Webology, Volume 11, Number 2, December, 2014

Exploring into regulatory mode for social order in cyberspace

Xingan Li

LLD, PhD, Associate Professor, Tallinn University Law School, Narva 29, 10120 Tallinn, Estonia.
E-mail: xingan.li (at) yahoo.com

Received October 26, 2014; Accepted December 22, 2014

Abstract

An increasing necessity for building social order in cyberspace through legal instruments has existed as one of many alternatives to regulate the world dominated by the globally connected Internet. This article discusses legal gaps of cyber-laws among different localities, with special regards to regulation over Internet content, through an approach with emphasis on players in three different steps of data movement that are separately characterized by human-machine, machine-machine and machine-human interaction with different degrees of human intervention. From the features of each stage, it is concluded that official action must be within the ability of the controller so that it can be effective, and that it must also cope with the utility of the controller so that it can be efficient, so that an ability-and-utility-oriented control mode would ideally functions.

Keywords

Social order in cyberspace; Regulation over cyberspace; Ability-and-utility-oriented control (AUOC); Steps in data movement

---

Introduction

Information and communications technologies (ICTs) come from and have significant impact on the global society. Many human activities with functions and patterns different from that of traditional society have been facilitated by the globally connected computer networks. Previous ethical and legal discourses are undergoing serious challenge from newly emerged cyber-semantics. If we are going to set a limit between meanings of cyber- and traditional activities, there can be found some clearly defined, however controversial, characteristics. The conundrum happens when organisers of society have the same interests in guaranteeing the successful expansion of their immanent regulatory instruments from traditional society into cyberspace without a loss in enjoying their

existing power. Nothing would be tolerated in case it is simply an activity that takes place in cyberspace, other characters being the same as that in the meat space. We can perceive some particular cases as exceptions; however, they can only be seen as exceptions to the mainstream tendency. It could be well expected that online behaviours would have no more difference from their offline counterpart in respects of getting regulatory results.

For some time, cyberspace enjoyed some extent of contentment from evading regulation as stringent as on the traditional society. A variety of negative effects emerged and countries have growing eagerness to contain activities in cyberspace into their jurisdictions. Nevertheless, a string of impediments deferred the process of integrating online and offline "activities". All countries are territorial-dependent, and no on single country has ever had claimed global control over all humans in the world, with rare exceptional situations where some countries extended their jurisdictions beyond their territories by domestic legal acts or according to international agreements. The networks-facilitated cyberspace has a virtually global reach in the sense of spatial concept, exactly going beyond single countries and in a certain sense incurring the ardour of countries to exercise control over it by one ultimate entity: a country, or an institution. However, it has never come true that a universal jurisdiction principle is accepted as a general rule in either meat space or cyberspace. Academia, legislature, and law enforcement agencies have all been devoted themselves to harmonising domestic laws or meliorating international laws in order that they are applicable to cyberspace in conformity with meat space.

Furthermore, cyber-activities have innovative players, processes, and objects. The new players are netizens hooked online through wire and wireless links, acting through transmitting digitalised information, and influencing status of objects without physical appearance in person. The identity of the players can effortlessly be concealed, the trace of their activities be eliminated, with their locality impossible to be spotted. Adding to these complexities are perplexities that even if they are identified they can still be involved in legal controversies, either that their activities regarded as legal by one country are denounced in another country, or vice versa.

We expect that the core arguments in this article concerning the approach to online content can also be useful in dealing with other online legal questions, such as unauthorised access to information systems, piracy of intellectual property, fraudulent schemes, destruction of data, defacement of websites, dissemination of malicious programmes and so forth. All these online activities with negative social evaluations have generalities in common, even though there are also many particularities. That is because of similar extent of social evaluations on these obnoxious activities that make countries to motivate their legal instruments to tackle them. Of these activities, online content has been one of the most controversial issues, over which many countries make efforts to exercise control. From the point of view of regulators, it is an urgent task to discover a route for installing previous rules in cyberspace regulation.

In determining the optimal selection from a variety of regulatory alternatives based on national orientation in cyberspace, we should first examine advantages and disadvantages of each option and reason which one has the highest meritoriousness capable of dealing with jurisdictional effectiveness and pecuniary efficiency.

Structure of the reasoning

Regulation of cyberspace has attracted great attention from academia since late 1990s. Many people have invoked laws of different countries for or against regulation of cyberspace. Therefore, there have been significantly different standpoints concerning whether cyberspace should be regulated, and if we give a positive answer, to what extent it should be regulated. In particular, online content may be the most controversial respects of such a disputation. In the U.S., for example, freedom of speech has been established on a firm constitutional foundation through its First Amendment. Oftentimes it has been interpreted in a broader way than many (if not any) of free speech provisions in the world. In China, for another example, both governmental and civil views, which usually distinguish between content considered legal or ethical and content considered illegal or unethical, are in favour of some kinds of regulation over online content (Fallows 2008). Even though people from the U.S. may assume that control of the Internet in China might be a discontented experience, majority of Chinese netizens seem not so resistant to such a way of control (ibid.). This fact indicates that different attitudes do not obstruct us from discussing ways of control.

This discussion is based on the assumption that some kind of regulation over cyberspace should be imposed, regardless of the extent to which such a regulation should be. Lessig's code approach (Lessig 1999) has (over)stated the role of code as a potential regulator (a subject, or a tool?). Kerr's perspectives approach (Kerr 2003) attempted to bridge the gap of understanding between cyberlegal problems and conflicts between internal and external perspectives. Weiser's competitive platforms approach (Weiser 2003) assigned each of cyber processes to a certain layer. Rather than calling them layers, I would simplify these aspects as nodes that comprising the whole chain of data movement. In practice, some others also mentioned different stages of data movement, such as Zittrain (2003), who divided the process into five stages: from source, to source ISP, to cloud, to destination ISP, and to destination. However, my typology would consider not only stages of data movement but also intervention of human elements with mechanical transmission and processing. In so doing, data movement will be considered as beginning with human intervention with mechanical transmission, without which no data can be input and no command can be sent for data processing and transmission. In this step, human intervention is a necessity for commencing the data movement through human-machine interaction. It is the human entity at the starting point of the run initiates the whole process, whatever the effect will take place. Subsequently, data movement will be realized in a step when human intervention is not a prerequisite but it can still be possible that human intervention is involved. This step is symbolised by machine-machine interaction, with or without human intervention. The third and last step ends with machine-human interaction that has impact on human entity at the destination. Here we use the term step instead of period, phase or stage by considering that the duration of the process of data movement is rather short, and that the beginning and the ending of the process are more like two temporal points than two periods. The only longer duration happens in between these two ends, that is, the movement itself, which is also rather rapid and instantaneous. People use such term as "synchronal," "synchronic," "synchronous," or "synchronized" to describe such a situation. Thus we establish a typology including three distinct steps in data movement: human-machine interaction step (HMIS), machine-machine interaction step (MMIS), and machine-human interaction step (MHIS).

Control at human-machine interaction step (HMIS)

Humans always predominate data movement. But humans also play different roles in data movement from the beginning users through deposition, hosting, transmission, and processing by machine to the end users. At human-machine interaction step of data movement, human acts more predominately than in other steps. It is these activities with predominate nature that primarily determine the human involvements at other steps, let alone mechanical involvements and human-machine interaction.

As far as online content is concerned, players at this step include online content authoring parties (OCAPs) and online service providing parties. OCAPs are those both individual and institutional users who write, create, demonstrate, perform, record, upload, review, publish, distribute, disseminate, propagate, lease, lend, sell by wholesaling or retailing, or have the content to enter the movement process by other means so that it can reach other users. Apparently, players at human-machine interaction step act more actively in putting data online. Besides authoring parties, online service providing parties are also involved in the initiation of this process by accommodating movement of content-related data.

Eliminating incentive of OCAPs may be the most effective option to exercise control over online content. If and only if potential authoring parties could no longer benefit, either financially or spiritually, from authoring, online content would no longer be authored. Thus the most effective control begins with control over authors. However, this effectiveness can not directly be translated into efficiency due to the geographical distribution of global users. Authorities are simply confronted with jurisdictional limits based on international political borders. Law enforcement is still operated in a rather conventional way that is reluctant to positively face jurisdictional conflicts, which is deepened by ideological, political, ethical, legal, procedural, methodological, and technical conflicts. As a result, to discourage authoring parties by various possible ways become an unfavourable idea.

Yet worse, once motivated authoring parties upload the content online, it is published to a media with a global audience and delivered on a nearly hybridly regulated platform. Even if the purpose of regulation is not for penalty itself, once spread, online publications can not simply be removed thoroughly. The existence and dissemination of such content become an eternal digital movement.

Now we have to turn to Internet service providing parties (ISPPs) who have certain ability to control data movement, even though their functions are originally not limited to do so. ISPPs may be immune from any liability in many situations, but they are imposed some kind of liability in some other situations. If we stop at discussing this issue only at the layer where ISPPs are supposed liable, it is a typical *mala prohibita* if ISPPs are imposed liability for their failure in fulfilling responsibilities that authorities would possibly assign to them. Because they are located in a condition where it is more possible to exercise control over online content authored by others, to assign them certain responsibilities, failing to fulfil which will be punished, is economically and judicially a more efficient way than attempting to prosecute authoring parties that are jurisdictionally impossible to prosecute.

ISPPs are usually more established, more organized and more centralized entities than authoring parties. They are more likely to act anonymously than single individuals and institutions. They are also likely to operate with more stable localities. These characteristics render ISPPs a status that the regulators can use to remove unfeasible content and even launch legal actions against ISPPs themselves.

ISPPs are not only passive in accepting authoritative commands, but they can actively exercise control over content within the scope of their services. For example, they have the capacity to take measures to direct content to where it is acceptable and avoid directing them to where it is unacceptable. In other words, ISPPs have much say on data movement: whether data move, when data move, where data move, or to whom data move. Thus, control over OCAPs can well be translated into control over ISPPs.

Control at machine-human interaction step (MHIS)

Online content consuming parties (OCCPs) are end users of data movement in the case of content-related transmission. They have both similarities with and differences from OCAPs in data movement. While OCAPs start up the process of data movement, OCCPs put the process of data movement to an end, ending in consuming: either downloading, reading, watching, listening, using, enjoying, borrowing, renting, redistributing, re-disseminating, or re-propagating, but mainly for their own consumption. Even though OCCPs as end users engage in passive acceptance and active mining of online content products (OCPs), their activities are passive in nature. If there is no online content existing for their consumption, these end users could never reach such OCPs in online content market (OCM). Thus it is a reasonable option for interest authorities to restrain their impulse to exercise control over activities of OCCPs. In particular, authorities of one country reluctantly have the motivation for impose certain liability on OCCPs in another country. Territorial jurisdiction stops before the borderline between countries.

It has never been a good idea to exercise jurisdiction on persons living in other political entities. The computer networks did not change the traditional concept much. Even if some people attempted to broaden the understanding of authoring activities to the extent that it covered the actual activities of reconstructing digits into complete files through downloading, viewing, browsing, retrieving and saving in magnetic media, they are increasingly put to an unfeasible place serving as the synonyms of “authoring” or “possession”. The applicability of rules against possessing or authoring such online content cannot be uncontroversially justified. Otherwise, to control individual and institutional OCCPs is confronted with the virtually same predicament as in the case of OCAPs: they are just similarly distributed in a geographically global space and control would be inefficient and ineffective. Morally or legal preventing such contents usually give place to technical measures, which are gradually invented to arm authorities all over the world to filter content that they separately classify as objectionable according to their own standards.

It happens that it is difficult for authorities to directly regulate each and every OCCP, and that there are also nodes directly serving end users. That is those nodes that have to take responsibility for controlling activities of OCCPs and those who fail to do so would be held liable for the

unfavourable consumptive activities involving retrieving of objectionable online content. Similar to ISPPs at the starting point of data movement, ISPPs at the end point of data movement also become the targets of authoritative regulation, for the sake of efficiency and effectiveness. ISPPs are neither end users nor regulators, but become controllers of end users and controlled by authorities. That's why ISPPs are usually not willing to orientate themselves as located in between end users and law enforcement.

Control at machine-machine interaction step (MMIS)

Control over activities of start uses and that of end users in the chain of data movement with special regard to online content market proves problematic. Extended control over ISPPs that are adjacent to star and end users can partly be justified. Because there are altogether three steps in the process of data movement, we must now clarify the controllability of the interstitial step.

Quite a lot of players live on digitally linking start and end users. At this step, human elements are automatically played down by deep involvement of technological and technical solutions. Technologically, portals and search engines attract and facilitate users to harvest online content. There have technological means to provide some kinds of options for data movement. Obviously, machine-machine interaction is in practise dependent on regulatory direction from humans, who receive another level of regulatory direction from authorities.

The possibility of human intervention through technological and technical measures at the step of machine-machine interaction of data movement does not automatically mean that it is easy for portals and search engines to filter and prevent large quantity of moving data. In fact, imposing liability for omission to filter and prevent objectionable online content would be less efficient and effective than imposing liability for commission to providing hyper links. This is exactly where the responsibility and liability should be positioned. Creating an incentive for human interveners to bear a burden for doing something extra would not work better than creating an incentive for them not to do something unfavourable. To move somebody doing something extra beyond their duty while no compensation is provided, she/he would manifest some kind of inertness in reaction. In case of punishing somebody for doing something objectionable from the point of view of government, she/he would present a higher degree of coordination. Purpose of regulation is just located in coordination but not punishment. In designing a mechanism to subject human elements to coordinative data movement, OCM would be operated following its orbit of economic utility. In sum, human interveners at the machine-machine interaction step have certain degree of ability to exercise control over data movement by bearing additional of filtering and preventing data but have less utility to do so. On the contrary, they would have both ability and incentive to exercise control by not providing access opportunities for certain data.

Ability-and-utility-oriented control (AUOC)

Our analysis on regulation and control at different steps of data movement reveals that the official action must be within the ability of the controller so that it can be effective, and that it must be also out of utility of the controller so that it can be efficient. On the contrary of this conclusion is that

control by controllers without ability will be ineffective, while control by controllers without utility will be inefficient. Only control by controllers with both ability and utility will be effective and efficient. Based on this principle, only local authorities who fall in the same jurisdiction as where players who play negatively are located may actually exercise control over relevant step or steps of data movement. Those authorities without interest in affairs that players play negatively are monetarily discouraged from exercising control.

The logic in online content market is that, those who are able to exercise certain extent of control, who are assigned the responsibility for control and who fail to exercise due control would be held liable. These players seem to play in a broad "online" ground. However, when responsibilities are assigned to players, they do not simply mean to do something in favour of authorities. On the contrary, they sometimes simply mean not to do something unfavourable to the authorities or society. In other words, omission is not taken into account when liability is imposed, but commission renders the players into perfect liable status if such commission leads to data movement that disseminates objectionable content to OCCPs, who without such commission would not have access to such content, or who without such commission would have less numerous, frequent, or convenient access to such content.

However, ability is a must in considering to whom the responsibility should be assigned. To assign responsibility to players in a status unable to fulfil, would make it morally unjustifiable to hold them liable in law enforcement stage.

Control over online content market has to be exercised in a way balance ability and utility of concerned players. Ability only or utility only is a vacuous design of regulatory framework. Taking both of them into consideration would avoid dilemmas in justification, and efficiency and effectiveness.

Control over online content is neither designed to exclude as much users from the OCM, nor to prevent as much users from the beneficial consumption of content. Utility is a must in considering mechanism for control. To assign responsibility to players in a status unbeneficial, would make it economically inadvertent to move them fulfil their responsibility.

Conclusion

Because traditional spatial divide between jurisdictions has almost been precisely transplanted into cyber-laws, legal gaps of cyber-laws among different localities survived. This paper explored a control model, that is, ability-and-utility-oriented control, with special regards to regulation over Internet content, through an approach with emphasis on players in three different steps of data movement that are separately characterized by human-machine, machine-machine and machine-human interaction with different degrees of human intervention. According to this mode, the official action must be within the ability of the controller so that it can be effective, and that it must be also out of utility of the controller so that it can be efficient. Therefore, the nature of ability-oriented control and utility-oriented control can be and must be combined so that the best outcome can be expected.

Endnote

Ideas in this paper were developed over the years. An early version of this paper was published in a book entitled "*Social Order in Cyberspace*", Amicus Law Books Division, ICFAI University, India, 2009. The book was printed in a small run and generally unavailable to external readers. This version of the paper, updated and revised, is to bring the ideas to a broader audience.

References

Fallows, D. (2008). *Few in China complain about Internet controls*. March 27. Retrieved December 2014, from http://www.pewtrusts.org/en/research-and-analysis/reports/2008/03/27/few-in-china-complain-about-internet-controls

Kerr, O.S. (2003). The problem of perspective in Internet law. *Georgetown Law Journal*, 91 (February), 357-405.

Lessig, L. (1999). *Code and other laws of cyberspace*. New York: Basic Books.

Weiser, P.J. (2003). The Internet, innovation, and intellectual property policy. *Columbia Law Review*, Vol. 103, pp. 534-613.

Zittrain, J. (2003). Internet points of control. *Boston College Law Review*, 44(2), 653-688.

Bibliographic information of this paper for citing:

Li, Xingan (2014). "Exploring into regulatory mode for social order in cyberspace." *Webology*, 11(2), Article 125. Available at: http://www.webology.org/2014/v11n2/a125.pdf