Establishing Legal Order in the Digital World: Local Laws and Internet Content Regulation [1]

Yulia A. Timofeeva
University of Leipzig

Abstract.
The need for establishing legal order in cyberspace is growing; the time has come when it is also possible in several different ways. One of the crucial issues in this respect is the worldwide reach of the global network. Legal rules for human activities, including online activities, vary from state to state, and regulation of cyberspace cannot occur in one single manner all over the world. The existence of various laws produces far reaching consequences both for users and for regulators. Thus, users might face legal consequences in a foreign state for activities lawful in their home jurisdiction, and states might not be able to enforce the laws if the offender resides in another state. This paper examines this issue, in particular the issue of Internet content regulation. The approach proposed here is to focus on the new actors in the online world and the new regulatory choices they offer.

Key Words: Content Regulation, Jurisdiction, Actors, Zoning

I. INTRODUCTION

The Internet enables a variety of human activities, all of them remarkably different from each other in their social and legal meaning. However, a state has one common task in respect of all these activities – to ensure that rules and principles developed for the offline world do not lose their significance in the digital word. In fact, no state would willingly tolerate a situation where a particular activity evades regulation just because it is committed by means of the global computer network. Even if currently there are still exceptions from this approach, the trend is clear – all activities going on online will be regulated to the same extent and to the same effect as the activities in the offline world, if not more.

The regulatory zeal of states is increasing, but there are several factors that complicate the task. The most obvious one is the globality of the Net. No state has ever claimed the authority to regulate all human activities in all parts of the world and the concept of territoriality has not lost its meaning in the digital age. Even though there have been several examples of states extending prescriptive jurisdiction beyond the principles developed in the offline world, it can hardly become a rule. States have yet to figure out how to ensure compliance with local laws in cyberspace. Another significant factor is a presence of new participants, which are not even analogous to the traditional actors in the offline world. Some of them can control the movement of bits of data at their respective level of the network; others do not directly participate in data exchange but can nevertheless produce a meaningful impact on availability and accessibility of online content. Whether these actors will be considered in regulatory schemes, how, and to what extent – these questions are of the utmost importance when dealing with the issue of Internet regulation.

The paper focuses on regulation of Internet content but the approach offered here may be equally applicable to other Internet-related issues. Any online activity involves movement of bits of data from one computer to another, be it dissemination of illegal content, copyright infringement, gambling or cybercrime. Of course, there are many specifics in each field, but there are also common features so that the main points for state intervention often remain the same. Among other issues, the issue of content regulation is particularly controversial – the discrepancy of what is considered objectionable across the world is enormous but many states attempt to achieve the same degree of control over online expression as they used to have over local publications in the offline world. The necessity to find a way to accommodate all existing laws is growing, at least from the regulator's perspective.

[1] The paper was published in Complex 4/2006 LSPI Conference Proceedings.

The analysis of the options that are available to a state for designing cyberspace according to local preferences is undertaken in two parts. The first part offers identification of the available regulatory options and examination of their advantages and drawbacks. The second part involves making a choice between them. Particularly, it considers such issues as limits of jurisdiction of a state and costs that are connected with one or another regulatory scheme for all concerned participants.

II. FRAMEWORK FOR THE ANALYSIS

There are a number of theories that offer guidance for dealing with regulatory problems arising on the Internet. For example, it is elaborated on the significance of the computer code that may determine the limits of online activities more successfully than law (Lessig, 1999); the analysis of perspectives explains the discrepancy between what we think we do in cyberspace and what is actually happening between computers on the network (Kerr, 2003); the theory of layers provides an insightful overview allocating the processes taking place on the Internet to certain layers (Weiser, 2003). The latter theory is particularly popular within the discussion on Internet regulation.

The theory of layers contributes to understanding the intrinsic relationships of various elements that support functioning of the global network and demonstrates that contrary to the physical world, there are several distinct layers where various kinds of regulatory intrusion can happen. For example, the four-layers model offered by Weiser (2003) distinguishes the physical, logical, application, and content layers. In restricting dissemination of an offline publication after it has been released to the public, one could intervene at one layer only – at the physical layer – and order forfeiture of the actual published work. In respect of an online publication, it is possible to intervene at the content layer and remove objectionable content directly from the hosting ISP so that it is not "in cyberspace" anymore. It is also possible to intervene at the application or logical layer and arrange filtering or zoning of content. It is even possible to destroy the wires connecting to the Internet, i.e. to intervene at the physical layer, although it wouldn't be the most reasonable option.

The layered analysis demonstrates the scope of the field and calls for considering new regulatory options. However, it does not clearly identify the addressees of state regulation. A more attractive strategy could be to concentrate on actors participating in the process of information transfer and on the functions they perform. Such an approach shows precisely, at which points a state can assume control. To be consistent, one can follow the movement of data from the author or content provider to the end user. Zittrain (2003b, p.657) regarded this process as having five distinct phases: "It begins at (1) a source, passes through (2) the source ISP, continues through transit and/or peering through (3) the cloud, is handled by (4) the destination ISP and then arrives at (5) the destination." To modify the above typology to enable a more precise analysis, two main phases can be distinguished. The first phase covers movement of data from the content provider, through several intermediaries, to an ISP providing hosting of content. It is a movement of data to the location, at which they are "in cyberspace," permanently available to all Internet users – it is the input side of Internet activities. The second phase covers movement of data from the hosting provider ("from cyberspace"), through several intermediaries, to a computer of the end user – it is the output side of Internet activities. The terms "input" and "output" emphasize the movement of information flows and the function a particular actor performs in any given moment.

In addition to the input and output actors, there are a number of actors that do not directly participate in information transfer but nevertheless produce a notable impact on availability and accessibility of Internet content to a user. For example, search engines disclose the existence of content to a user; registries allow surfing without having to remember an IP address of each site. These actors offer indirect points of control and increase the variety of options for state regulation of Internet activities.

III. INPUT CONTROL

The actors that ensure that content gets and remains online include individual users publishing content in cyberspace and ISPs performing a variety of functions, from providing Internet connection to hosting third-party content. Of course, in reality many actors perform their functions on the input side and output side

simultaneously. Thus, unless a user is a passive visitor of websites, he or she is both an author and a reader of content. Similarly, an ISP providing Internet access is usually performing both the input function and output function, carrying the data from the user and to the user at the same time. However, the legal position of the same actor is quite specific in each role. There is a difference, whether a state prosecutes an author or a viewer of objectionable material, as well as there is a difference in legal obligations of an access provider carrying the data to the user and from the user.

A. Input User as a Point of Control

Measures directed at a user placing material on the server connected to the Internet offer the most obvious solution. To prevent illegal content from getting online, a state may establish civil and criminal sanctions on the input user. This is a popular approach; in fact, no state would feel reluctant to prosecute an author of an online publication any more than an author of any other publication.

However, a state can only effectively prescribe the rules to those users who reside on the state's territory. Even though international law recognizes the authority of a state to prescribe laws to foreign actors under certain circumstances, the power to enforce the laws often works as a practical limitation on it. The opportunity to exercise jurisdiction over foreign actors is rare. The most prominent example involving Internet content is the prosecution of an Australian citizen when he came to Germany on a vacation trip. He was charged with dissemination of statements on Holocaust denial, which is prohibited in Germany.[2] But, this example is rather an exception than a rule.

When the goal of regulation is not only to punish the offender but also to remove objectionable content from cyberspace or at least make it inaccessible to local audience, prosecution of the input user is not necessarily the best solution due to persistency of Internet content. Once content has been published on the Internet, it is not always possible to exercise control over its dissemination. Other persons can overtake content management; adherents can create mirror sites and continue to spread the message. Thus, the controversial site that was a cause for prosecution in the above case is still online, freely accessible in Germany.

B. Internet Service Providers

The actors gaining power in the digital age are becoming visible – any online activity needs the services of Internet Service Providers (Ahlert et al., 2004). Precise definition of this category of actors is hardly conceivable due to the abundance of tasks they carry out, but almost any ISP is able to exercise control over information flows at its respective level. Depending on a particular function an ISP performs, it may be a subject to different state-imposed obligations.

1. Content Providers and Zoning

The legal status and controllability of an ISP that acts as a content provider is similar to the status of an individual user. An ISP may face civil and criminal sanctions for the authored content in the same way. However, several factors make an ISP a more attractive point of control. First, in comparison with an individual a corporation has fewer opportunities to hide or to remain anonymous, being an easier target for a state (Swire, 1998; 2005). Second, state measures directed at a corporation are more likely to actually remove objectionable content from the Internet. Thus, it is probable that in the German case mentioned above, the controversial website would not be available on the Internet anymore if Germany could assert jurisdiction over the Adelaide Institute, which offers a base for Australian revisionists, instead of prosecuting just one of its members. Finally, a corporation may be required to take specific measures to keep its content from locations where it is considered objectionable, i.e. to exercise zoning.

Zoning refers to a technical procedure undertaken by a content provider to direct information flows to particular users only. Metaphorically, it can be described as creating zones in cyberspace that are open for some categories of users and closed for others. A distinction may be drawn between zoning technologies aimed to

[2] BGHSt 46, 212 (Federal Court of Justice, Decision of 12.12.2000).

restrict access of a particular group of users (as a rule, children) and technologies aimed to restrict access of all users within a given location (as a rule, within a state). The latter is of a particular interest for the present discussion.

In terms of geographical zoning, various tools already exist to identify the geographical location of users and many companies routinely employ these tools for targeting advertising purposes (Geist, 2001; Goldsmith, 2000). Employment of geo-location technologies as a means for compliance with local laws without refusing to carry the content generally has not yet become a rule but it is a hot issue. For example, Yahoo! stopped running online casino advertisements after a prosecution threat by the United States but limited the measure to the US territory. Many states would be relieved to have foreign content providers zone content according to states' local laws but such an obligation is hard to impose on foreign actors. So far, there is no obligation to perform regional zoning in any legal norm and only one court addressed the issue of zoning in its decision. In 2000, a French court ordered the US company Yahoo! to restrict French citizens' access to auctions bearing Nazi items.[3] Yahoo! changed its auctions policy to exclude the controversial items but claimed that the French decision was not a reason for the policy change, so that the practical lesson from this decision is not significant. In any case, zoning would be a very convenient option if a state had sufficient power to impose the obligation to zone on a respective content provider.

2. Hosting Providers

An ISP that hosts objectionable content of a third party offers an excellent point of control for a state. Measures directed at this actor can even turn out more effective than targeting the actual content provider considering that the latter does not always have full control over the dissemination of his or her content. Thus, many states impose liability on a hosting provider for the illegal material it hosts. The most severe method is to make hosting providers directly liable irrespective of knowledge of the material's existence and legality. This approach involves a lot of risk for a hosting provider and is likely to influence the decision of an ISP to provide hosting altogether. Many states choose a more flexible model of hosting provider liability – the notice and takedown procedure. It shields a hosting provider from legal consequences as long as a hosting provider does not have knowledge of objectionable content or acts expeditiously to remove objectionable content upon obtaining such knowledge. For example, this approach is followed by the European Union.[4] In the United States, the law grants immunity from liability to hosting providers[5] but there are a number of exceptions from this rule. *Inter alia*, the notice and takedown procedure is applied in case of a copyright infringement.[6] In sum, the imposition of liability on a hosting provider is an effective measure for regulation of Internet content provided that a state has jurisdiction over the hosting provider.

3. Access Providers

An ISP providing Internet access has not yet been regarded as an attractive point of control. No access provider has been held directly liable for actions of its customers anywhere in the world. The European Union's E-Directive explicitly proscribes ISP liability for mere conduit and caching;[7] the United States has similar provisions in 47 U.S.C. § 230(c) (1). Besides, access providers usually reside in the same jurisdiction as their customers so that a state can easily draw to liability the actual author or provider of illegal content.

A different issue is an obligation of access providers to intervene in the process of information transfer from a user to the Internet. Thus, the European Union E-Directive allows a state to require the access provider to

[3] T.G.I., Ordonnance de référé du 22 mai 2000, Association "Union des Etudiants Juifs de France", la "Ligue contre le Racisme et l'Antisémitisme" Yahoo! Inc. et Yahoo France.
[4] Art. 14, Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market [hereinafter E- Directive].
[5] 47 U.S.C. § 230(c)(1).
[6] 17 U.S.C. § 512(c) (Digital Millennium Copyright Act).
[7] Art. 12 (1) and Art. 13 (1), E-Directive.

terminate or prevent an infringement[8] and the states do not ignore this possibility. The United States follows the same line in respect of copyrighted material.[9] Currently, this approach is not applied broadly. However, as technology develops, an access provider might face more obligations imposed by a state. Considering the general move for control in the name of security all over the world, many states obligate ISPs to monitor all incoming and outgoing traffic. Theoretically, once facilities are there and monitoring is a rule, an obligation to report or to block objectionable content incoming from a user could follow. Of course, other values are to be considered within this approach, from privacy to freedom of expression. Nevertheless, access providers provide another point of control for a state.

IV. OUTPUT CONTROL

The actors on the output side are the same or similar to the actors on the input side – a user and an ISP. However, the functions they perform in the process of information transfer make their legal position, obligations, and liability distinctly different. In contrast to the input actors, the actors on the output side are always closely connected to a local forum. Indeed, a state has no, or only very remote interest in regulating the output side of data transfer beyond its borders. No state has ever prescribed to residents of another state what content they are allowed to look up in cyberspace or elsewhere. It means that there are no jurisdiction or enforcement concerns for a state on the output side.

A. Output User as a Point of Control

A user receiving information from the Internet is a subject of control in many states. Criminalization of online activities involving illegal content is a common measure. For example, where criminal codes proscribe creation or possession of illegal content, these restrictions are automatically applicable to the Internet. Thus, downloading illegal material from the Internet is interpreted as "production" or "making" of illegal material by many courts and is punishable. Similarly, possession of illegal material that a user downloaded from the Internet is often a separate offense. Besides, several states establish liability of a user for "mere viewing" of objectionable sites. Because every instance of "viewing" of prohibited material means a copy of it in the "temporary Internet files" folder, some courts interpret it as possession of illegal content.[10] At least one country, Australia, explicitly criminalizes the act of accessing illegal material.[11]

Theoretically, another way to control online activities of users is conceivable. Thus, computer owners could be forced to configure their computers to filter out illegal material. Already, the digital rights management initiatives work on developing computers, which would give a user only limited rights in managing content (Zittrain, 2003b; 2006). This development is primarily directed at protection of intellectual property but it also opens the way for more control of private Internet usage generally. However, this option might not be worth the effort for a state since the same effect may be achieved by filtering obligations on output access providers.

In addition to the above measures, some governments are very creative in inventing further tools to decrease the incentive of users to look up prohibited content. For example, the computer of a Chinese user can become frozen as a reaction to the attempt to download prohibited information from the Internet; Uzbek authorities use "modified mirrors" – they do not just restrict access to the controversial sites but redirect users to the copies of these sites containing less controversial material.

B. Output Access Providers

The category of output access providers includes not only technical actors responsible for Internet connection, such as a dial-up ISP or a backbone computer, but also those access providers that offer Internet access in the most literal meaning, such as libraries, schools, and Internet cafés. Output access providers are central players

[8] Art. 12 (3) and Art. 13 (2), E-Directive.
[9] 17 U.S.C § 512(j).
[10] *See, e.g.*, United States v. Tucker 150 F. Supp. 2d 1263 (D. Utah 2001).
[11] Section 474.22, the Criminal Code Act (in respect of child pornography material).

for regulation of Internet content. First, they are by their nature local and always available for state regulation. Second, they are more visible than millions of individual users and can be easier subjected to state control.

Currently, the majority of states use output access providers for filtering or blocking Internet content on its way to the end user. Extent and methods of filtering vary all over the world, as well as the ways of ensuring compliance with the filtering obligation. Sometimes ISPs are actually extension of the government; in some states compliance is ensured by licensing requirements; access providers may also be held liable for actions of their customers if they don't prevent the forbidden activity. For example, cyber cafés in the United Kingdom have been held responsible for letting visitors download music files from the Internet.

The main problem of regulation through output access provides is that they have to rely on filtering technologies and these technologies cannot always ensure the desired result. The issues of underblocking and overblocking are widely discussed; besides, various technical tools are available to circumvent local filtering. Nevertheless, filtering can achieve a remarkable degree of effectiveness if a state is not too concerned about blocking harmless information and the usage of circumvention tools is forbidden. For example, China managed to create a sophisticated and well functioning filtering system – "the Great Chinese Firewall". In this way, access providers act as the right hand of a state determining what kind of Internet content residents of a state can access.

V. INDIRECT POINTS OF CONTROL

The input actors and output actors directly participating in information transfer are likely to remain the main points of control for a state. However, the Internet offers a vast playing field for innovative approaches. There are a number of actors whose activities influence availability and accessibility of online content indirectly but significantly. While it is impossible to cover all of them, the most significant players can certainly be distinguished, such as search engines and registries for the purpose of the present analysis.

A. Search Engines

Search engines have become remarkable players in the information age. An average user is totally dependant on search engines and their results, in view of the volumes of content available in cyberspace. The power of a selection mechanism is compared to journalism in non-virtual media and arguably goes beyond it. "It's focus that brings knowledge and power, not diffusion" (Shenk, 1997, p. 174), and search engines, as controlling the focus, are unfailingly increasing their influence. Google, which is one of the most popular search engines at present, fully reveals the role search engines may play in regulation of Internet content.

The search engine Google appeared on the market in 1998 and developed into an extraordinarily powerful actor within a couple of years. Today its meaning is exceptional, both for commercial entities and individual users. If Google fails to list a site in its results, the site becomes almost non-existing. Though the affected site remains on the Internet and can be accessed by a knowledgeable user, other users would not be able to reach it or even to know that it is there. Google makes invisible and Google makes popular. For instance, to the 100th anniversary of Gaston Maurice Julia, Google changed the logo of Google's homepage and awaked enormous interest to the scientist's site almost endangering the site's functioning. In addition, the search engine provides cached copies of the majority of indexed sites that allow users to see content of the site even if the site itself is blocked.

Not surprisingly, many states want to get Google under their control. However, the company is firmly rooted in the United States where its search results fall under protection of the First Amendment of the US Constitution. Apart from the United States, no other state can influence Google, at least not by legal means. However, as a successful transnational company Google cannot completely ignore local laws, especially when interests of economically powerful states are involved, and many regional versions of Google conform to local policies. For example, searches on "google.de" and on "google.com" produce different results in respect of extremists' sites. Similarly, regional news services might reflect government preferences. But, Google often refuses to accommodate its "google.com" results to regional preferences and they remain freely accessible to all users (provided the site "google.com" is not blocked, of course).

This soft form of self-regulation perfectly corresponds with the intention of the states to ensure compliance with their local laws in cyberspace. More liberal states can leave it as it is considering that Google directs all users to the respective regional site first. More restrictive states can block access to the US version of the site letting their residents use the regional version compliant with local laws as it happened in China soon after the introduction of the Chinese Google news service.

B. Registries

The significance of registries is based on the role they play in supporting the functioning of the Domain Name System (DNS). Every computer connected to the Internet has a unique address – a string of numbers – called Internet Protocol address (IP address). The Domain Name System allows a string of letters to be used instead of numbers. It also enables websites to keep their names even if they move to another IP address. While IP addresses "locate resources, location-independent names identify them" (Bechtold, 2003, p. 1249). There are generic Top-Level Domains (gTLD) that do not have a connection to a particular state (such as ".com," ".net," or ".org") and country code Top-Level Domains (ccTLD) that are country specific (such as ".de," ".uk," ".ru"). Although ccTLDs give no information as to the location of the owner of a domain name, they are closely connected to a respective state. In fact, the authority of a state to administer its respective ccTLD space may be compared to the authority over activities on its physical territory (Köhler, Arnd, 2000).

Registries are responsible for allocation of IP addresses and for registration of domain names. They provide an excellent tool for regulation. If a registrar cancels a domain name, the respective website becomes quasi invisible. Although it is still in cyberspace and can be accessed with an IP address, most people wouldn't be able to discover an IP address of a specific website. However, the legal status of registries is not settled. There is a tension between ccTLD registries and the Internet Corporation for Assigned Names and Numbers (ICANN), which is the main supervising body over the Domain Name System generally. Some ccTLD registries are independent entities, such as the German registrar DENIC and the British registrar Nominet UK, while many others have signed agreements with ICANN. As a rule, ccTLD registries have to comply with the official state policy and local laws but ICANN does not always promote the local solution. For example, an American company was entrusted with managing ccTLD of Iraq ".iq" denying this state the right to manage its ccTLD according to local preferences for a long time. Recently, a number of ccTLD were handed over to the respective states, among them the "iq." ccTLD, and this move is certainly to welcome. States need at least some means of control within the general Internet structure and regulation through registries offers the necessary means, even though only in respect of activities that take place under the respective ccTLD.

V. REGULATORY CHOICE AND POLICY CONSIDERATIONS

To ensure compliance with local rules most effectively, states tend to address the actors who are directly responsible for creation and dissemination of online content, namely, the input actors. However, common sense suggests that for any given state most of input actors are outside the state's jurisdiction and a state would not be able to enforce its rules. This is certainly a significant drawback for successful regulation of online activities but it can be mitigated by the fact that no state has an interest to regulate all activities taking place in cyberspace. Rather, a state has only an interest to regulate activities that have a direct connection to this state.

Surprisingly, many online activities are remarkably locally oriented. Thus, a German study of links demonstrates that most of websites are nationally directed (Bucher, 2002). In another example, by the estimation of Russian providers only seldom national users address international sites and two thirds of Russian Internet traffic stays in Russia. The same is likely to be true for other countries or regions. As Swire (2005, p. 1975) correctly noticed, "Although there is the possibility of diverse national laws in every Internet encounter, some mysterious mechanisms are reducing the actual conflicts to a handful of cases". Thus, a state will usually have jurisdiction over the input actors, even if the situations where the necessary input actors are outside the state's jurisdiction will undoubtedly come up as well.

The next actors in terms of effectiveness are registries. Their involvement does not completely remove content from cyberspace but the actual result is very similar in practice. But, similar to input actors, there are the

same enforcement concerns. While a state will have jurisdiction over the registry of the respective ccTLD, it will have no influence over registries of other TLDs.

If the measures directed at the input and indirect actors fail, local filtering through local ISPs remains an always available tool. However, local filtering is not a very attractive regulatory option. Particularly, technical deficiencies of filtering technologies and the inevitable overblocking might influence a decision of more liberal states to employ filtering. Obviously, among other participants the input actors are in the best position to take measures against specific content, be it removing this content from cyberspace or zoning it in accordance with local preferences. There is no risk of overblocking or inaccurate identification of content when input actors restrict specific content at their respective level. Thus, it becomes crucial to create incentives for foreign input actors to comply with laws of other states. The solution is not yet clear but two alternatives can be considered.

Under the first alternative, because objectionable content is a concern for every state, all states could work together on a common solution. It has long been argued that once adequate means are available to control information flows, these means must be employed (Goldsmith, 1998; Spencer, 2006). Today, the technical possibility to direct information flows to some users but not the others is undisputed and it could be used for designing cyberspace according to local laws. For example, states could prescribe content providers residing on their territory to zone content for foreign users according to the preferences of a respective foreign state (for instance, on a reciprocity basis). The consequence for incompliance with the zoning obligation would be liability in local courts or recognition of extraterritorial jurisdiction of the injured state and enforcement of foreign judgments.

The second alternative for making a content provider comply with laws of a foreign state is to deal through ccTLDs. This alternative calls for recognition of the authority of a state over content hosted under its respective Top-Level Domain so that each state would have jurisdiction over a respective "portion" of cyberspace. The authority of a state to prescribe the rules for this portion would perfectly correspond with the authority to enforce the rules, since in case of an infringement a state could act through the registry and cancel the domain name. At the same time, this proposal is not uncontroversial. For example, when ICANN granted control over the Kazakh ccTLD ".kh" to the Kazakh government, some commentators reacted negatively blaming the United States for handing censorship of the Net to other governments of the world. However, the unilateral control of the US over the Internet is hard to justify. As Bertola (2005) noticed, "while I would like the Internet not to be censored at all, I prefer the Kazakh TLD to be censored by the Kazakh government, rather than by the US government." Indeed, the Internet is a worldwide phenomenon and the interests of the main international players, particularly states, cannot be ignored.

Once the need for respecting local laws in cyberspace is recognized and the authority of states over respective ccTLDs becomes undisputed, each state has to determine how far it would go in ensuring compliance with local laws in cyberspace. The most restrictive option would be to limit the Internet access to local content only. A state could also include content from other states sharing similar values or having signed treaties on jurisdiction and enforcement. More liberal states could continue allow access to any Internet "location", assuming the risk that some illegal content will be accessible within the state.

Comparing the two alternatives, there are differences and similarities. Free access to information is equally endangered by both of them. If the first alternative is followed and the obligation to zone content according to laws of foreign states is established, zoning would not only deprive users of content illegal in their home jurisdiction but legal elsewhere but it would also deprive many users of perfectly legal content. Compliance with the zoning obligation for the whole world is not a simple procedure. For some content providers "it may become easier to withhold speech from foreign countries than to sort out inconsistent foreign laws that specify what counts as harmful where" (Van Houweling, 2003). As Zittrain (2003a) predicted, "overcautious or simply indifferent Internet content providers will omit "unimportant" countries from the list of places able to view their offerings, enhancing a digital divide even though such countries are not explicitly seeking strong control over Internet content."

The effect of the second alternative is somewhat different but also dramatic. If a state allowed access to content under its ccTLD only, it would drastically limit access of users to the invaluable information pool in

cyberspace. The Internet would stop being a global network and would transform into a number of local networks that overlap sometimes, such as denet, runet, uknet, etc. Input participants would not be able to reach the worldwide audience. On the other hand, this approach would certainly drive big businesses to establishing local offices. In fact, many significant international players already went local (e.g. Google, Yahoo, eBay, Amazon, etc.).

While the second alternative might seem more restrictive in terms of access to information, it has a clear advantage that a choice remains with a state. It is particularly obvious on the example of less prosperous countries. Thus, under the first alternative, if it is not profitable for a content provider to filter out illegal content or to find out what content is considered illegal under the laws of a poorer state, the provider will simply refuse to respond to requests for content originating within this state. Under the second alternative, a state can decide independently whether to block content of providers that didn't go local or leave unrestricted access to their sites.

Another effect of any form of zoning that should be considered when making a choice is that zoning raises the costs of Internet activities for all participants. As Watt (2003) pointed out, "the real issue seems to be far less "Who regulates?" as "Who bears the burden of zoning?" However, the costs are different under the two alternatives. Under the first alternative, the obligation to zone implies a particular burden on individual users, unless the regulation makes a difference between individual and corporate content providers. It is very doubtful that an individual, as opposed to a corporation, will have the necessary expertise and resources to be able to limit risk of liability through technology (Dauterman, 2002; Strossen, 2000). But, even if the burden of zoning remains on ISPs only, the costs are high. First, there are actual costs of zoning technologies and legal advice. Second, few ISPs would provide free or cheap hosting services when impeded by the obligation to employ geographical filtering in respect of content placed by their customers. Remarkably, the more liberal a country is, the heavier burden would lay on its content providers since they produce a lot of content that has to be zoned for other locations. It appears irrational for states with a more liberal attitude to impose a burden on its residents to enable foreign restrictions.

The second alternative, which implies zoning through ccTLD and voluntary compliance of foreign actors, has a clear advantage in this respect. While the actor performing zoning would have to bear the costs of zoning as well, these costs would be voluntary, driven by a business decision whether to be present in a country or not.

Finally, regulation through ccTLD has another advantage. There are no spillovers from this approach in comparison with liability of a foreign content provider for content legal in his home jurisdiction. It contributes to legal certainty and predictability of the online world – ccTLDs are always associated with respective countries, their values, and policies. Once a corporation wants to go local and establishes a country-specific site, it knows what norms are in force and what laws it has to obey. Input users would not have to fear legal sanctions for speaking in cyberspace without specifically targeting a particular audience and output users could enjoy safe surfing on websites of their own country without risking to encounter content deemed as offensive in their culture as long as they restrict their surfing to country-specific sites.

VI. CONCLUSION

States are increasingly willing to regulate online activities and the time has come when it is also possible in several different ways. However, legal rules for human activities, including online activities, vary from state to state and regulation of cyberspace cannot occur in one single manner all over the world. It is not to expect that states will change their policies just because the Internet is equally present in every part of the world. Thus, the first step to establishing legal order in cyberspace is to recognize the authority of states to regulate online activities according to local preferences.

One of the options always available to regulators is to intervene on the output side and undertake filtering or blocking of controversial content. However, it is not always regarded as an attractive solution. Local filtering is rather a defensive than regulatory measure and it does not address the actual malfeasants. For example, France and Germany do not extensively use filtering or blocking technologies but insist on their right to regulate behavior of foreign actors when their expression is accessible within the state's territory. Conceding to the reality, one has to look for other regulatory options.

The form of regulation states are accustomed to is targeting the author, the publisher, the distributor, or (seldom) the reader of content. In order to adjust the traditional methods to the digital world states would have to claim jurisdiction over all participants anywhere in the world. However, this approach is not only ineffective because of enforcement concerns, it also means a departure from predictability and legal certainty that we used to rely on in our offline activities, and it also means costs for all participants.

There is no need for this drastic measure if one considers the whole range of participants acting in the digital age. Above all, regulation through registries of ccTLD can help to establish legal order similar to the rules of the offline world, where participants have proper notice of the relevant rules and where a state not only has the authority to prescribe the rules but also the ability to enforce them. Regulation through ccTLD has also a weakness – it implies that states do not insist on authority to regulate content beyond their respective ccTLD. But, it also leaves within the discretion of each state the decision on employment of other tools, such as ordering filtering or blocking to local access providers or criminalization of downloading of illegal content.

Of course, regulation through ccTLD implies balancing between the ability of a state to ensure compliance with local rules and the ability of local users to access the invaluable information pool in cyberspace. Similar to the offline world, some states might be more restrictive than the others. At the same time, the diversity of values cannot disappear overnight. While the influence of the international community and international cooperation might contribute to convergence of values, the authority of a state to make an independent choice is undisputed. The Internet is the worldwide technology and its regulation cannot be successful without considering all the interests involved. In the offline world the concepts of sovereignty and territoriality played and continue to play an important role, defining not only the state authority but also the limits of this authority and contributing to peaceful coexistence of different states and cultures. So should it remain in cyberspace.

References

1. Ahlert, Christian; Marsden, Chris; Yung, Chester (2004). How 'Liberty' Disappeared from Cyberspace: The Mystery Shopper Tests Internet Content Self-Regulation. Retrieved Feb. 2006 from http://pcmlp.socleg.ox.ac.uk/liberty.pdf.
2. Bechtold, Stefan (2003). Governance in Namespaces. *Loyola of Los Angeles Law Review*, 36, 1239-1320.
3. Bertola, Vittorio (2005, Dec. 31). Message posted to the mailing list "governance". Retrieved February 2006 from https://ssl.cpsr.org/pipermail/governance/2005-December/005229.html.
4. Bucher, Hans-Jürgen (2002). Internet und globale Kommunikation. Ansätze eines Strukturwandels der Öffentlichkeit? In Andreas Hepp and Martin Löffelholz (Eds.), *Grundlagentexte zur transkulturellen Kommunikation* (pp. 500-530). Konstanz: UVK-Verl.-Ges.
5. Dauterman, Walter C. Jr. (2002). Internet Regulation: Foreign Actors and Local Harms – at the Crossroads of Pornography, Hate Speech, and Freedom of Expression. *North Carolina Journal of International Law and Commercial Regulation*, 28, 177.
6. Geist, Michael (2001). Is There a There There? Toward Greater Certainty for Internet Jurisdiction. *Berkeley Technology Law Journal*, 16, 1345-1407.
7. Goldsmith, Jack (1998). Against Cyberanarchy. *University of Chicago Law Review*, 65, 1199.
8. Goldsmith, Jack (2000). Unilateral Regulation of the Internet: A Modest Defence. *European Journal of International Law*, 11, 135-148.
9. Kerr, Orin S. (2003). The Problem of Perspective in Internet Law, *Georgetown Law Journal*, 91, 357-405.
10. Köhler, Markus; Arnd, Hans-Wolfgang (2000). *Recht des Internet.* Heidelberg: Müller.
11. Lessig, Lawrence (1999). *Code and Other Laws of Cyberspace*. New York: Basic Books.
12. Shenk, David (1997). *Data Smog: Surviving the Information Glut*. London: Abacus.
13. Spencer, Benjamin A. (2006). Jurisdiction and the Internet: Returning to Traditional Principles to Analyze Network-Mediated Contacts, *University of Illinois Law Review*, 44. As retrieved February 2006 from http://ssrn.com/abstract=706629.
14. Strossen, Nadine (2000). In Jens Waltermann (Ed.), *Verantwortung im Internet: Selbstregulierung und Jugendschutz* (pp. 120-129). Gütersloh: Verl. Bertelsmann-Stiftung.
15. Swire, Peter P. (1998). Of Elephants, Mice, and Privacy: International Choice of Law and the Internet. Retrieved February 2006 from http://ssrn.com/abstract=121277.

16. Swire, Peter P. (2005). Choice Of Law And Jurisdiction On The Internet: Elephants And Mice Revisited: Law And Choice Of Law On The Internet. *University of Pennsylvania Law Review*, 153, 1975-2001.
17. Van Houweling, Molly S. (2003). Enforcement of Foreign Judgments, The First Amendment, And Internet Speech: Notes for the Next Yahoo! v. Licra. *Michigan Journal of International Law*, 24, 697-717.
18. Watt, Horatia Muir (2003). Yahoo! Cyber-Collision of Cultures: Who Regulates? *Michigan Journal of International Law*, 24, 673-696.
19. Weiser, Philip J. (2003). The Internet, Innovation, and Intellectual Property Policy. *Columbia Law Review*, 103, 534-613.
20. Zittrain, Jonathan (2003a). Be Careful What You Ask For: Reconciling a Global Internet and Local Law, in *Who Rules the Net*. As retrieved February 2006 from http://ssrn.com/abstract=395300.
21. Zittrain, Jonathan (2003b). Internet Points of Control, *Boston College Law Review*, 44, 653-688.
22. Zittrain, Jonathan (2006). The Generative Internet. *Harvard Law Review*. As retrieved February 2006 from http://ssrn.com/abstract=847124.