rules. A recent study of the foundations of conflict of law rules concludes:

> Private international law rules and approaches do not merely reflect ... a dialectic between public policies (such as justice, certainty, individual autonomy) within each State. They are also engaged in both responding to and indeed in constructing an international order which is reflected in a set of international norms.[47]

To reconcile these two imperatives – to protect local values without encroaching on the territory of other states – is the fundamental problem of state intervention on the Internet. Protection of local values is often presented as coming at the price of severe extraterritorial effects.[48] But juridical and technical mechanisms are currently developing which will allow one to navigate more securely between Scylla and Charybdis. On the one hand, one may discern the re-emergence of a latent understanding that private international law is not exclusively private in its nature and function, that it goes far beyond supporting the global (in this case electronic) market economy and that it may, in accordance with Savigny's original approach, have a global regulatory role to play in the international community of law, in principled contradiction to the

[43] *Ibid.*, at 35: '[i]t is central to Savigny's approach that the private international law rules he developed were universal and common to all nations – part of an international community of law, derived from the fact of a community of nations. This may be contrasted with the conception of private international law resulting from the positivist theory of international law described above, in which private international law is (sometimes ambiguously) excluded from the domain of international law, and conceived of as part of each State's (voluntary) domestic law'.

[44] Gillroy, *supra* note 38, at 31.

[45] J.H. Currie, *Public International Law* (2001), at 299.

[46] I. Brownlie, *Principles of Public International Law* (6th edn, 2003), at 290. See also A. Cassese, *International Law* (2nd edn, 2005), at 55, who explains that the principle of non-intervention in internal affairs of other states is 'designed to ensure that each state respects the fundamental prerogatives of the other members of the community'.

[47] Mills, *supra* note 31, at 3–4. This takes position against a radical positivist theory of international law which, illustrated by Dicey's approach, holds that private international law 'is not part of any sort of international law or international order': Mills, referring to A.V. Dicey, *Digest of the Law of England with Reference to the Conflict of Laws* (1896) and L. Collins (ed.), *Dicey and Morris on the Conflict of Laws* (13th edn, 2000), at 4.

[48] E.g., Reidenberg, *supra* note 24, *passim*, e.g., 265.

acceptance ascribed to it by the positivist theory of international law.[49] On the other hand, a distinction in the regulatory approach of states is increasingly being made between, first, the sanctioning of behaviour and the redistribution of resources and, secondly, the *ex ante* prevention of certain actions from exerting certain effects. The first part of these developments relates to a fine tuning of jurisdictional heads and the second to information filtering strategies.

Both parts of these developments, which will be reviewed in the following sections, appear likely to lead to an increase in the exercise of regulatory power by states, which in turn would contribute to the carving up of the Internet on the basis of national delimitations. To be sure, the substantive differences among nation-states are more likely to cause different efficacious national, or possibly regional, regulations than to pre-empt the problem of conflicting values by dint of global harmonization, which is the opposite variant into which the regulation of the Internet is sometimes said to crystallize.[50] This is what I mean by the billiard balls evolution of the regulation of the Internet.[51] The examples that follow are meant to serve as illustrations of this issue.

At this juncture, it must be pointed out that I will scarcely discriminate between civil and criminal cases, contractual and tort matters. The focus of this article is on foundational common trends,[52] and it is thus not the place for an exhaustive survey, or even a selective survey, of the many discrete legal developments presented elsewhere.[53]

A *Illustrations*

In early 2000, Marc Knobel, a French Jew, was surfing on the Internet when he suddenly stumbled upon a website displaying various Nazi memorabilia, ranging from

[49] See generally Mills, *supra* note 31. See further Neff, 'A Short History of International Law', in M. Evans (ed.), *International Law* (2003) at 31, 45; Kennedy, 'International Law and the 19th Century: History of an Illusion', 65 *Nordic J Intl L* (1996) 385, at 409–410.

[50] Goldsmith, 'The Internet, Conflicts of Regulation, and International Harmonization', in C. Engel and K.H. Keller (eds), *Governance in the Light of Differing Local Values* (2000), at 205. See also, for an account of the concrete failure of harmonization through international conventions, with particular consideration of the Cybercrime Convention, Goldsmith and Wu, *supra* note 7, at 165–167.

[51] The image of billiard balls was, for instance, used by Arnold Wolfers in his model explicating the Realist claim that only the actions of states mattered despite the on-going development of the power of supra- and sub-national actors: A. Wolfers, *Discord and Collaboration; Essays on International Politics* (1962). The same image will be used here in the same spirit, but taken to a less radical extent.

[52] At this generalist level one may side with Brownlie, *supra* note 46, at 298, when he writes that '[t]here is in principle no great difference between the problems created by assertions of civil and criminal jurisdiction over aliens'.

[53] For such a survey see the following: on jurisdiction for contract claims, Kaufmann-Kohler, 'Commerce électronique: droit applicable et résolution des litiges', *Hague Lectures* (forthcoming, 2009) and Hörnle, 'Country of Origin Regulation in Cross-border Media: One Step beyond the Freedom to Provide Services', 54 *ICLQ* (2005) 89. On jurisdiction for tort claims see Bigos, 'Jurisdiction Over Cross-border Wrongs on the Internet', 54 *ICLQ* (2005) 585. On jurisdiction for criminal cases relating to the Internet see Kohl, 'Who has the Right to Govern Online Activity? A Criminal and Civil Point of View', 18 *Int'l Rev L, Computers & Technology* (2004) 387; Hayashi, 'The Information Revolution and the Rules of Jurisdiction in Public International Law', in M. Dunn, V. Mauer, and S.-F. Krishna-Hensel (eds), *The Resurgence of the State: Trend and Processes in Cyberspace Governance* (2007), at 59.

replicas of Zyklon B gas canisters, pictures of concentration camps, swastikas in various forms, to pieces of the equipment of Waffen-SS soldiers. All these objects were up for sale on the web page, which was hosted by Yahoo. The page was hosted on the American server of an American company, but it was, just like almost any website, accessible from France. Selling such objects is illegal under French criminal law,[54] but it is legal in the United States as it is protected by the First Amendment. Marc Knobel decided to initiate proceedings against Yahoo in a Paris court on behalf of various anti-Semitism and anti-racism associations. The French judge who heard the case quickly rose to fame by deciding that the Tribunal de Grande Instance de Paris had jurisdiction over the case and handing down a judgment ordering Yahoo to take down the web page, and to pay a symbolic fine.[55] Yahoo vehemently protested, arguing that if French law were to apply to an American website, then why not English law, Russian law, Israeli law, as well as the laws of Saudi Arabia, Iran, and China.[56]

A second story starts in October 2005, when the French fashion design company Louis Feraud International requested enforcement in New York of a French court decision which had awarded damages to the fashion designers because the defendant, a US company called Viewfinder, had posted fashion show photos on its website. These photos, the French company claimed, constituted a copyright violation because they showed fashion designs that belonged to the French company and thus violated the company's intellectual property rights granted by French law. The New York court rejected the motion for enforcement on the ground that the photos were published in the United States and were protected by the First Amendment, acting as a barrier to the extent of copyright.[57] In other words, the New York court held that the assertion of prescriptive jurisdiction by the French state had gone too far, that it was exorbitant and that it could not be admitted that it extended to publications in the United States.

These two cases serve as illustrations of two radically different ways of thinking about the relationship between Internet activities and territory, and thus about the appropriate scope of state power. If they were followed globally, both of them would have tremendous disadvantages. The former translates into a too broad basis of jurisdiction, the latter into a too narrow one – a middle path is needed. This is what the following will expound.

[54] Art. R.645 of the French Penal Code.

[55] See *La Ligue Contre le Racisme et l'Antisémitisme (LICRA) and l'Union des Etudiants Juifs de France (UEJF) v. Yahoo Inc! and Yahoo France*, Trib. de 1re Instance, Paris, interlocutory court orders of 22 May 2000, 22 Aug., and 20 Nov. 2000.

[56] The *Yahoo* case is the single most frequently examined case in the field of cyberlaw. Its details have been simplified for illustrative purposes. For a particularly enjoyable description see Goldsmith and Wu, *supra* note 7, at 1ff. This case has been analysed by a large number of authors in various fora, among whom the following have provided some of the most interesting discussions: Muir-Watt, 'Yahoo! Cyber-Collision of Cultures: Who Regulates?', 24 *Michigan J Int'l L* (2003) 673; Reidenberg, *supra* note 24; Berman, 'The Globalization of Jurisdiction', 151 *U Pennsylvania L Rev* (2002) 311.

[57] *Louis Feraud Int'l SARL v Viewfinder Inc,* 406 F Supp 2d 274 (SDNY 2005).

B *Jurisdiction Heads*

The following, in an effort to systematize and to simplify, seeks to bring under three heads the main past, present, and (predictably) future jurisdictional approaches to the regulation of Internet content: subjective territoriality, the effects doctrine, and different standards that may be referred to as targeting.

1 Subjective Territoriality

What the New York court in *Louis Feraud v. Viewfinder* did was in substance to express, through its refusal to grant enforcement, its disapproval of the exercise of jurisdiction as it was effected by the French court. It considered that the appropriate rule for jurisdiction in such cases was the subjective territorial principle – a state's authority under international law to regulate activity originating within its territory.[58] If this approach was followed globally, then websites would be subject only to the law of the state from which the flow of information stems. It would make forum shopping very easy, as it would be sufficient to find a country with the appropriate legal regime and publish any content there, such content remaining, in principle, accessible from the place where the publisher actually wanted it to be accessible, even if it was in violation of the laws of the country from which it was accessed. In other words, a strict application of the territoriality principle, as contemplated by the New York court, would lead to the under-protection of the values and the public policy choices of the forum state. It would seem inappropriate to 'decline to intervene simply because a defendant is wholly absent, since the effects of the defendant's Internet behaviour are still felt locally'.[59] Or, as Horatia Muir-Watt puts it, 'there is no reason that the interests of the society in which the harmful effects of free-flowing data are suffered should subordinate themselves to the ideological claim that the use of a borderless medium in some way modifies accountability for activities conducted through it'.[60]

It may well be that the territoriality principle is, in and of itself, 'by far the soundest basis of prescriptive jurisdiction',[61] but it quite clearly seems a too restrictive basis of jurisdiction in the face of information flows potentially having effects in every country of the world.

2 Effects

It was because the effects of Internet behaviour were felt in France that the French court in the *Yahoo* case decided to assert jurisdiction.[62] The Court considered that Yahoo's behaviour in violation of the French Penal Code, which 'was revealed to be unintentional', led to 'damages [which] were incurred in France'.[63] The French Yahoo court did not phrase the debate in terms of rules of jurisdiction in international

[58] Currie, *supra* note 45, at 300.

[59] Zittrain, *supra* note 17, at 18. See also Kohl, *supra* note 53, at 403 and Geist, 'Is There a There There? Toward Greater Certainty for Internet Jurisdiction', 16 *Berkeley Tech LJ* (2001) 1345, at 1357.

[60] Muir-Watt, *supra* note 56, at 695. See also Goldsmith and Wu, *supra* note 7, at 157.

[61] Currie, *supra* note 45, at 300.

[62] See, for instance, Geist, 'The Legal Implications of the Yahoo! Inc. Nazi Memorabilia Dispute' (2001), available at: www.juriscom.net/en/uni/doc/yahoo/geist.htm.

[63] *Supra* note 55, French interlocutory orders of 22 May and 22 Aug. 2000.

law, but merely decided that 'by permitting the display of these items and the possible participation of Internet users in France in such an exposition/sale, Yahoo commits a wrong within French territory'.[64] Had the court considered the issue in terms of jurisdiction in international law, one may surmise that it would have relied on either the effects doctrine or objective territoriality.[65] The former, the admissibility of which under international law is controversial,[66] grants authority to regulate to the state on the territory of which deleterious or harmful effects are exerted.[67] The latter is the basis of a state's authority to regulate activity that is consummated on its territory.[68] The distinction is more precisely that only the effects doctrine may be a basis for jurisdiction when 'no constituent element of the offence takes place within the territory of the prescribing state'.[69] Whether the jurisdiction of France in the *Yahoo* case was covered by the objective territoriality principle or only the effects doctrine depends on whether we consider the availability of information within a territory to be a constituent element of the offence. As I will maintain below, to reject this consideration and to argue that the only basis for jurisdiction in the *Yahoo* case was the effects doctrine seems to be the most reasonable solution.[70] It does not in any event make any significant difference for the present developments.

Now, what would happen if the approach of the *Yahoo* case were followed globally, if the effects doctrine or the objective territoriality principle generally were used as a jurisdictional basis for Internet behaviours? It is a generally held view that this would lead to the 'slowest ship in the convoy problem'.[71] This is the idea that the universal availability of information on the Internet may potentially have universal effects which, if the effects doctrine is given application, may lead to assertions of jurisdiction in virtually every state over wrongs created by information being available on the Internet.[72] Such over-broad regulatory reach and overlapping jurisdiction would

[64] *Ibid.*

[65] See, e.g., Hayashi, *supra* note 53, for an interpretation of the *Yahoo* case as an instance of objective territoriality.

[66] J. Combacau and S. Sur, *Droit international public* (6th edn, 2004), at 339, 354–355.

[67] See *United States v. Aluminium Company of America,* 148 F 2d 416 (2nd Cir. 1945) and Currie, *supra* note 45, at 300–303. It may be noted that, outside the Internet at least, the effects doctrine tends to relate to economic effects rather than effects generally – this is a first hint that, as we will see in what follows, this basis for jurisdiction is inappropriate to regulate the effects of Internet activities.

[68] See *The SS Lotus (France v. Turkey)* [1928] PCIJ Series A, No 10, at 25.

[69] O'Keefe, 'Universal Jurisdiction – Clarifying the Basic Concept', 2 *J Int'l Criminal Justice* (2004) 735, at 739; Bowett, 'Jurisdiction: Changing Patterns of Authority over Activities and Resources', 53 *BYIL* (1982) 1, at 7.

[70] Similarly, Kohl, 'Eggs, Jurisdiction, and the Internet', 51 *ICLQ* (2002) 555, at 577; Manolopoulos, 'Raising "Cyber-Borders": The Interaction between Law and Technology', 11 *Int'l J Law & Technology (IJL & T)* (2003) 40.

[71] Zittrain, *supra* note 17, at 20.

[72] As David Post put it in his slightly provocatively simplifying style, '[t]he effects of cyberspace transactions are felt *everywhere*, simultaneously and equally in all corners of the global network': Post, 'Governing Cyberspace', 43 *Wayne L Rev* (1996) 155, at 162. See further Zittrain, *supra* note 17, at 20. Going on a test based on objective territoriality would of course produce the same results if any inflow of information were construed to constitute the consumption of an act.

make the life of producers of information flows impossible. They would have to comply with the laws of the most restrictive jurisdiction to avoid the risk of being hauled before unexpected courts.[73] The nub of the argument is that information made available on the Internet would have to comply with the laws of the entire world, and the most restrictive law in the world – the 'slowest ship' – would thus be able to set the tone.[74]

In reality the problem is less severe than this general view suggests. This is so because, as Jack Goldsmith observes, enforcement jurisdiction is not affected by this overlapping of a large number of laws.[75] Enforcement jurisdiction, one may recall, is the authority actually to enforce the law by inducing or compelling compliance with it.[76] It is what gives regulation its teeth and makes it effective. This form of jurisdiction has a strictly territorial basis,[77] which means that in the absence of extradition – which is unlikely to be granted with respect to the vast majority of Internet matters[78] – a state can enforce its laws only against in-state actors, against entities with a presence on the territory of the state or with assets there. The distinction between prescriptive and adjudicative jurisdiction, on the one hand, and enforcement jurisdiction, on the other, is what allowed Joseph Story, almost 200 years ago, to maintain that 'whatever force and obligation the laws of one country have in another, depends solely upon [the latter's] own express or tacit consent'.[79] It means that providers of Internet content need to worry mainly about the regulations of the states in which they have a presence or assets. Enforcement jurisdiction acts as a limiting factor, reducing the overlapping of directly effective regulations to the various states where Internet actors have a presence or assets, which falls somewhere short of all the nations of the entire world. The submission of Internet actors to a worldwide range of paper rules may be true, but their submission to effective rules is far more limited.

If the jurisdictional quagmire should thus not be overstated, it should not be underestimated either. The mechanism of protection through the limits of enforcement jurisdiction does not drain the problem of all its substance. A first apparently germane point may be made on the plane of abstraction: to contend that only enforcement jurisdiction matters and that no significance can be ascribed to prescriptive jurisdiction heads, however broad and overlapping the competences they provide for, would deny any *raison d'être* to the limitations by international law of prescriptive

[73] See, e.g., Kohl, *supra* note 53, at 403.

[74] Zittrain, *supra* note 17, at 20: 'the global convoy of Internet publishers operating under respective countries' motley laws would harmonize at those of the most restrictive major jurisdiction – the slowest ship'.

[75] Goldsmith, *supra* note 50, at 198–200.

[76] P. Daillier and A. Pellet, *Droit international public (Nguyen Quoc Dinh)* (6th edn, 1999), at paras 334, 336.

[77] *The SS Lotus, supra* note 68, at 18–19.

[78] Goldsmith, 'Against Cyberanarchy', 65 *U Chicago L Rev* (1998) 1199, at 1216–1222.

[79] J. Story, *Commentaries on the Conflict of Laws, Foreign and Domestic* (1834), at 23.

jurisdiction. A second point, on a more practical plane, can be made about the possibility of having foreign judgments recognized and enforced in the states in which the entity to be regulated has a presence or assets. Admittedly, foreign judgments are typically not recognized and enforced if they stand in contradiction to the public policy of the state in which enforcement is sought. But the contours of public policy are frequently relatively unclear, which creates uncertainty about the possibility of a foreign judgment being imported into a state where it will become effective. In cases where it is clear that the foreign judgment does not violate the public policy of the state where enforcement is sought, the risk that foreign exorbitant assertions of jurisdiction are given effect to is even greater. To follow the approach of the *Yahoo* case would create important indirect extraterritorial effects, by means of extraterritorial enforcement.[80]

Enforcement in a foreign state may not even be necessary: Internet content providers may have assets in countries where they have no intention of sending information, where it would be unpredictable for them to be hauled before a court. An Australian business may, for instance, publish information exclusively destined for Australian territory but have assets in Switzerland for reasons entirely unrelated to the publication activity. The information flow may have effects in Switzerland[81] and the ensuing judgment may be used to induce or compel compliance with Swiss regulations.[82]

Finally, we have to remain alert to the preservation of the 'Westphalian Equilibrium'.[83] This equilibrium, the cohabitation of states, is partly based on international law's requirement that there be a genuine link between the state asserting jurisdiction and the activity that the regulatory scope is meant to encompass.[84] On the Internet, the states' regulatory actions have more global effects than in the normal world; they may more easily interfere with the sovereignty of foreign states. Consequently, in order to preserve 'the systemic value of reciprocal tolerance and goodwill'[85] necessary

[80] Over time one may see the development of new jurisdiction rules in international law for the Internet, by virtue of the emergence of consistent practice of refusal to recognize or enforce foreign judgments, which may amount to a process equivalent to diplomatic protest as a source of customary international law: Hill, 'The Exercise of Jurisdiction in Private International Law', in P. Capps, M. Evans, and S. Konstadinidis (eds), *Asserting Jurisdiction: International and European Legal Perspectives* (2003), at 43. Meanwhile, one may only conclude, with Jonathan Hill, that 'any judgment which ensues from an exorbitant exercise of jurisdiction *should not* be entitled to recognition and enforcement in other countries' (at 56, emphasis is mine).

[81] Or it may be a constituent part of an action there, depending on the view.

[82] Cf. Berman, *supra* note 56, at 409–410.

[83] See Gillroy, *supra* note 38, and *supra* notes 38ff.

[84] See Currie, *supra* note 45, at 298–299 and F.A. Mann, *Further Studies in International Law* (1990), at 12. See also Brownlie, *supra* note 46, at 313, listing the following conditions for an extraterritorial assertion of jurisdiction: 'substantial and bone fide connection between the subject-matter and the source of the jurisdiction', the respect of the 'principle of non-intervention in the domestic or territorial jurisdiction of other states' and the respect of 'accommodation, mutuality, and proportionality'.

[85] *Société Nat'l Industrielle Aérospatiale v United States Dist. Court*, 482 US 522, 555 (1987). Justice Blackmum thereby expressed his conception of judicial comity.

to allow the international legal order to function favourably with regard to the fundamental prerogatives of each state, a more conservative approach than in the normal world needs to be adopted. In this context at least, reciprocity considerations ought to win out over a state's ability to obtain remedies for its citizens. In determining their sphere of jurisdiction, states need to exercise higher moderation and restraint than in the offline world.[86] The genuine link between the state and the activity needs to be taken to a higher threshold, it would seem, on the Internet than elsewhere because in principle all countries have a link to all websites by virtue of their accessibility. Since the effects doctrine is met in the offline world with objections that it does not attain this threshold of a sufficient link,[87] it should *a fortiori* be rejected entirely on the Internet.[88] At the very least, the principle of comity, which one may recall has classically been defined as 'neither a matter of absolute obligation, on the one hand, nor of mere courtesy and good will, upon the other',[89] seems to call for such a non-expansive jurisdictional approach. To play with the words of Anne-Marie Slaughter, who states that comity is the concept substantiating the foundational position that foreign courts are 'co-equals in the global task of judging',[90] one may argue that all states are co-equals in the global task of regulating Internet content and that this position can be sustained only by relying on the principle of comity.

In sum, to follow the approach of the *Yahoo* case seems to lead to problems of unpredictability, due to the uncertainty of extraterritorial enforcement, and a general jeopardizing of the principle of non-intervention, because of the 'slowest ship in the convoy' problem in its moderated guise, taking into consideration the need for enforcement jurisdiction. Seen from the perspective of Internet content providers, the problem is, as mentioned above, that they may be subject to regulations of states to which they had no intention of sending information and to local laws the application of which they could thus not legitimately be expected to foresee.

As effects can more or less voluntarily take place in a large number of jurisdictions, an additional element is increasingly being taken into consideration in the context of Internet jurisdiction. It is the foreseeability criterion, the predictability of being

[86] One may recall here the words of Judge Gerald Fitzmaurice in *Barcelona Traction*: 'every state [has] an obligation to exercise moderation and restraint as to the extent of the jurisdiction assumed by the courts in cases having a foreign element' in order to avoid 'undue encroachment on a jurisdiction more properly appertaining to, or more appropriately exercisable by, another state' in *Barcelona Traction, Light, and Power (Belgium v. Spain)* (Second Phase) [1970] ICJ Rep 3, at 105.

[87] Currie, *supra* note 45, at 300–303.

[88] To those contending that the Yahoo approach was merely an application of the objective territoriality principle one may object that to consider that the accessibility of information is a constituent part of an activity on a given territory leads to an unreasonably broad interpretation of the objective territoriality principle, and that the effects doctrine is precisely such an 'extremely broad interpretation of the objective territorial principle' (*ibid.*, at 301). See further Akehurst, 'Jurisdiction in International Law', 46 *BYIL* (1972–1973) 145, at 155.

[89] *Hilton v. Guyot*, 159 US 113, 163–164 (1895). Alex Mills argues that comity is in this sense a '[m]ixture of international (mandatory) and national (discretionary) elements': Mills, *supra* note 31, at 25.

[90] Slaughter, 'Judicial Globalization', 40 *Va J Int'l L* (2000) 1103, at 1112–1113.

brought before a court in the forum in question.[91] Its most developed instantiation is the principle of targeting,[92] which forms the substance of the next section.

3 Targeting

The conclusion of Lowenfeld's general theory of jurisdiction, developed in his Hague Lectures, was that the principles underlying the overall dynamics of jurisdiction are reasonableness and fairness.[93] These principles shed light on the problems of jurisdiction on the Internet: the main bases of jurisdiction – subjective territoriality and effects or objective territoriality construed broadly – are both unfair and unreasonable.[94] The subjective territoriality principle leads courts to decline to intervene despite the fact that effects are clearly felt locally, while the effects doctrine permits worldwide overlapping prescriptive jurisdictions, and enforcement jurisdiction (and actual enforcement procedures) in states whose identity is not easily predictable. Between too broad and too narrow jurisdictional bases, a better way of 'managing trans-border externalities', 'reinvented parameters of reasonableness', new 'distributive methodologies of jurisdiction implemented in the international order'[95] had to be found.[96] A middle path had to be chosen. This middle path is the principle of targeting.[97]

[91] Kohl, 'The Rule of Law, Jurisdiction and the Internet', 12 *IJL&IT* (2004) 365. On the rationale and origin of this principle see *World-Wide Volkswagen Corp. v. Woodson,* 444 US 286, 298 (1980).

[92] Geist, *supra* note 59, at 1385ff. Whether the concept of targeting does indeed achieve foreseeability is another matter, as we will see below. For the time being, one may point to the likely circularity of the reasoning: courts should use foreseeability as a standard of jurisdiction and what is foreseeable may well be, in substance, the courts' settled practice: Wille, 'Personal Jurisdiction and the Internet – Proposed Limits on State Jurisdiction over Data Communication in Tort Cases', 87 *Kentucky LJ* (1998) 95, at 136.

[93] Lowenfeld, 'International Litigation and the Quest for Reasonableness: General Course on Private International Law', 245 *Hague Lectures* (1994) 9.

[94] Longworth, 'The Possibilities for a Legal Framework for Cyberspace', in T. Fuentes-Camacho (ed.), *The International Dimensions of Cyberspace Law* (2000), at 33–34; Podgor, 'International Computer Fraud: A Paradigm for Limiting National Jurisdiction' 35 *UC Davis Law Review* (2002) 267, at 315–316.

[95] Muir-Watt, 'Aspects économiques du droit international privé', 308 *Hague Lectures* (2004) 219, at 224, 350. Further on the 'reasonableness' of jurisdiction required by the general dynamics of international law see P. de Vareilles-Sommières, *La compétence de l'état en matière de droit privé: droit international public et droit international privé* (1997) and Kaufmann-Kohler, 'Internet: mondialisation de la communication – mondialisation de la résolution des litiges?', in K. Boele-Woelki and C. Kessedjian (eds), *Which Court Decides? Which Law Applies?* (1998), at 93–95.

[96] The details of the evolution of jurisdictional standards for the Internet have been simplified in order to focus on the underlying fundamental principles. Several other jurisdictional standards can be distinguished analytically or can be found in court decisions (for instance the opposition of the 'country of origin' approach and the 'country of destination' approach, which are various instantiations of the jurisdictional categories of international law), but they do not make significant enough difference in practice to be examined here. For a discussion of these other standards see, for instance, Spencer, 'Jurisdiction and the Internet: Returning to Traditional Principles to Analyze Network-Mediated Contacts', *U Illinois L Rev* (2006) 71; Kohl, *supra* note 91; Geist, *supra* note 92, at 1379 and, for a more chronological account of the evolution of the standards, Berman, *supra* note 56, at 512ff.

[97] Zittrain, *supra* note 17, at 19. For a short review of US intellectual property and criminal cases applying the targeting test see Reidenberg, *supra* note 24, at 269–272.

Targeting means in essence that the activity must be intended to have effects within the territory of the state asserting jurisdiction – it is, so to speak, a 'tighter' version of the effects doctrine. To apply the principle of targeting is to 'identify the intentions of the parties and to assess the steps taken to either enter or avoid a particular jurisdiction'.[98] Other wordings of the same principle include 'conduct targeted at a plaintiff whom the defendant knows to be a resident of the forum state',[99] 'direct[ing] activities to that ... State or to several States including that ... State',[100] and taking 'reasonable steps to avoid concluding contracts with [parties] habitually resident in that State'.[101] To put it simply, it is 'something more than effects, but less than physical presence'.[102]

This approach is illustrated by another well-known Internet case: *Gutnick v. Dow Jones*.[103] Joseph Gutnick, a well-known Australian businessman-philanthropist-rabbi-political player, initiated court proceedings against US publisher Dow Jones because of a defamatory portrait of him which appeared in the American magazine *BarronsOnline*. The online magazine, although primarily addressed to American readers, had also sold a fair share of subscriptions to readers located in Australia. These subscriptions, the High Court of Australia concluded, constituted a reasonable and strong enough link between the defendant and this country. The publisher of the magazine intended to have readers in Australia and was aware that its publications would be read and have an impact there. Had Dow Jones refused to sell subscriptions to *BarronsOnline* in Australia, the courts may well have concluded that they did not have jurisdiction over the dispute.

In the *Yahoo* case, the targeting approach would have led to the same outcome, as Yahoo was providing country-specific advertising, serving French Internet users, written in French and related to France. Hence Yahoo knew and even intended to have French visitors.[104] Had the advertising been absent, a targeting approach probably would have led the French courts to deny their right to intervene.

The principle of targeting has appreciable advantages over the standards concretizing the principle of subjective territoriality, or the effects doctrine as it is usually understood. First, it reduces the number of overlapping jurisdictions – it reduces the number of ships in the convoy, to use the image mentioned earlier – as the number

[98] Geist, *supra* note 92, at 1345–1346, 1362.

[99] *Bancroft & Masters, Inc. v. Augusta National Inc.*, 223 F 3d 1082, 1087 (9th Cir. 2000).

[100] Art. 15(1)(c) of Council Reg. 44/2001 of 22 Dec. 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, OJ (2001) L 012/1.

[101] This was version 0.4a of Art. 7 (3)(b) of the Draft Hague Convention. It was never adopted, as the final version of the Convention has been radically stripped down to focus on forum selection clauses.

[102] Zittrain, *supra* note 17, at 19. For further definitions and discussions of the contours of this principle see, for instance, C. Reed, *Internet Law* (2nd edn, 2004), at 227ff; Perritt, 'Economic and Other Barriers to Electronic Commerce', 21 *U Pa J Int'l Econ L* (2000) 563, at 574; *Am. Info. Corp. v. Am. Infometrics, Inc.*, 139 F Supp 2d 696, 700 (D Md 2001), American Bar Association Global Cyberspace Jurisdiction Project, 'A Report on Global Jurisdiction Issues Created by the Internet', 55 *Bus Lawyer* (2000) 1801.

[103] *Gutnick v. Dow Jones & Co. Inc.* [2001] VSC 305.

[104] See French interim order of 20 Nov. 2000. See further Geist, *supra* note 92, at 1406, Reidenberg, *supra* note 24, at 267ff.

of states whose territory is targeted in a specific instance is likely to be lower than the number of states on whose territory effects take place. Secondly, it provides for a more foreseeable standard of jurisdiction, as Internet content providers should be subject to the regulations of states only where they intended to 'send' information which they can legitimately be expected to respect.[105] Thirdly, it would constitute a more reasonable and fair head of jurisdiction because targeting sets higher the threshold of what constitutes a genuine or sufficient link between an activity and a state's territory. Fourthly, compared to a strict application of the principle of subjective territoriality, it makes shopping for lenient legal regimes more difficult as Internet content providers cannot simply move to more friendly jurisdictions while still targeting the same territory with the same information.

If the approach of targeting appears to be instrumentally valuable for resolving individual cases, it still has some important failings with regard to such fundamental goals as the protection of local values and the avoidance of unforeseeable extraterritorial effects of regulations, as should be apparent from the following arguments.

Counter-intuitively, it may first be said that the definition of targeting as 'something more than effects, but less than physical presence'[106] is the most (descriptively) accurate one, despite its being the vaguest wording of the concept. The problem with targeting is that the concept does not have an inherently precise meaning. Whereas the reasonable scope of interpretation of the notions of subjective territoriality (where the activity originated) and effects is relatively straightforward to determine, what it means to target seems to be very much up for grabs. The semantics of targeting no doubt allow one to conclude that '[b]y choosing to use the Internet the wrongdoer is deemed to be aware of its global reach, and just as he receives the benefits of wider circulation of his content, he is exposed to a corresponding risk by making content accessible on the Internet'.[107] This may mean that an Internet content provider is deemed to target all the world's countries save those with which it effectively prevented all contacts. A lower degree of jurisdictional avoidance may alternatively be required – for instance declarations by users and some form of filtering. Then again, positive actions to direct activities towards specific states may also constitute the threshold of what amounts to targeting. Is the language or the currency used on a website a necessary or even a sufficient condition to enter or to avoid a jurisdiction? Do clauses in terms and conditions matter, and in which language must they be drafted to be given effect? Must a commercial Internet content provider filter according to the place of issue of the credit card being used or otherwise be deemed to target the entire world? The words of Humpty Dumpty echo: targeting simply appears to be a concept which may very well mean whatever a government chooses it to mean, neither more nor less.

It is not only the problem of jurisdictional foreseeability that the targeting approach does not resolve satisfactorily. Local values and public policy choices are also left under-protected, as information violating such values or public policy choices in

[105] Geist, *supra* note 92, at 1404.
[106] See *supra* note 102.
[107] Bigos, *supra* note 53, at 619.

principle still flows into the territory of a given state, even if the territory of that state was not targeted.

C *Filtering Strategies*

1 At the Sender's End

The problems surrounding the remaining issues with the targeting approach should not be exaggerated. If targeting goes some way towards reducing jurisdictional ambiguities and their problematic overlapping, as well as attributing a less ineffective jurisdictional basis to states seeking to react to a violation of the fundamental values they are to protect, another technique may help fill in the rest of the solution. We should not be startled to find that this complement is technological in nature and that its function is, in a sense, to impose limits on the global character of the Internet. This technique is filtering at the sender's end or at the source. It has latterly developed quite substantially, in the wake of the shift of focus that the *Yahoo* case inaugurated.

This shift of focus was inaugurated when the French judge in the *Yahoo* case requested an advisory opinion from renowned experts of Internet technologies regarding the feasibility of Yahoo filtering out French Internet users, to prevent them from accessing the Nazi memorabilia. The experts' verdict was without appeal. It was all the more convincing as it seems to have imposed itself against their global ideology: two of the experts were outspokenly against the introduction of technologies which would diminish the global character of the Internet.[108] Nevertheless, their conclusion was that geolocalization technologies were readily available and that they could already achieve an accuracy of possibly up to 90 per cent.[109] Yahoo, in other words, was capable of filtering to whom it intended to send information. This is not dissimilar to how it managed to provide French advertising to French visitors, as was mentioned above.[110] At this point, the focus started to shift from taking advantage of the Internet's global character to exploiting the localizable nature of information travelling through it.[111] Both the offer of and demand for geolocalization technologies surged, bringing further technological refinement and thus accuracy in filtering.[112]

This appears to have two sorts of effects. First, Internet content providers seeking effectively to reduce the risk of being taken before courts and of being subjected to

[108] On the subsequent repudiation of the judgment by two of the experts see Zittrain, *supra* note 17, at 26.

[109] See the Opinion of the Consultants Ben Laurie, François Wallon, and Vinton Cerf referred to in the interim court order of 22 Nov. 2000. See also Reidenberg, *supra* note 24, at 268. Of course, the more interesting the material is for the user, the greater will be the incentives she has to circumvent such geolocalization technologies, causing their accuracy and efficacy to diminish. So argues van Houweling, 'Enforcement of Foreign Judgments, the First Amendment, and Internet Speech: Notes for the Next Yahoo! v. LICRA', 24 *Michigan J Int'l L* (2003) 697. But it is difficult to imagine that these technologies will not be improved over the years, which will be likely to leave the possibility of circumvention open only to high-profile Internet users, who represent a quantitatively insignificant portion of the population.

[110] On all this see Goldsmith and Wu, *supra* note 7, at 7–10, 58–63.

[111] The simplest way to experience the workings of geolocalization technologies is to use Google and to watch out for the *local* advertisements appearing in the right-hand sponsored links.

[112] On filtering technologies see H.S. Spang-Hanssen, *Cyberspace & International Law on Jurisdiction: Possibilities of Dividing Cyberspace into Jurisdictions with Help of Filters and Firewall Software* (2004), at 7–190.

enforcement proceedings where they have a presence or assets, will resort to filtering technologies to obtain better control over the direction of their information flows. They have strong incentives to replace their attempts at legal filtering – targeting specific jurisdictions or avoiding the jurisdiction of certain countries by means of, for instance, terms and conditions or general statements on their websites – by much more effective procedures of technical filtering. Secondly, as filtering at the source increases, the concept of targeting is likely to evolve and crystallize into the assumption that all countries of the world are targeted except those which are technically excluded.[113] At this stage of the analysis it seems legitimate to maintain that, by choosing to use the Internet to the full extent of its global reach without narrowing down the geographical scope of the information flow produced, an Internet content provider should be deemed to seek the benefits of this global reach, and thus legitimately be exposed to the risks associated with it. The same rationale of legitimacy also applies to any other scale to which the global reach of the Internet is used: seeking the benefit of reaching *X* countries legitimately subjects the provider to the risks associated with the regulation of those *X* countries, since *X* can be determined by the provider.

Surely, filtering at the sender's end should then be welcome? Its benefits, after all, appear overwhelming. Yet two factors may prevent the stabilization of the uncertain grounds of Internet jurisdiction in the manner exposed above. The first factor is an issue of efficacy: the combination of targeting and filtering at the source will allow the exertion of efficacious control only over elephants. Mice will still escape. I mean this in the sense of the distinction Peter Swire draws in his essays titled 'Of Mice and Elephants'.[114] Elephants are, as the name suggests, large entities, typically sizeable companies or other organizations which are clearly identifiable and often have presence and assets in several countries. Just like the mammal, they are easy targets and can escape an applicable regulation only with the greatest difficulty, through complicated and often costly legal battles. Mice are petite and quick, small companies or individuals quickly opening a website to carry hate speech, child pornography, an online casino, libel, copyright violations, and the like. They are typically difficult to identify and to localize. As Peter Swire concludes, '[w]here harm over the Internet is caused by mice, hidden in crannies in the network, traditional legal enforcement is more difficult'.[115] Mice typically will not implement filtering technologies. To assert jurisdiction over them – whatever the basis of jurisdiction – typically will not suffice to shut them down. What is to be done?

The second factor is more ideological. Provided the targeting test does evolve so as to entail a condition of jurisdictional avoidance by filtering (in order to be deemed not to have targeted a given territory), Internet content providers other than those of the mouse breed will have an incentive to choose an opt-in approach rather than an

[113] Cf. Muir-Watt, supra note 56, at 687, Reidenberg, *supra* note 24, at 276.

[114] Swire, 'Of Elephants, Mice, and Privacy: International Choice of Law and the Internet', 32 *Int'l L* (1998) 991; Swire, 'Elephants and Mice Revisited: Law and Choice of Law on the Internet', 153 *U Pa L Rev* (2005) 1975, at 1979.

[115] *Ibid.*

opt-out one. I mean this in the sense that they are likely to distribute their information only to those countries in which they have real interests and for which they are consequently willing to carry out an analysis of the legal risks. Instead of filtering out potentially problematic countries, they are likely to filter in only those areas they do specifically target. It may be true that it is 'prohibitively expensive for a small business or individual to filter out users from selected jurisdictions', as certain authors submit,[116] but the reverse appears to be false. Conditioning access to information on positive identification (filtering *in*) of the user's IP address, which provides reasonably accurate geographic localization, is a matter of five minutes of HTML programming and costs virtually nothing. This would perfectly fulfil the goals of the targeting principle. But it would also lead incidentally to an impoverishment of the Internet, as the amount of information accessible from at least the less 'important' countries – those for which the pay-off of a legal-risk analysis is smaller – would diminish. Particularly critical, subversive, or generally non-agreeable information is likely to be the first victim. And such contentious information is an important factor of innovation in general and of the Internet's revolutionary capacity in particular.[117] Again, what is to be done?

One solution which seems to respond to both these concerns – mice undermining local values and the filtering to narrow geographical bands which diminishes the Internet's informational wealth – is filtering at the receiver's end or at the destination.[118] It is more likely to catch mice and seemingly less likely to impoverish the Internet of unorthodox information, at least within non-repressive regimes. This will lead to an even stronger carving up of the Internet. A discussion of how this might work forms the substance of the next section.

2 At the Receiver's End

In starting to look at the ways in which filtering at the receiving end may contribute to the carving up of the Internet, I must begin with two distinctions not directly generated by the subject-matter of the analysis. The first distinction pertains to law's normativity, the second to law's functions.

With regard to law's normativity – the modalities of how it directs behaviour – the distinction I wish to draw relates more precisely to two ways in which the law may create prudential reasons for compliance.[119] Prudential reasons for compliance with the law may in essence be created by two means (this is the first distinction I

[116] E.g., Berman, *supra* note 56, at 409.

[117] On targeting and filtering at the sender diminishing available information see Zittrain, *supra* note 17, at 26–27, 30–31 and van Houweling, *supra* note 109, at 714–715.

[118] Similarly, Kwon, 'Filtering the Smoke out of Cigarette Websites: A Technological Solution to Enforcing Judgments Against Offshore Websites', 30 *Brooklyn J Int'l L* (2005) 1067, at 1093–1094 and Fagin, 'Regulating Speech Across Borders: Technology vs. Values', 9 *Mich Telecomm Tech L Rev* (2003) 395, at 451–452.

[119] Prudential reasons for action are typically opposed to moral reasons for action, in that the former, and not the latter, rely on objective interests, on objective gains and losses associated with different courses of action: see, for instance, M.H. Kramer, *In Defense of Legal Positivism: Law Without Trimmings* (1999), at 81–83 and J. Raz, *Practical Reason and Norms* (1999), at 155–156.

promised): threats of an *ex post* sanction and imminent obstacles.[120] Sanctions operate by depriving someone of advantages normally due on the ground that he or she has violated a norm.[121] Obstacles operate by modifying the feasibility of certain actions: if an action becomes more difficult or altogether impossible to perform, then a person has strong prudential reasons not to expend resources on efforts to perform it, and is thus expected to refrain from acting.[122] Obstacles, to be effective, do not have to be impossible to circumvent. They need only to make an action substantially more difficult to perform, thereby 'altering the prices one has to pay for the performance of actions'.[123]

With respect to law's function, the distinction I wish to introduce opposes the orientation of behaviour to the production of a cathartic or symbolic effect. The function of orienting behaviour is relatively conspicuous, and it was assumed in the distinction just sketched between sanctions and obstacles. The cathartic or symbolic function of law, by contrast, operates chiefly by means of the approval or disapproval of an action bestowed by judgments.[124] It is law taking an official position through the courts' actions on the acceptability of a given behaviour under the nation's legal norms which, in principle, reflects its social norms and expresses its fundamental cultural values.[125] Brutally simplified, it is one of law's functions to say what, according to the law governing and tying together a nation, is right or wrong, without necessarily punishing as a consequence. This, sometimes more than the sanctions *qua* retribution, is a central goal of certain profoundly symbolic judicial actions, such as international criminal proceedings ensuring that war criminals do not go down in history as heroes.[126] In international proceedings generally, states often ask for a declaration of the wrongfulness of conduct, in order to obtain 'satisfaction', as opposed to compensation and restitution.[127] Catharsis is also the central idea behind the practice, followed in certain countries, of court decisions allocating symbolic monetary awards of extremely low amounts.

Let us now probe the possible consequences that these distinctions may have for jurisdiction on the Internet. If law can prevent behaviour by either threatening with sanctions or by making the relevant actions difficult enough, then a state may

[120] A similar distinction is drawn by Lessig, 'The New Chicago School', 27 *J Legal Stud* (1998) 661.

[121] E.g., Rawls, 'Two Concepts of Rules', 64 *Philosophical Review* (1955) 3, at 10.

[122] The most typical example of such an obstacle is a speed bump.

[123] Rawls, *supra* note 121, at 12. See also, for the same idea applied to the Internet, Goldsmith and Sykes, 'The Internet and the Dormant Commerce Clause', 110 *Yale LJ* (2001) 785, at 812.

[124] A. Garapon, *Bien juger. Essai sur le rituel judiciaire* (1997), at 220–221, 249.

[125] See also Berman, *supra* note 56, at 517.

[126] See, e.g., Chesterman, 'Never Again ... and Again: Law, Order, and the Gender of War Crimes in Bosnia and Beyond', 22 *Yale J Int'l L* (1997) 299, at 311–317; Binder, 'Representing Nazism: Advocacy and Identity of Klaus Barbie', 98 *Yale LJ* (1989) 1321.

[127] See, e.g., Arts 36 and 37 of the International Law Commission's Articles on responsibility of States for internationally wrongful acts. See further the *Rainbow Warrior (New Zealand/France)*, RIAA, vol. XX, 217 (1990), at 272–273, para. 122, where the arbitral tribunal held that the public condemnation of the conduct of France amounted to appropriate satisfaction, and *Corfu Channel*, Merits [1949] ICJ Rep 4, at 35.

consider its jurisdictional reach not in terms of which entities it should sanction through the application of its regulation – which has been the approach adopted so far. It may instead consider the jurisdictional basis of its regulation in terms of trammels imposed on extraterritorial activities. Similarly, if we accept the idea that law does not necessarily need to punish the authors of invidious or pernicious behaviour, but may simply declare such behaviour unwanted and then exert some action to bring reality into line with the values so expressed, then we may again see that sanctioning foreign actors is not necessarily the only avenue to follow.

In light of the foregoing, one might consider treating differently cases involving a targeting practice and those for which the only jurisdictional basis would be the effects doctrine. To divorce blocking from sanctions appears to be the most fertile 'reinvented parameter of reasonableness'.[128] Courts might apply a narrowly construed targeting test to foreign activities and, if the territory of the forum state were found to be targeted, they might simply apply local regulations as usual and seek to sanction the foreign actor through enforcement procedures where the actor has a presence or assets. The narrow construal of targeting would seek to diminish as much as possible the informational impoverishment of the Internet by risk-averse content providers over-limiting the geographical bands into which they send information. Cases where undesirable effects are felt locally but the foreign actor is not to be deemed to have targeted the territory of the forum state might conversely be handled with greater jurisdictional latitude. Confronted with such cases, the forum state would in this scheme assert jurisdiction, relying on the effects doctrine, but the court seised of the case would render only a declaratory judgment and refrain from awarding damages or imposing fines. Such a judgment would seek the attainment of two ends: catharsis and blocking incoming information traffic. How these ends might be reached is what I will try to expound in the following paragraphs.

The idea with catharsis is that a dispute, especially one which involves strong emotions, as is generally the case with cases involving public policy considerations, disrupts the link between an individual and her community. Judging a case is a way to rebuild this link. It is, as was briefly sketched above, a process through which a community expresses what is acceptable within the community and what is not; it is an expression of the estimableness of an action with regard to the values of the community. It is a way of saying that the shock felt by the people in France who accessed the Nazi memorabilia on the Yahoo website was legitimate. Judging is meant to have a declaratory effect of re-expressing and re-affirming the norms by which the community lives. Without a doubt, it was important for the citizens of France – as well as for other nations sharing similar values in this regard – that the Paris court made the French legal system say that the accessibility of Nazi memorabilia in France was simply not admissible. The law's addressees were comforted in their belief that the availability of such information was intolerable, regardless of whether the French territory was targeted or not.

[128] Muir-Watt, *supra* note 95, at 224. See also *supra* note 95 and accompanying text.

A manifestation of this rationale found its way into the Canadian *Citron v. Zündel* case.[129] Ernst Zündel, a resident of the United States, was posting anti-Semitic material on his American website, which was accessible from Canada, a country where such material is incompatible with human rights legislation. The Canadian Human Rights Commission in this case acknowledged that an 'order issued against the Respondent would have virtually no effect in eliminating this material from the World Wide Web'.[130] Nevertheless, to issue a cease and desist order, the Commission went on, would serve a

> significant symbolic value in the public denunciation of the actions that are the subject of this complaint. Similarly, there is the potential educative and ultimately larger preventative benefit that can be achieved by open discussion of the principles enunciated in this or any Tribunal decision.[131]

Let us now probe the idea of blocking traffic. Such a judgment based on the effects doctrine might be used not to sanction the foreign actor, but as a legal basis to block incoming Internet traffic originating from the website the contents of which have been declared to be unlawful and unwanted in the forum state. The following sketches, very briefly, how this might work.

Internet service providers (ISPs) have three roles.[132] The first one is to host information, essentially website contents, on their server and to make it available to the rest of the world. Such ISPs may be called sending ISPs. They can, of course, refuse to host certain contents and sometimes display quite restrictive policies in this respect. But the hosting policy of an ISP depends on the laws and values of the state in which it is located. Imposing hosting rules on an ISP with servers located within the territory of another state would amount to an encroachment on the territory and an infringement of the sovereignty of that other state. Trying to control website contents at the sending or source ISP raises jurisdictional problems, and enforcement issues as well.

The second role of ISPs is simply to pass information on. From the sender, through the Internet cloud represented earlier in this article, the information reaches the receiver after having travelled over the servers of sundry ISPs. The path the information will take is, as was mentioned earlier, unpredictable. As the path cannot be foreseen, controlling contents transmission there does not appear possible, and it would also raise jurisdiction issues because some of these passing ISPs are likely not to be located in the forum state.

The third role of ISPs is to deliver information directly to the user. One might label them receiving ISPs. They represent the locus at which regulatory intervention is most likely to strike. The idea is to block undesirable incoming Internet traffic as it travels through their servers. We will see in the following that they represent the most appealing junctures for control.[133]

[129] *Citron v. Zündel* [2002] CHRD No 1 (CHRT).
[130] *Ibid.*, at para. 295.
[131] *Ibid.*, at para. 300.
[132] See Zittrain, *supra* note 17.
[133] *Ibid.*, at 672 ff.

One of the main advantages is that receiving ISPs are in principle located within the same territory as the end-user, and therefore on the territory of the state seeking to regulate. Their regulation does not pose problems of extraterritoriality, not strictly speaking at least.[134] Filtering information that originated abroad certainly has extraterritoriality effects, as it influences and regulates the foreign actors' activities, typically increasing their costs of providing information into this territory. But these are 'extraterritorial spillover effects' of national regulations, as Jack Goldsmith argues. And they are 'both inevitable and legitimate', and actually also very common.[135] In the language of the distinctions drawn above, indirect extraterritoriality caused by obstacles is less objectionable than direct extraterritoriality involving sanctions. From a jurisdictional perspective, it is doubtless less objectionable for state *X* to make it impossible for residents of state *Y* to send certain information into the territory of state *X* than to impose economic penalties for the residents of state *Y* trying to send information into state *X*.[136] As Jonathan Zittrain writes, '[i]mposing control on destination ISPs has been the approach of governments that wish to control the flow of content over the Internet but who cannot project that control beyond their boundaries'.[137] This applies not only to governments that *cannot* project their regulatory actions beyond their boundaries but also those that *do not wish* to project such actions onto the territories of other states, seeking to avoid or limit the extraterritorial effects of their laws.[138] In addition, and as is implied in Zittrain's position just mentioned, the other advantage of receiving ISPs being located on the territory of the regulating state is that this allows the resort to local enforcement procedures against the assets of the ISPs. The state being thereby able to rely on one of its most usual control levers, the compliance of these entities should not pose particular problems of the type that could be posed by foreign actors.

Another advantage of this approach is that it would be more effective against small and disruptive actors which do not fear traditional legal enforcement

[134] Fagin, *supra* note 118, at 402–403; Kwon, *supra* note 118, at 1100.

[135] See Goldsmith, *supra* note 50, at 200–201.

[136] This is notwithstanding international obligations following for instance from trade agreements guaranteeing market access, which typically prohibit discrimination between foreign and domestic service suppliers, limited by public morals and public order protection clauses and possibly rules of customary international law. On Antigua and Barbuda's ultimately failed attempt to invoke WTO law to have US regulations prohibiting offshore online gambling declared 'an illegal barrier to trade in services', where the WTO appellate body ruled that the regulations in question were 'necessary to protect public morals or to maintain public order' (Art. XIV GATS), see *United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, Report of the Appellate Body, AB-2005-1, WT/DS285/AB/R (20 Apr. 2005), note Trachtman, 16 *EJIL* (2005), available at: www.ejil.org/journal/curdevs/sr47.rtf. For an analysis of this case see Wunsch-Vincent, 'The Internet, Cross-border Trade in Services, and the GATS: Lessons from *US-Gambling*', 5 *World Trade Review* (2006) 319.

[137] Zittrain, *supra* note 17, at 673 (emphasis is mine). Similarly Frydman and Rorive, 'Regulating Internet Content through Intermediaries in Europe and the USA', 23 *Zeitschrift für Rechtssoziologie* (2002) 23, at 44.

[138] In this sense, this solution seems to meet Yochai Benkler's call for state cooperation in the interdependent digitally networked world where unilateral regulatory efforts have much stronger mutual implications than in the offline world: Benkler, 'Internet Regulation: A Case Study in the Problem of Unilateralism', 11 *EJIL* (2000) 171.

processes – 'mice', in the words of the discussion above. Traditional legal enforcement regarding foreign actors may well be both inefficacious and inefficient against small and elusive actors whose real identity is difficult to establish, but technological enforcement should not be or at least much less so. The marginal costs of blocking one more mouse, or of updating the blocking of an actor who has closed her window to the Internet and opened another one elsewhere can be expected to be far lower than those generated by one more international court procedure. The complications following from lifting the technological veil in order to identify the actor behind an information flow can also be dispensed with: all that matters is to identify the technological source or characteristics of the information flow in question. The cost and efficacy of such identification will necessarily decrease with further technological development. In sum, it will often be more effective and efficient to identify and block certain information flows than to prosecute their authors, in particular if they are of murine quality and are located outside the territory of the state asserting jurisdiction.

The revolutionary capacity or information wealth of the Internet is likely to be less damaged by recourse to filtering at the receiver's end compared with filtering at the sender's end. Compare the scenario where all countries allow the circulation of all information but the information that undermines local values with the scenario where a significant proportion of Internet content providers allow their information to be accessed only from those countries where they really wish the information to go. Admittedly, many variables of this equation remain undefined, e.g., what is the ratio of information deemed to 'undermine local values', what is the proportion of content providers implementing filtering technologies, and how many countries will they seek to target on average. But assuming, as seems reasonable, that the first and third variables are low and the second high, scenario 2 appears to be quantitatively less restrictive. Then again, an important caveat should be entered: the situation in repressive regimes is likely to be worse in scenario 2; they are, however, likely in any event to adopt such filtering practices.

This regulatory approach based on filtering of information flows by receiving ISPs has largely been neglected because of the technological complexity of such filtering. Yet certain regimes, more enthusiastic about control than the average, have lately contributed significantly to the development of more effective systems and are already using nation-wide filtering processes. These technological developments constitute readily available tools for implementing filtering practices more in conformity with Western liberal democratic ideals, and accordingly seem likely to be used. One may argue that such systems are far from perfect, and it is highly probable that some unwanted information will always continue to sift through, but such a contention would amount to forgetting that perfection is not a necessary element of regulation. In Pennsylvania, for instance, such a system has been used to keep out child pornography – but it was struck down as unconstitutional, mainly because of the too numerous false positive results (i.e., overblocking) produced by the filtering technology being used.[139] In the United Kingdom, the Home Office is gradually introducing

[139] *Center for Democracy & Tech. v. Pappert,* 337 F Supp 2d 606, 655 (ED Pa 2004), striking down Pennsylvania 18 Pa.Const.Stat., paras 7621–7630 (2003).

an obligation for all ISPs to implement a content blocking system to filter out child pornography identified as such by the British Internet Watch Foundation, irrespective of the information's geographic source.[140] In France, the *loi pour la confiance dans l'économie numérique*[141] provides that a judicial authority can request French receiving ISPs to block access to websites hosted abroad if the same could not be obtained from the foreign sending ISPs. This provision, for instance, has been used by French courts to prevent access from the territory of France to a negationist website hosted in the United States.[142]

Just as in the Pennsylvanian system, where ISPs had to block access to sources of information only if specifically instructed to do so by the state attorney general,[143] the scheme under consideration here would not imply any affirmative obligation for the ISPs to monitor the information which flows through their servers and proactively to report problematic material. Their role would be limited to enforcing the filters that legal authorities have determined and thereby to prevent access to the offending source of information.[144]

This controllability of information flows seems to be contingently reinforced by the fact that ISPs currently appear to operate in a highly concentrated market, a small number of ISPs delivering information to a vast majority of users.[145] Filtering consequently would appear to be sufficient if administered at a relatively low number of junctures.

Such a scheme necessarily conjures up some typical criticism. It would seem troublesome that the decision to block access to certain sources of information depends uniquely on the unilateral decision of a state attorney general or on another *ex parte* procedure before an equivalent authority – which was a further ground on which the Pennsylvania statute was struck down.[146] A third-party determination would be less contentious if it involved adversarial proceedings open to the defendant whose information was about to be blocked. But can one really ask for a judicial decision from such a system for every case of information access blocking? The answer would clearly seem to be in the negative. Courts are not typically overstaffed and lacking work, and court decisions do not typically come about very quickly. But the intervention of courts, as opposed to other dispute resolvers, may not be necessary in every

[140] HC Debs, Written Answers for 15 May 2006, col 708W, Home Office Minister Vernon Coaker, available at: www.publications.parliament.uk/pa/cm/cmhansrd.htm.

[141] Art. 6-1.8 of loi no 2004-575 of 21 June 2004, JORF no 143 of 22 June 2008, consolidated version of 5 Jan. 2008.

[142] Paris CA, 14th chamber, 24 Nov. 2006, *Tiscali Acces et autres v. Free, Uejf et autres* and Trib. de grande inst. Paris, Ordonnance de référé, 13 June 2005, *UEJF et autres v. Free, AOL et autres.*

[143] See Zittrain, *supra* note 17, at 674ff.

[144] Their role would thus be that of mere instrumentalities of state power. They should thus not be considered publishers with a certain liability for the information they pass along – their liability should be limited to enforcing the specifically targeted filtering order they receive – because otherwise they would be likely to overblock information so as to avoid any financial risk, as put forward by Frydman and Rorive, *supra* note 137, at 44–45, 54–57.

[145] Zittrain, *supra* note 17, at 673.

[146] *Center for Democracy & Tech. v. Pappert, supra* note 139, at 656ff, 660ff.

case. The need for catharsis, as discussed, does not call for a full-blown court decision, or even a court decision *tout court*, in every case. Instead one may imagine the following scheme: submit such blocking cases to private online dispute resolution institutions, able to give decisions within very short periods and at very lost cost,[147] and maintain recourse to courts to *a certiorari* review – for cases which have an important symbolic or legal impact.

In sum, the advantages of such an approach are important: it seems to be the most efficacious system, its duality (targeting on the one hand and the effects doctrine on the other, the latter seeking to achieve catharsis and blocking certain contents) provides what is likely to be the best solution to the problem of jurisdictional bases, being either too broad or too narrow. It appears to impoverish the Internet less than the likely reactions of Internet content providers to a wide-scale practice of the targeting test. Its disadvantages – mainly that further technological development is needed – are likely to be solved, given some time.

It seems more than plausible that such a form of carving up of the Internet will be followed.[148] This is especially so in an era where, on the one hand, recent international events create strong incentives for a crackdown on sources of potentially problematic information and, on the other hand, globalization frequently reactively triggers increased community expectation and pressure to protect local values.[149]

This constitutes the first form of Internet segmentation announced above, a segmentation which might be viewed as juxtaposed billiard balls of state law. But this is just one likely evolution of the Internet, covering only certain types of behaviour, to the exclusion, for instance, of what might be considered culture-neutral commercial relationships. How these and other relationships are driving another aspect of the evolution of the Internet is what will form the substance of the next main section.

4 The Layers Evolution

I now turn to Internet balkanization in another guise, which appears to take place in parallel with the phenomenon explored thus far. The evolution now to be introduced relates to the forming of separate legal spheres on the Internet, delimited not according to territories but with respect to different aspects of the exercise of human agency. Certain distinct types of activities, or 'slices of life', are regulated by distinct legal systems. Such legal systems are quite atypical. First, they are non-territorial. Instead they are transnational and formed not by the virtual communities that are nation-states but

[147] On online dispute resolution see, for instance, G. Kaufmann-Kohler and T. Schultz, *Online Dispute Resolution: Challenges for Contemporary Justice* (2004). On making dispute resolution more efficient through information technology, see further T. Schultz, *Information Technology and Arbitration* (2006).

[148] Similarly, Reidenberg, *supra* note 13, at 223, 229–230.

[149] See, e.g., Giddens, 'The Globalization of Modernity', in D. Held and A. McGrew (eds), *The Global Transformations Reader* (2000), at 61; Franck, 'Clan and Superclan: Loyalty, Identity and Community in Law and Practice', 90 *AJIL* (1996) 359, at 374. On the link between community expectation and jurisdiction assertions, typical of McDougal and the 'policy' or 'New Haven' approach to international law see M.S. McDougal, H.D. Lasswell, and I.A. Vlasic, *Law and Public Order in Space* (1963), at 95.

by communities of choice clustering around shared interests. Secondly, they are non-comprehensive, in the sense that they do not claim to rule over 'virtually all aspects of social and individual life in a given region',[150] which in principle is a fundamental, albeit unnecessary, characteristic of a legal system.[151] A third unusual feature may be ascribed to the developing systems examined here: they are devoid of the public policy considerations that typically partake of each system's foundational precepts and vary from one public legal system to another. As a consequence of the transnational characteristic just mentioned, the systems exposed here transcribe into legal rules only values that are of general or possibly even universal acceptability, not unlike the substantive contents of the concept of 'transnational public policy'.[152] Because of the aforementioned characteristics, I have called such systems 'layers', as this metaphor illustrates the dissimilarities with the 'billiard balls' of national public legal orders.

The development of legal systems of this kind heralds a transformation of cyberspace differing in a number of respects from the carving up introduced in the previous section. As may be inferred from my exposition just sketched, such dissimilarities relate to the geometry and content of the resulting legal spheres, the identity of the underlying community, and the values such systems enforce by virtue of their regulatory sway. In addition, and more importantly to understand the phenomenon depicted here, the causes of the 'carving up' differ. The following will give an account of these reasons and in the process revert to some of the characteristics of the resulting legal systems. In order to demonstrate that the developments portrayed do not rely on some elusively utopian archetype of a transnational non-comprehensive non-state legal system,[153] the balance of this section will then discuss a particular instance thereof, using eBay as an example.

A *Private Commercial Legal Systems on the Internet*

This evolution in layers, as it is envisaged here without any claim to exhaustiveness, is not caused by a quest for the protection of local values and public policies but by a response to commercial needs, or more precisely by the market responding to economic incentives. As Pierre Lalive wrote, long before the popular use of the Internet, 'it is an obvious fact that is never sufficiently recalled: individuals who are parties to an international relationship or seek to enter into one have a need for security which is all the greater for their awareness to venture into the unknown, leaving their own legal system'.[154] Security, here, is meant as a response to the legal needs of predictability and the possibility of obtaining an effective remedy, which is foundational for

[150] Kramer, *supra* note 119, at 97.

[151] See, e.g., L. Fuller, *The Morality of Law* (rev. edn, 1969), at 124 and A. Marmor, *Positive Law & Objective Values* (2001), at 40.

[152] Lalive, 'Transnational (or Truly International) Public Policy and International Arbitration', in P. Sanders (ed.), *Comparative Arbitration Practice and Public Policy in Arbitration* (1987) 276.

[153] This a flaw that marked many of the early evocations of the emergence of private legal systems on the Internet, depending on how high one sets the threshold of juridicity.

[154] Lalive, 'Tendances et méthodes en droit international privé: cours général', 155 *Hague Lectures* (1977) 69.

all human agencies aspiring to commercial benefit.[155] Seen from this perspective, this second form of carving up of the Internet is a consequence of the economic inaccessibility of courts and judicial enforcement proceedings for low-value disputes. Courts are particularly inaccessible for small disputes involving large geographic distances between the parties, for reasons including travel costs and general legal fees. A factor not uncommon on the Internet which further aggravates this issue is the cross-border nature of a transaction; this causes additional economic barriers due to the need to co-ordinate legal action in several legal systems, and possibly to translate documents.[156] Some countries have introduced low-cost court proceedings, typically in the form of small-claims courts, but this solves only one part of the problem: a judgment, once obtained, must be easily enforceable to constitute an effective threat, one likely to induce compliance. International enforcement procedures, involving the need to have a decision recognized abroad, raise cost issues that bear many affinities to the obstacles constituted by ordinary court actions.

Some marketplaces, recognizing this demand, have addressed the problem by introducing both low-cost online dispute resolution mechanisms and private enforcement systems. The former essentially are systems of computer-assisted negotiation, online mediation, and online arbitration – in other words, procedures conducted through computers over the Internet. Such systems usually are tailored specifically to address low-cost disputes involving distant parties, a task structurally facilitated by the absence of travel costs. Private enforcement systems (or self-enforcement systems) rely on the private control of resources which are valuable to the parties – typically money or reputation. They may take one of the following forms, or a combination thereof: trustmarks and other reputation management systems, 'naming and shaming' reports, exclusions from marketplaces, payments for delay in performance, escrow systems, judgment funds, transaction insurance mechanisms, or credit card charge backs. Low-cost online dispute resolution mechanisms ensure that the access to a remedy is effective, while self-enforcement mechanisms ensure that the remedy itself is effective.[157] In addition, the regulatory framework usually governing the type of disputes considered here is frequently such that it denies many parties an effective appraisal of the legal consequences attached to a number of behaviours relating to their commercial endeavour. Online shoppers are not typically well versed in conflict of laws and the study of the authoritative formulations of foreign laws, nor can they reasonably seek legal advice for such small transactions. This lack of effective user ascertainability undermines the functionality of the traditional legal framework in guiding and steering commercial conduct, since such endeavours entail predictability. In order to avoid this problem, and again to respond to the market demand

[155] Teubner, 'Zur Eigenständigkeit des Rechts in der Weltgesellschaft: Eine Problemskizze', in R.J. Schweizer, H. Burkert, and U. Gasser (eds), *Festschrift für Jean-Nicolas Druey* (2002), at 148.

[156] See H. von Freyhold, V. Gessner, E.L. Vial, and H. Wagner, *The Cost of Judicial Barriers for Consumer in the Single Market* (1996) and B. Feldtmann, H. von Freyhold, and E. Vial, *The Cost of Legal Obstacles to the Disadvantage of the Consumers in the Single Market* (1998).

[157] T. Schultz, *Réguler le commerce électronique par la résolution des litiges en ligne : une approche critique* (2005), at 470–504.

of easily ascertainable and predictable legal frameworks, certain marketplaces have developed highly detailed user policies used in the dispute resolution process as the applicable 'law', to the exclusion of many of the normally applicable national laws, including their mandatory non-derogable rights.

Such constructions cause their normative environments to be largely divorced from public legal systems: a private dispute resolution mechanism applies privately developed norms and the outcome of the procedure is enforced through private means. Such constructions create marketplace-specific legal systems. From an external and global point of view, these systems form a patchwork of private legal orders each specific to an online marketplace or to an equivalent context of Internet activities. They form 'layers' as they can pile up so as to be several which apply to the same individual, governing different facets of her life.

B *Ubi Societas, Ibi Regula*

As should already be evident from the discussion thus far, the layers evolution also differs from the billiard balls developments with regard to the communities underlying these movements. In a landmark article on jurisdiction and the Internet, Paul Berman argues that all current approaches to jurisdiction fail to tackle the foundational misconception, namely 'the assumption that the nation-state is the only appropriate community for jurisdictional purposes'.[158] Surely, it seems unlikely that private international law, devised and handled by officials of public legal systems, will come to grant the normative spheres of non-state communities a standing equivalent to national laws, and in so doing recognize them as legal systems as designated by rules of conflict of laws. The ideology underlying classical legal positivism and state voluntarism – that only state law sufficiently guarantees democratic legitimacy to deserve to be called law – is too strongly rooted in our legal cultures for private international law to take such a path.[159] It is vastly more likely that non-national communities engender their own legal systems by constructing nearly self-contained spheres of normativity, adopting their own rules, applying them in their own dispute resolution fora and ensuring the implementation of outcomes by means of their own enforcement mechanisms. In other words, what matters is not that states attribute law-making functions and capacities to non-national communities, but rather that such communities create normative systems which are jural by themselves, by virtue of their autonomous or autarkic functioning. The state does not confer, as François Rigaux would say, 'to private orderings a juridicity that they do not possess by themselves'.[160] Berman seems to have noticed this possibility, writing that '[n]on-state communities also assert lawmaking power through more informal networks and organizations and through the slow accretion of social custom itself'.[161] But his assertion, precisely, does not go far enough. Non-state communities can regulate not only through such

[158] Berman, *supra* note 56, at 424 and throughout parts III and IV.

[159] Duguit and Kelsen, 'Foreword', 1 *Revue internationale de la théorie du droit* (1926–1927) 1, at 3.

[160] F. Rigaux, *La loi des juges* (1997), at 28.

[161] Berman, *supra* note 56, at 504.

informal and spontaneous norm formation – norm formulation of this sort is social in nature and should not be considered jural for fear of 'losing all sense of what [law] is', as Simon Roberts would say.[162] These communities can also regulate through much more sophisticated and formal structures, with proper legislative, adjudicative, and enforcement powers (as portrayed here), structures that operate in a fashion much closer to a public legal system and, for that reason, deserve to be called law – at least much more than the mechanisms Berman evokes.

I have furtively introduced into these developments an argument about non-national and non-geographic communities which remains to be directly addressed. If the invocation of such communities comes across as an incongruity, it is because it was traditionally considered that social structures rely on physical spaces that sociability is dependent on geography.[163] But as the informational wealth of distant communication increased, and since communication is the essential vehicle of community formation,[164] geographic proximity became increasingly less a necessary condition of sociability.[165] The Internet enabled this increase to such an extent that sociologists now readily acknowledge the existence of delocalized communities based on electronic communications[166] – one of many forms of 'transnational communities [as] communities of interest that cut across nation-state boundaries'.[167] What binds the members of such communities together is no longer the localness of their presence but the 'selective ties' that they choose to establish which are typically shared affinities, interests, and goals.[168] And these are, not infrequently, of a commercial nature.

The importance of identifying such online communities hopefully goes beyond the intuitive when we contemplate certain considerations informing the principle *ubi societas, ibi ius*.[169] The central tenet of some of the most astute and illuminating distillations of the process of law's emergence, for instance those of H.L.A. Hart, Noberto Bobbio, Paul Bohannan, François Ost, and Michel van de Kerchove, resides on the observation that, as soon as people gather to form a group, social norms will start to emerge. Under some circumstances, these social norms subsequently become jural, forming a legal system.[170] (Properly speaking, the phrase should thus rather be *ubi*

[162] Roberts, *supra* note 2, at 24.

[163] M. Castells, *The Internet Galaxy: Reflections on Internet, Business, and Society* (2002), at 125–126.

[164] Anderson, *supra* note 34, at 5–6, 36.

[165] See generally A. Giddens, *The Consequences of Modernity* (1990); J. Meyrowitz, *No Sense of Place: The Impact of Electronic Media on Social Behavior* (1985).

[166] Virilio, *The Information Bomb* (2000), at 59; H. Rheingold, *The Virtual Community: Homesteading on The Electronic Frontier* (rev edn, 2000); Noveck, 'A Democracy of Groups', 10 *First Monday* (2005), available at: www.firstmonday.org/issues/issue10_11/noveck.

[167] Berman, *supra* note 56, at 476.

[168] Castells, *supra* note 163, at 119–125.

[169] 'Where there is human interaction, there is law.'

[170] See, for instance, H.L.A. Hart, *The Concept of Law* (2nd edn, 1994), at 91ff; Bobbio, 'Ancora sulle norme primarie e norme secondarie', 59 *Rivista di filosofia* (1968) 35; Bohannan, 'The Differing Realms of the Law', 67 (6) *American Anthropologist* (1965) 33, at 34–37; M. van de Kerchove and F. Ost, *Legal System Between Order and Disorder* (1994), at 110. See also J. Stone, *Social Dimensions of Law and Justice* (1966). It may have to be pointed out that the position defended here rejects the idea of *ubi societas ibi ius stricto sensu*, that wherever there is a society, there is *ipso facto* law, as defended for instance by Sacco, 'Mute

societas, ibi regula.[171]) Brutally simplified, the circumstances required for juridicity are the autonomy of the normative system in formation *vis-à-vis* other normative systems (and, with respect to private legal systems, *vis-à-vis* the public legal system in particular),[172] the presence of clearly demarcated secondary rules, in the Hartian sense, conferring specific people particular powers and roles within certain institutions,[173] such institutions having the jurisdictional capacities to prescribe, adjudicate, and enforce.[174] Communities form the backbone of this process, they constitute the *sine qua non* element of the emergence of social norms that may then become legal systems. Identifying online communities helps to understand that nation-states are not the only relevant communities with regard to the assertion of jurisdictional powers, though they remain the most important ones.[175]

It can probably be surmized that all online communities, merely by their quality of being communities, develop norms of conduct of their own. Some of these communities, primarily those which most urgently need some of law's typical functions, are then likely to turn these social norms into legal norms. It is apparent that commercial online communities are those, among online communities, which require most strongly the fulfilment of law's functions of predictability and the provision of access to an efficacious remedy, because of the stakes involved in the relationships. They are those which seem to have the strongest urge to be equipped with a normative system that is autonomous, formalized, and clearly defined so as to be predictable – the best instance of which is law.[176] They were, as it seems, the first to develop such transnational, non-comprehensive legal systems which lead to a carving up of the Internet into layers of normativity.[177]

Law', 43 *Am J Comp L* (1995) 455; del Vecchio, 'Sulla statualita del diritto', 9 *Rivista internazionale di filosofia del diritto* (1929) 1, at 19; L.J. Pospisil, *Anthropology of Law: A Comparative Theory* (1971), at 96; Cover, 'The Folktales of Justice: Tales of Jurisdiction', in M. Minow, M. Ryan, and A. Sarat (eds), *Narrative, Violence, and the Law: The Essays of Robert Cover* (1992) 173, at 176; J.-F. Perrin, *Sociologie empirique du droit* (1997), at 38.

171 'Where there is human interaction, there are rules.'

172 H. Kelsen, *Pure Theory of Law* (1967), at 71; van de Kerchove and Ost, *supra* note 170, at 135–142.

173 See Hart, *supra* note 170. See also G. Gurvitch, *Eléments de sociologie juridique* (1940), at 185–186.

174 See J. Locke, *The Second Treatise on Civil Government* (1986 [1690]), at chap. IX, secs 124–126; Rigaux, 'Les situations juridiques individuelles dans un système de relativité générale', 213 *Hague Lectures* (1989) 28.

175 Berman, *supra* note 56, at 440.

176 On autonomy, formalization, and ascertainability cf., though in a different context, M. Koskenniemi, *From Apology to Utopia: The Structure of International Legal Argument* (1989), at 2.

177 Not just commercial online communities have developed their own sophisticated regulatory framework, which ought to be recognized as a legal systems. The online encyclopaedists' community of Wikipedia appears to be moving into the same direction: see, e.g., Katsh, 'Dispute Resolution Without Borders: Some Implications for the Emergence of Law in Cyberspace', 11 *First Monday* (2006), available at: www.firstmonday.org/Issues/issue11_2/katsh/index.html. See also Reagle, 'A Case of Mutual Aid: Wikipedia, Politeness, and Perspective Taking', in *Proceedings of Wikimania 2005* (2005), available at http://reagle.org/joseph/2004/agree/wikip-agree.html; Benjamin, 'Public Participation and Political Institutions', 55 *Duke LJ* (2006) 893, at 925.

Before we move on to an illustration of such systems, a final point must be made. I have invoked the existence of 'proper' transnational legal systems, based on a conception of the legal system that is proximate to the public legal order as it involves prescriptive, adjudicative, and enforcement jurisdictional powers. This conception is opposed to the watered down acceptance of a legal system typically used by those asserting that the *lex mercatoria* forms a transnational legal system or that there is such a thing as a worldwide *lex electronica* covering all Internet-related activities. If this invocation now comes across as an incongruity, it is because of the public legal system of the modern state having been so preponderantly present that it largely has been obscuring other possibilities of juridicity. Yet one should remember, as anyone with an interest in history would enjoin us to do, that the nation-state is a recent (on the scale of Western civilization[178]) historical and political construction, that it was 'a brief historical moment when the ideas of nation and state were being joined by a hyphen to create a historically contingent Westphalian order'.[179]

C *Illustration*

Departures from sound and honest business practice are pervasive and inevitable, as are mere misunderstandings leading to disputes. eBay is no exception in this regard.[180] A small fraction of the several million transactions concluded each day on this electronic marketplace go awry. There more than in many other contexts, this fact of life initially raised several important issues: the average value of a dispute is low; the parties are typically more distant, geographically speaking, from one another than in comparable commercial relationships outside the Internet; and the typical level of trust between trading partners is lower than, for instance, on a brick-and-mortar marketplace. This low level of trust generated by the absence of traditional points of reference[181] was accentuated by the parties' awareness that they could rely with difficulty on an effective remedy when faced with a dispute. Courts, as was mentioned above, do not offer a rational option, because the costs they entail are prohibitive for the typical eBay dispute. The Internet is more conducive to such cost problems than the ordinary real-world environment, because of the characteristically heightened geographic distances and jurisdictional ambiguities, as well as the need for translation and other

[178] Reference is made here to Western civilization because it formed the cradle of the early law of nations and of the nation-state itself: J. Crawford, *The Creation of States in International Law* (1989), at 9, R.H. Jackson, *Quasi-States: Sovereignty, International Relations, and the Third World* (1990), at 59ff. See further Graveson, 'The Origins of the Conflict of Laws', in H. Bernstein, U. Drobnig, and H. Kötz (eds), *Festschrift für Konrad Zweigert* (1981) 93, at 96ff.

[179] Berman, *supra* note 56, at 320.

[180] The example of eBay was examined in more detail in Schultz, 'Private Legal Systems: What Cyberspace Might Teach Legal Theorists', 10 *Yale JL & Tech* (2007) 151.

[181] These points of reference are formed by material features (see Lessig, *supra* note 13, at 30–42) and familiar social contexts which usually permit the assessment of the trustworthiness of an offline situation (see Nadler, 'Electronically-Mediated Dispute Resolution and E-Commerce', 17 *Negotiation Journal* (2001) 333, at 335). See further Schultz, 'Does Online Dispute Resolution Need Governmental Intervention?' The Case for Architectures of Control and Trust', 6 *NC JL & Tech* (2004) 71, at 77.

similar factors. The result is the extreme rarity of an eBay dispute ending up in court – generally estimated to be in the range of less than one in 1,000 cases. Social sanctions, for instance spreading the word about deceitful business practices, were not available either, the parties involved being mostly unknown traders engaging uniquely in one-shot transactions. The resulting lack of trust prevented eBay from reaching its full commercial potential. A practicable and effectual dispute resolution framework had to be developed. The solution took a triple form: first, eBay gradually developed eBay user policies; secondly, it introduced a reputation management system; and thirdly, it put in place a dispute resolution mechanism.[182]

The reputation management system is first worthy of attention. It can be conceived of as an instance of the re-creation, on the Internet, of the social context that usually allows the emergence of reputation as a control lever.[183] To develop, online reputation needs to attach to a social context featuring two particularities. First, a long-lasting link must be established between the online identity and the real identity of a person. In eBay's system, this is achieved by a verification of some determinant personal details of the users seeking to obtain an online profile. The profile then lastingly attaches to the real identity, and subsequent modifications are clearly marked on the avatar of the user. The second required feature is the establishment of a traceable history of actions: on eBay, users leave permanently accessible feedback, formalized into a positive, neutral, or negative rating point, following concluded transactions. This 'fills' the online identity with information that will constitute the online reputation.[184]

The dispute resolution mechanism consists of online computer-assisted negotiation followed by online mediation. These dispute resolution services have been outsourced, for clearer independence, to a company called SquareTrade, which resolves about 1.5 million disputes per year, mainly, though not exclusively, for eBay. The first stage of the dispute resolution process consists of the parties negotiating from afar using an interactive computer programme. The programme helps the parties pin down their issues by suggesting standardized dispute descriptions based on prior cases. It then helps the parties reach a solution by recommending settlement agreements that, according to

[182] For a more detailed account of the response to this need for an effective remedy, which took the form of a spontaneous social regulation before becoming the more formal framework of dispute resolution about to be described, see, for instance, Baron, 'Private Ordering on the Internet: The eBay Community of Traders', 4 *Business and Politics* (2002) 245, at 246–247.

[183] Let it be noted that reputation is typically used as an instrumentality of social norms but is also serviceable for the pursuit of jural ends: legal systems, public or private, may rely on reputation to create incentives for compliance. See, for instance, Lessig, *supra* note 120. On reputation as a vector of control see, for instance, F. Fukuyama, *Trust: The Social Virtues and The Creation of Prosperity* (1995), at 26 and, generally, K.J. Arrow, *The Limits of Organization* (1974). See also Laufer, 'Confiance, esthétique et légitimité ', in R. Laufer and M. Orillard (eds), *La confiance en question* (2000), at 204.

[184] An economic experimental study on the value of reputation on eBay showed the following: '[a] high-reputation, established eBay dealer sold matched pairs of lots – batches of vintage postcards – under his regular identity and under new seller identities (also operated by him). As predicted, the established identity fared better. The difference in buyers' willingness-to-pay was 8.1% of the selling price': Resnick, Zeckhauser, Swanson, and Lockwood, 'The Value of Reputation on eBay: A Controlled Experiment', 9 (2) *Experimental Economics* (2006) 79.

the data aggregated by the programme, have frequently been accepted before in similar situations. The programme, technically called an expert system, learns from prior failures and successes. The second stage of the process (online mediation) intervenes if the parties consider that the expert system is unable to bring them to an agreement. In this case, the mediator merely replaces the expert system and goes about her task in much the same way as the technical system.[185] This dispute resolution procedure has been designed to operate at very low costs: it takes place online, it is mostly handled automatically by a computer system,[186] and it is simple enough for the parties to dispense with legal counsel.

Smooth operations on eBay still required two further elements: the direct ascertainability by the users of the relevant norms and a low-workload process for the assessment of cases and each party's position. The former is a necessary condition of predictability, allowing eBay users to 'apprise themselves of the legal consequences that attach to various courses of conduct', so as to inform their reasoning about appropriate courses of action.[187] The latter, which a slightly simplified account may call a requirement of simplicity, is indispensable to maintain the costs and time necessary for the resolution of a dispute at a low level, proportional to the value of the transaction.

The response provided by eBay to these two needs was a 'uniform law', which took the form of user policies. The objective is to avoid the jurisdictional questions posed by the application of state law. Regularly updated and completed on the basis of new commonly observed practices of eBay members,[188] they have progressed into a well-developed, relatively dense, detailed, and formalized set of rules of conduct. As we will see, they appear to regulate the behaviour of eBay members in a fairly comprehensive manner.

One should be alert to the fact that they do not regulate the members' conduct merely as a contractual framework would, within the limits and in the shadow of state law. Rather, for the sake of predictability and simplicity and in apparent realization of the users' desiderata, they appear to effect an overriding of mandatory rules.[189] Their regulatory workings appear to be closer to a legal system than to a contractual framework. A testament to this is the fact that, when asked under the shadow of which law they negotiate or mediate, eBay disputants have reportedly replied that it was 'eBay

[185] On this process see Abernethy, 'Building Large-Scale Online Dispute Resolution and Trustmark Systems', in *United Nations Forum on ODR* (2003).

[186] Its marginal costs to resolve one supplementary dispute are thus virtually nil.

[187] M.H. Kramer, *Objectivity and the Rule of Law* (2007), at 116, arguing that 'public ascertainability' (or user ascertainability), which he derives from a re-understanding of Fuller's principle of promulgation as an indispensable feature of law, is a 'necessary condition not only for the rule of law but also for any viable mode of governance', as it would otherwise be 'thoroughly inefficacious in channeling people's behavior'.

[188] Calliess, 'Transnational Consumer Law: Co-Regulation of B2C E-Commerce', in O. Dilling, M. Herberg, and G. Winter (eds), *Responsible Business? Self-Governance in Transnational Economic Transactions* (2008).

[189] On eBay ignoring certain mandatory rules, which the public legal system does not allow to contract out of see *ibid.* (focusing on German law).

law', in other words the policies described here.[190] eBay members faced with a dispute seemed to view the legitimate order determining their rights and obligations not as national consumer protection law, but as eBay's policies. What probably leads to this situation is the exceptionality of the resolution in court of an eBay dispute – a situation in which the relevant national consumer protection regime would be applied. It is realistic for eBay members not to expect that their dispute will end up in court, due to the high costs of litigation, and to draw the conclusion that state law is inefficacious for such disputes, and hence has limited relevance. Another factor of this situation is the fact that eBay's user policies have a high level of efficacy and constraining power, by virtue of the instrumentalization of the reputation of its members. This is achieved by sanctioning members who refuse to participate in the dispute resolution process or who subsequently fail to comply with its outcome. The sanction consists of the attribution of a negative point of reputation or, if negative feedback has already been given by the other party to the transaction, the loss of her best chance to have it removed. This is not a threat taken lightly by the vast majority of eBay members, since reputation points are one of the main determinants of the success of a sale on eBay. In addition, if the member in question bears on its offerings a special icon from SquareTrade called a seal or trustmark (which testifies to the fact that she has pledged to submit to the dispute resolution process and in the past has been shown to have complied with this pledge), this icon may be removed as well. This trustmark appears to have a significant economic importance: when an eBay trader displays it, the number of bids placed for each of her items will typically increase by 15 per cent and the average selling price by 20 per cent.[191] Non-compliance with the eBay user policies comes at the price of reputation, and thus of economic well-being. The outcomes of eBay's dispute resolution process are reportedly complied with in 98 per cent of cases, which suggests a high level of efficacy in the use of reputation as a control lever.[192]

Through this scheme eBay has developed, as I hope the preceding has shown, a normative system which is autonomous: eBay creates its own norms, has mandated a private company to apply them, and indirectly enforces them through the reputational incentive. It is further relatively formalized and predictable (since the user policies are well defined), it is easily accessible and does not require the complex legal reasoning that conflict of law rules often require. eBay has created its own law, it controls the procedure in which this law is (indirectly) applied to the dispute, and it controls the mechanism used to enforce the outcome of this procedure.

[190] Katsh, Rifkin, and Gaitenby, 'E-Commerce, E-Dispute, and E-Dispute Resolution: In the Shadow of "eBay Law"', 15 *Ohio State J on Disp Resol* (2000) 728. On the concept of the 'shadow of the law' see Mnookin and Kornhauser, 'Bargaining in the Shadow of the Law: The Case of Divorce', 88 *Yale LJ* (1979) 950, at 968; Cooter, Marks, and Mnookin, 'Bargaining in the Shadow of the Law: A Testable Model of Strategic Behavior', *J Legal Stud* (1982) 225.

[191] See interview with Steve Abernethy, CEO of SquareTrade, in Kaufmann-Kohler and Schultz, *supra* note 147, at 328.

[192] Calliess, 'Online Dispute Resolution: Consumer Redress in a Global Marketplace', 7 *German LJ* (2006) 647, at 653.

Conclusion

This article has told a story about national government and global law, about values and identities, about the proverbial homogenizing effects of globalization and what has aptly been called 'the other side of globalization: the determined preservation of difference'.[193] We have seen that, on the Internet as in any other regulatory context, values seem to play a crucial role: when they are common on a transnational level and relate primarily to ensuring the proper functioning of business, they allow and even call for the creation of transnational private legal orders. These orders lead to a carving up of the Internet into discrete transnational private spheres, which may be pictured as layers. When the values relate to identity and vary from one region or nation to another, they rather call for a return to stronger government intervention, leading to a carving up of the Internet into discrete national or regional spheres, which may be pictured as billiard balls. This double evolution seems to respond to the fundamental question about the Internet: 'ultimately, can states take advantage of the commercial and expressive capacities of a global network, while at the same time protecting local values?'[194]

Such a double phenomenon is not unheard of. It is reminiscent of the *lex mercatoria*, for instance, where international arbitration and global commercial and trade law push for the emergence of transnational regulatory spheres, while the concepts of public policy in arbitration,[195] public morals and public order in WTO law,[196] or 'overriding public interest' opposed to the freedom of movements in EU law[197] are there to preserve cultural exceptionalism. But on the Internet, this dual phenomenon seems radically stronger, with transnational private legal systems that much more clearly constitute legal systems than the *lex mercatoria* and methods of preservation of local differences that appear much more powerful than the concepts of public policy and the like. In this sense, the regulation of the Internet is a paradigmatic example of the dialectical progression of law on the international plane, of the duality of globalization. Such is the descriptive part of the considerations developed here.

The normative part of the considerations developed in this article revolves around the idea that the regulation of the Internet should rely, at its most foundational level, on both a universal and a national social contract. This dialectic mainly has consequences for assertions of jurisdiction and filtering of information. The argument is that the Internet, more than most other contexts, calls for a return to a natural law approach to conflicts of laws – a return to Savigny and von Bar, where conflicts of laws were 'part of a single international system, not [purely] part of domestic law',[198] where the determination of jurisdictional scopes were not 'dependent merely upon

[193] Goldsmith and Wu, *supra* note 7, at 183.

[194] Fagin, *supra* note 118, at 399.

[195] The concept of public policy in arbitration is for instance used to challenge and oppose enforcement of arbitral awards.

[196] Art. XIV(a) GATS.

[197] See especially Case 33/74, *van Binsbergen* [1974] ECR 1299, at 1309ff, paras 10ff.

[198] Mills, *supra* note 31, at 37.

the arbitrary determination of particular states'.[199] This means that national regulations must take into consideration their effects on the territory and population of other nations as well as on the information wealth of the common good that is the Internet. States must recognize that they are all co-equals in the global task of regulating the Internet, a notion reminiscent of a universal social contract. At the same time, states cannot dispense with the legitimate central ideology that has been underlying for so long the positivist approach to international law, namely that states are entitled and have a duty to pursue 'the protection of national interest [and] the enforcement of national values'.[200] The resulting implications are, as I have argued, a call for moderation and restraint with respect to assertions of jurisdiction seeking to sanction a behaviour (using the concept of targeting narrowly construed as a jurisdictional standard) and public filtering of unwanted incoming content in order to enable catharsis and protect local values. In a recent brilliant article on the interface between public and private international law, Alex Mills reminds us that '[p]rivate international law was invented as a mechanism for the reconciliation of higher level natural law with the existence of diverse laws'.[201] In that sense, restraint and moderation in the exercise of jurisdiction should be viewed not as the consequence of a voluntary deference to a foreign national, but as a 'natural law requirement', in accordance with the original purposes of private international law.[202] Combined with filtering technologies, such an approach would appear to promise the best future for the Internet and its users.

[199] von Bar, *supra* note 36, at 2.
[200] Mills, *supra* note 31, at 46.
[201] *Ibid.*
[202] *Ibid.*, at 47.