XX THE FOOTPRINT OF REGULATION

How information systems are affecting the sources of control in a global economy

Prodromos Tsiavos, Ian Hosein and Edgar A. Whitley
Department of Information Systems
London School of Economics and Political Science
Houghton Street, London WC2A 2AE, United Kingdom
E–mail: P.Tsiavos@lse.ac.uk
Web page: http://is.lse.ac.uk

Abstract
Whilst the issue of jurisdiction—the question of how far control extends—has always been controversial, the introduction of information and communications technologies only exacerbates the problem. The first generation of scholars to consider this question tended to see technology creating a separate space—cyberspace—with its own *legal* boundaries. A second generation of scholars, however, has argued that there is nothing new with cyberspace and that conflicts over boundaries have always existed in the law; as a result, they argue that technology is not as remarkable a factor as the first generation believe. By considering the case of copyright and peer–to–peer technologies together with the regulatory environments surrounding their development, use and control, this paper proposes a further refinement in the dialectics of control through technology that refines our notions of jurisdiction in an era of globalisation enabled by new technologies.

INTRODUCTION

The bursting of economic bubbles and the emphasis upon global security has given rise to a new form of scepticism regarding technology and society. It is common nowadays to dismiss previous technologically–optimistic claims regarding the information society. Whereas earlier it was claimed that "no one knows who or where you are on the internet" (Turkle 1996), or "governments are powerless to regulate global networks" (Angell 2000) such views are now considered by many to be unrealistic, or worse, deterministic. Indeed, it is now claimed that regulating data flows is no different than regulating other activities.

Deciding which of these views holds has important implications for understanding the developing nature of globalization and the ways in which information and communications technologies may be shaping the globalization debate. The future is likely to be very different if governments have (or believe that they have) the sovereignty to act than if they don't. This principle of sovereignty is often summarised as the "government's exclusive power within its borders and virtually nowhere else" (Leeds 1998 p. 6–7).

The jurisdiction of regulation and control, regardless of what is being regulated, has a particular domain of application. For instance, when referring to the regulation of copyrighted material by the UK Copyright Act 1988, its domain would be the geographical area and the natural and legal persons on which it may be enforced. Video rental records privacy laws in the United States specify a specific geographical area. The domain is sometimes even more limited than geography; the jurisdiction of U.S. privacy protection regulatory regimes include video rental records, but does not include electronic commerce conduct. The domain of regulation constitutes the **footprint** of each regulatory form and often is found to have the same meaning as the term jurisdiction. There is a series of diverse definitions regarding what is and what is not jurisdiction, but for the time being this paper will refer to the term jurisdiction as having the same notion as the application domain of a set of regulations. We note that many of the examples cited in this paper draw on cases in Western legal systems, this is primarily because other than censorship, these issues have not yet arisen in many non-Western contexts. Similarly, the developing nature of these issues in relation to new technologies means that no transnational structures exist, as yet, to address them.

Jurisdiction has been traditionally linked with the concept of the state since the latter has been the institutional mechanism supporting and cultivating the main regulatory mechanisms of the modern society. The globalization debate, (see for example, Avgerou (2002) (Beck 2000) (Walsham 2000)), however, has highlighted that the arbitrary physical boundaries of countries are becoming increasingly irrelevant to the global world.

One useful articulation of this argument is given by Ulrich Beck who argues that we have entered "a second modernity". He defines the first modernity as being based on the assumption that *"we live and act in the self–enclosed spaces of national states and their respective national societies"* (2000 p. 20 emphasis in original) and suggests that this assumption no longer holds in an era of globalism.

That is, our actions are no longer restricted to the self–enclosed spaces where they take place. Rather our new global connections mean that things as diverse as "money, technologies, commodities, information and toxins 'cross' frontiers as if they did not exist. Even things, people and ideas that governments would like to keep out (for example, drugs, illegal immigrants

or criticisms of human rights abuses) find their way into new territories" (p. 20). In the global economy of the second modernity it does not make sense to speak only of 'national' effects; any actions can only sensibly be considered in terms of their global effects, even if the immediate effects might appear to be fairly localised.

As a result, "nothing which happens on our planet is only a limited local event; all inventions, victories and catastrophes affect the whole world, and we must reorient and reorganize our lives and actions, our organizations and institutions, along a 'local–global' axis" (p. 11–12).

This globalization debate, therefore suggests that regulation as a source of control is not limited to the State. Coupled with this, since the 1960s, the Chicago School of Regulation and Economics has been arguing that norms and markets are also sources of regulatory control. Each has different effects on jurisdiction. Markets are increasingly globalized, bringing with them a form of regulation that is not necessarily state–sponsored; the same may be said for norms.

This broader conceptualisation of regulation and its impacts on jurisdiction in a global environment are considered further below. First, however, the paper presents the two major ways in which the regulation of cyberspace has been considered.

TECHNOLOGY AND CONTROL OF CYBERSPACE: TWO VIEWS

The international regulatory environment has been of interest to a number of scholars as they studied the control of "cyberspace" or "the Net". The views and findings of these scholars may be divided into two generations.

First generation: Staking out a new place

The first generation of scholars argued that under traditional notions of sovereignty and jurisdiction, governments relied on borders to enable their power, give effects to their rules, create legitimacy to their enaction, and notice to those who were regulated. Jurisdiction was therefore essential to regulation; but over computer networks, this was challenged.

Johnson and Post (1996) argued that

> (M)any of the jurisdictional and substantive quandaries raised by border–crossing electronic communications could be resolved by one simple principle: conceiving of Cyberspace as a distinct "place" for purposes of legal analysis by recognizing a legally significant border between Cyberspace and the "real world".

In effect, they were making both descriptive and normative arguments (Goldsmith 1998a). First, their claim was that applying regulation limited by geographic–borders to an a–geographic–border environment would be senseless. This claim for a new space for cyberspace was famously developed by John Perry Barlow in his "Declaration of the independence of cyberspace" (Barlow 1996) which asked "On behalf of the future" to be left alone by those of the past as they "have no sovereignty where we gather" (Barlow 1996).

Second, they claimed that regulation by one jurisdiction would have spillovers immediately upon another because of the a-geographic–border nature of cyberspace. If one country decided that the internet was to be in their jurisdiction, then the rules dictated by this country would affect the entire internet. For example German hate speech laws could have a chilling effect on the willingness of service providers worldwide to host controversial content.

Second generation: Reclaiming the space

The second generation of scholars, however, regard this view as promoted by "regulation–sceptics" who exaggerate the problems of regulating cyberspace and ignore how similar it is to older forms of regulation and infrastructure (Goldsmith 1998b c.1130).

The critique is that cyberspace transactions are not all that different from transnational transactions, in that they both involve people in "real space" in different territorial jurisdictions causing "real–world" actions and effects.

Most "cyberspace" issues, therefore, have real–space analogies. According to Goldsmith, data havens may be created in the same way that tax havens may in the real world. Conflicts of law will occur in cyberspace the same way as they occur regularly in real–space; and the response to the real–space problem in the past has been international harmonization strategies. The feasibility of regulation will thus increase as the practices become more common in various jurisdictions, and once knowledge of laws in other jurisdictions grow and experiences are shared (Perrit 1996).

The second generation argues that the changes in transportation and communications technologies of modernity have made multi–jurisdictional activity more common. International law permits States to "apply its law to extraterritorial behavior with substantial local effects"; that is "in modern times a transaction can legitimately be regulated by the jurisdiction where the transaction occurs, the jurisdictions where significant effects of the transaction are felt, and the jurisdictions where the parties burdened by the regulation are from" (Goldsmith 1998a c.1207). That this is happening with the internet and global data flows, to these thinkers, is just more of the same.

As a result countries have been establishing regulation of data flows. The European Union finalised a harmonizing directive on data protection in 1995 that included two articles regulating transborder data flows (European Union 1995). Countries as diverse as Australia (Australian Broadcasting Authority 1999), China (BBC news 2002a), and Saudi Arabia (Lee 2001) have implemented censorship regulations to control the kind of information that was sent, received, or both (cf. (Rapporteurs sans Frontieres 1999)); despite claims of infeasibilities and inaccuracies (cf. (Clarke 1999; Dogcow 1999; Electronic Privacy Information Center 1997)). In 2000, a French court decided that Yahoo! was obliged to prevent French users from accessing material on Yahoo!'s sites that were illegal according to French law. This was done despite the fact that the servers and services were in the United States (Akdeniz 2001), and technological arguments about the infeasibility of implementing the ruling and legal claims about the jurisdiction of the French courts.

The changing nature of technology also affects the ability to regulate a technological infrastructure. However, the regulation literature notes that *every* new technology can be seen to disrupt existing regulatory regimes, not just computing technologies. For example, Peltzman includes "changes in the 'politics' and changes in the 'economics' of the regulated industries" as factors that alter regulatory regimes, adding that political change also comes from "changes in the underlying organization and information technologies" (Peltzman 1989 p.108).

While this second generation argues that technological change is not that big a deal, this paper contends that ignoring the constitution of technology may lead to problems in understanding regulation and jurisdiction.

There may be value in investigating the details of how technology changes regulation; or how technology enforces regulations, and other such interactions between technology and regulation. Then it is possible to have a deeper appreciation of how technology and jurisdiction interact.

A THIRD GENERATION UNDERSTANDING

Whilst the first generation argument perhaps placed too much emphasis on technological issues, the second generation places too much emphasis on how the environment is similar to previous practices, technologies, infrastructures and laws. A third generation argument has recently evolved that seeks to combine an appreciation of the role of technology in changing the regulatory habitat (Hood 1994) whilst also allowing for the ongoing evolution of established legal practices.

Drawing on the Chicago School of Regulation which argues that markets and norms, together with laws play a role in controlling action, Laurence Lessig has also used ideas from Bentham and Foucault to include architecture

(Lessig 1998) and and more particularly code / technology (Lessig 1999) as other modalities of regulation. In his proposal for a New Chicago School, Lessig warns that it is necessary to look to how code or technological architectures are also capable of regulating human action. His model incorporates all these elements as modes of regulation.

The third generation understanding therefore acknowledges both the new practices enabled by technology and the role of existing laws (and markets and norms) in regulating behaviour. In the next section the paper considers how a third generation understanding can be used to analyse peer–to–peer networks and copyright before coming back, in the concluding discussion to review the impacts of this understanding for our views of effects of technology on regulation and the globalisation more generally.

CASE: COPYRIGHT, NAPSTER AND PEER–TO–PEER SYSTEMS

"Copyright means many things to many people"

The aphorism, which Sterling uses as an introductory phrase for his "World Copyright Law" (1998), reflects in a very eloquent way the idiosyncratic—if not protean—nature of copyright. Copyright affects people in a multitude of different ways and thus it becomes a myriad of different things for them.

In the past few years, MP3 files, services like Napster and peer–to–peer networks more generally were seen by many as the latest and perhaps the most significant challenges to the copyright status quo. The small file sizes of MP3 files that allowed near CD quality music to be searched for and downloaded quickly from all over the internet were leading to an order of magnitude increase in the problems of the copyright management industry.

Throughout its history copyright has tended to be used to protect the interests of the content disseminators rather than those of the content creators. This does not mean that the interests of the creators or the consumers of intellectual creations were not protected; it is just that the mapping of the interests was much more in favour of the disseminators and other intermediaries than anyone else. The only case where such a situation is reversed is that of the authors' collecting societies, especially those of continental Europe and Germany in particular (Sterling 1998), although again the collecting societies are intermediaries. This is due to both the content and structure of copyright and author's right laws, and the way these laws are constructed. In the terms of content, almost all the rights granted to a creator can be—and are—transferred to intermediaries that vary from a disseminator, such as a music label, to a collecting society or a software house. In terms of structure, copyright laws have been built based on the assumption of a

hierarchical system of distribution where the points of original dissemination are controlled.

In the digital version of copyright laws, especially as it has been manifested in the DMCA or the European Copyright directive, the control becomes even more stringent, with copyright being transformed into an access–right. In terms of the way copyright laws are created, it seems that content disseminators or intermediaries of all kinds have a much stronger lobbying presence than consumers or creators. This becomes increasingly apparent after the mid 1990s, when there has been a realisation of the potential of digital dissemination.

Napster and peer–to–peer file sharing

In May 1999 Shawn Fanning, an undergraduate student at Northeastern University, created an application called Napster. The idea behind Fanning's software was to enable end–users to share the MP3 files stored in their computers, using a centralised indexing service to locate the files. Two years after its launch, Napster had experienced an exponential growth to reach an audience of over fifty million users. Napster's popularity resulted in a lengthy legal battle between the music industry and Fanning's newly founded company on issues of copyright infringement (Alderman 2001).

Most of the peer–to–peer services have been entangled in legal disputes with the media industries. Napster was sued in 1999 and a shortly thereafter Scour faced a very similar fate (Alderman 2001). Both companies had to suspend services (from July 2001 and December 2000 respectively). In the midst of a series of legal developments and extensive media hype, the Recording Industry Association of America (RIAA) and Motion Picture Association of America (MPAA) have also gone after a number of other peer–to–peer services based on the most advanced peer–to–peer technology available at the time: that provided by FastTrack. Morpheus, KaZaA, Xolox and Grokster have been the targets of the media industry both in the U.S. and in The Netherlands. Xolox was shut down in the process only to open some months later when the case against FastTrack in The Netherlands was resolved in favour of the technology company. Morhpeus and KaZaA have survived to become two of the most widespread file–sharing applications.

ANALYSIS

In order to understand these developments, this paper will use the third generation understanding and, in particular, Lessig's four modalities of regulation: markets, laws, norms and technology. These will be used to show

the different ways in which the audio–visual industry has sought to address the threat to copyright from peer–to–peer networks.

Markets The main strategy of the content industry up to now for dealing with the copyright problems offered by Napster and peer–to–peer networks has been to identify bottlenecks of control and then charge them with contributory, vicarious or wholesale infringement of copyright, thus directly impacting the 'market' for such files. This is a tactic that makes sense, especially in terms of copyright law, since the latter is structured in such a way that it encourages the monitoring of the content users by the content distributors through liability clauses. Copyright law is structured on the assumption that the distribution of copyrighted material happens in a more or less centralised and therefore more or less controllable way: if the bottlenecks can be controlled then the end users can be controlled. RIAA and MPAA have followed a variety of methods for controlling bottlenecks, from high profile lawsuits against peer–to–peer services to recommendations to colleges and universities, where much file sharing is happening, accompanied by warnings that if no measures are taken in due time, legal action would follow. Prominent examples include that of Carnegie Mellon University in Pittsburgh, where in late 1999 seventy–one students were disciplined for the illegal use of MP3 files on the University's intranet (Wired News 1999b).

Laws Another approach for the copyright holders is to sue directly the infringers, i.e. the end users. This approach has some inherent problems since it is problematic for a company to start suing its own actual and potential customers. This was manifested in the Levy case. Geffrey Gerard Levy was a student at the University of Oregon and was prosecuted under the No Electronic Theft (NET) Act v1997 for illegally distributing MP3 files as well as pirated software and clips from theatrical movies (Wired News 1999a). He was reported by network administrators at the University of Oregon. Despite its success in legal terms, the Levy case has proven to be a public relations disaster for the audio–visual industry and it does not appear to have deterred any users from file–sharing practices. The content industry has repeatedly leaked to the press its intentions to go after the file–swappers themselves. It has also been the case that internet service providers have addressed e–mails to their customers asking them to stop sharing certain files under the penalty of having their accounts terminated.

Norms The litigation instigated by the audio–visual industry have been supplemented by a series of awareness initiatives, but these have tended to have limited success. For instance, in October 2001 the Disney Channel aired an episode of the Proud Family, a cartoon series aimed at the pre–teen audience, where the heroine Penny Proud realises the dark side of file–trading after she has been threatened with arrest by the police, been deprived of her computer and found that her local store had gone out of business (Wired News 2001). It would, however, be quite na?ve to believe that an industry that has been based on the production of content that emphasizes

anti–conformism and rebellion could manage to pass the message of compliance as easily as some of the top executives would like it to happen. "Homer's gaffe" (whereby the UK website for the Simpsons briefly gave advice on how users could circumvent the technological measures that limit where the DVDs could be played (BBC news 2002b)) is only the latest in a series of self–conflicting practices that the media industry has followed.

Technology Other strategies that the audio–visual industry has adopted include the development and evolution of Digital Rights Management (DRM) systems for the protection of their content. Despite the enthusiasm that followed the introduction of DRMs as an alternative way to protect content, it has become increasingly apparent that the very construction of DRMs has been their main problem. Most of the existing DRMs impose restrictions on the way the users experience music either in terms of the time(s) they can listen to a track, or the players they can use to listen to it or in terms of the portability of the files. The existing distribution systems used can match neither the ease of use nor the variety of content that the peer–to–peer services provide their users with. Nevertheless research on DRMs continues and is still seen as one of the possible solutions to the peer–to–peer "problem". Most of the last generation file–sharing networks allow the display of information concerning the files being shared to help users in their searching and this could be seen as a form of DRM forerunner. Files distributed by EMI's 2Ksound music label can be found over the KaZaA network and this has been used as an argument for supporting the distribution of music files with DRMs over peer–to–peer networks.

All these developments happen in the footprint of the U.S. Digital Millennium Copyright Act that contains provisions supporting technical measures of protection and under the debate concerning the proposed Security Systems Standards and Certification (SSSC) Act, which would make it a civil offence to sell or create any kind of computer equipment that "does not include and utilize certified security technologies" approved by the federal government.

Providing safe harbours: where technology and jurisdiction interact

Despite their multi–level nature, the efforts of the audio–visual industry to combat the file–sharing phenomenon have not been met with particular success. Following a trajectory of increasingly stricter measures and after having exhausted legal, technical and audience–shaping methods, the copyright holders have to find refuge in other kinds of measures. These are called "self-help measures" by their proponents and "hacking" by their opponents.

This solution has been advocated by Congressman H. L. Berman and is based on the idea of allowing a safe–harbour status for copyright holders when trying to protect their content even if in the course of their attempts they are committing acts including "interdiction, decoy, redirection, file-blocking, and spoofing" (Berman 2002) (CEI 2002).

DISCUSSION: RECONCEPTUALISING JURISDICTION: GLOBALISATION, REGULATION AND TECHNOLOGY

The third generation approach supports the presence of multiple modalities of regulation, including norms, markets, and technologies. Law is merely one form of regulation that is subject to national jurisdiction, and sometimes even more limited than that. Norms and markets are increasingly global; while technology may be used across borders. In this sense, any given user is subjected to a number of regulatory jurisdictions at a given time and information and communication technologies only increase this diversity.

There are two main implications for this approach. The first is the mixing of modalities that subject the user to greater control and possibly coercion, with decreased accountability. The second is the notion of regulatory patching that may indeed grant the user some autonomy. These are then combined in the notion of the commodification of regulation (Romano 1985).

Mixing modalities

As there are multiple sources of regulation, each may establish jurisdiction over the user. The sources of regulation also intermix with each other. Laws are created to shape technology. As discussed above, DRM technologies are protected in the U.S. by the DMCA.; if you reverse–engineer the protections within a DRM technology you are in contravention of U.S. law, regardless of whether under traditional copyright laws you are permitted to access the protected data. National laws and policies that dictate the form and structure of information technology are interpreted and embedded within a technological solution, and when this solution is used world–wide, it carries the politics of its creation: in effect, it enforces foreign law and policies. The jurisdiction of the law therefore extends. In one recent case, because the reverse–engineered solution was made available on the internet and was to be discussed at a conference within the U.S., the U.S. Department of Justice established jurisdiction over conduct occurring abroad when a Russian computer programmer visited the U.S. for a conference (Sklyarov 2002).

As a result, the first generation thinkers may have had a point: information and communications technologies do extend space; but it is not

necessarily a space of its own. The interaction amongst the modalities is what is interesting; not the idea that one modality operates in isolation of the others. Whilst the second generation thinkers would argue that being regulated by multiple jurisdictions at one time is what they have been arguing all along, they fail to appreciate exactly how the technology takes on a regulatory form, how the other modalities may shape its regulatory tendencies, and how the modalities together may extend (or decrease) each others jurisdictions.

The challenge for a user then becomes a situation of trying to understand their jurisdiction. While users are normally subject to national law while operating within a country, they may be subject to foreign laws: technology–use policies of DRM systems, acceptable–use policies of service providers, and even the regulations embedded within peer–to–peer services. The legal and ethical problem is then to identify the political system that can be held accountable for the existence of the regulation, and who to appeal to for changes to it.

Regulatory patching

A second implication can be considered the inverse of the regulatory polyphony that exists under the mixing of modalities. This inverse situation can be called "regulatory patching". It refers to the situation where the subjects "build" the regulatory 'ecology' that they wish to be subjected to. Unlike the traditional regulatory model where there is a single non–modifying regulation for all subjects, traditionally the state, there may be multiple regulatory modalities acting upon the user. As a result some form of regulatory selection may occur.

For instance, a person may choose to use MP3.com with its streaming technology in order to access independent label artists and KaZaA to download mainstream music. That means that the person is subjected to the KaZaA regulatory regime that allows the sharing of music amongst the participants of what is referred to by the KaZaA company as the "KaZaA community", but at the same time it installs spyware on the participants computers. Spyware is a kind of software that transmits data about web usage and the kind of files that users store on their hard drive.

Users may not want to be subjected to such kind of regulation. Therefore, they have the option of altering the regulatory regime and thus shifting the boundaries of jurisdiction with the addition of software patches that allow the bypassing of spyware during the execution of the original KaZaA program — with the use of KaZaA lite — or the removal of spyware components once the use of the program has terminated, e.g. with Ad–Aware.

In addition, in order to regulate the phenomenon of free–riding, where participants of a peer–to–peer network only download files and do not post

files for others to download, KaZaA has implemented the participation level specification in their software. The participation level relates to the computing and content resources, in terms of computing power, bandwidth and number of files that an individual user is ready to devote to the network. The higher the participation level the more the access to the content that the user has. Thus, in order to download files you must provide files for upload. This is a regulatory mechanism enforced in order to encourage participation of the users. However, the user can always download the patch of KaZaA lite 2.0 which creates a fake participation level for users and thus allows them to continue to download files without really sharing them. In such a case there is not a common regulatory mechanism for everyone but each user has—at least in principle—the option to construct their own regulatory scheme. This can be considered as 'regulatory patching'.

There are also alternative technologies that allow users to change their internet protocol addresses, in effect changing their network–apparent geographical location. Many of these services actually exist in the U.S., however, and as it pertains to intellectual property laws, locating one's self virtually in the U.S. may actually be more hazardous; but if the users are concerned about other regulations such as free speech protections in their home country, then the shift to the U.S. jurisdiction might be understandable.

To some extent, there are parallels with real–world legal issues. A classic example is that of off–shore companies that choose to be located in jurisdictions that have a more relaxed taxation regulations. While this practice of regulatory arbitrage (ie of companies in particular, choosing to be subjected to one particular set of laws and not to another because of the better regulatory options that one jurisdiction offers over another) is not uncommon, what is special about this case is the way in which the arbitrage can be created through the technology on an individual basis. Users may, even in the absence of knowing what regulations they are necessarily subjected to, choose to alter the controls through regulatory–patching.

The commodification of regulation

The practice of "regulatory patching" proves the fundamental change regulation has been subjected to. It is not a new theoretical understanding of what regulation does or how regulation operates in a global setting; it is how individuals actually interact with regulatory structures (including technology) that seems to become substantially different to all pre–existing regulatory notions. The findings presented in this paper are just based on policy makers' interventions or theoretical assumptions regarding the nature of interventions. Sources like these were certainly helpful for understanding the trajectory of regulatory evolution, however, it is the practice of those subjected to regulatory regimes that leads this new regulatory debate. This

constitutes a paradigmatic shift from traditional regulatory studies. Even in cases where formulations such as self–regulation were studied, the sources of regulatory intervention were not coinciding in their entirety with the subject of regulation. When, for instance, the self regulation of the banking sector is studied, the consumer who is essentially affected and regulated by such a mechanism is either not examined at all or is approached as a passive receptor of the regulatory effort. On the contrary, in this paper, the information systems that have been studied allow regulation to move from a "turn key" agreement, where the only choice fo the regulated is that of which regulation to choose but to a "do it yourself" construction, where the end–users "construct" their own regulatory ecology.

REFERENCES

Akdeniz, Y. "Case Analysis of League Against Racism and Antisemitism (LICRA), French Union of Jewish Students, v Yahoo! Inc. (USA), Yahoo France, Tribunale de Grande Instance de Paris, Interim Court Order, 20 November 2000." Electronic Business Law Reports, Volume 1, Number 3, 2001, pp. 110-120.

Alderman, J. Sonic boom: Napster, P2P and the future of music. London: Fourth Estate, 2001.

Angell, I. O. The new barbarian manifesto: How to survive the information age. London: Kogan Page, 2000.

Australian Broadcasting Authority. Broadcasting, co-regulation and the public good. 1999, NR 101/1999.

Avgerou, C. Information Systems and Global Diversity. Oxford: Oxford University Press, 2002.

Barlow, J. P. Declaration of the independence of cyberspace. 1996. Available from http://www.eff.org/~barlow/Declaration-Final.html.

BBC news. China internet firms 'self-censoring'. 2002a. Available from http://news.bbc.co.uk/1/hi/world/asia-pacific/2098530.stm.

BBC news. Homer says hack your DVD player. 2002b. Available from http://news.bbc.co.uk/hi/english/sci/tech/newsid_2124000/2124345.stm.

Beck, U. What is globalization? Translated by Patrick Camiller. Cambridge: Polity Press, 2000.

Berman, H. L. Regarding Solutions to Peer to Peer Piracy. 2002. Available from http://www.house.gov/berman/p2p062502.html.

CEI. IP And Technological Self-Help: Barbed Wire For The Digital Age. 2002. Available from http://cei.org/gencon/016,03114.cfm.

Clarke, R. "Subject: ABA Demonstrates Its Ignorance to the World." Forwarded to the Politech Mailing List, message titled FC: More on Australian official demanding Net-regulation -- demonstrating ignorance to the world, November 3, 1999 10:42:30 -0800 1999.

Dogcow. Evading the Broadcasting Services Amendment (Online Services) Act 1999. 2600 Australia, 1999.

Electronic Privacy Information Center. Faulty Filters: How Content Filters Block Access to Kid-Friendly Information on the Internet. 1997.

European Union. Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. 1995, Official Journal L281.

Goldsmith, J. L. "Against Cyberanarchy." University of Chicago Law Review, Volume 65, 1998a, pp. 1199-1250.

Goldsmith, J. L. "Symposium on the Internet and Legal Theory: Regulation of the Internet: Three Persistent Fallacies." Chicago-Kent Law Review, Volume 73, 1998b, pp. 1119-1131.

Hood, C. Explaining Economic Policy Reversals. Buckingham, England: Open University Press, 1994.

Johnson, D. R., and Post, D. G. "Law And Borders--The Rise of Law in Cyberspace." Stanford Law Review, Volume 48, Number 1367, 1996.

Lee, J. S. "Companies Compete to Provide Saudi Internet Veil." The New York Times, November 19 2001.

Leeds, J. W. "United States International Law Enforcement Cooperation: A Case Study in Thailand." Journal of International Law and Practice, Volume 7, Number 1, 1998, pp. 1-14.

Lessig, L. "The New Chicago School." Journal of Legal Studies, Volume 27, Number June, 1998, pp. 661-691.

Lessig, L. Code : and other laws of cyberspace. New York, N.Y.: Basic Books, 1999.

Peltzman, S. The Economic Theory of Regulation after a Decade of Deregulation. Brookings Papers on Microeconomics, 1989.

Perrit, H. H., Jr. "Jurisdiction in Cyberspace." Villanova Law Review, Volume 41, 1996, pp. 1-64.

Rapporteurs sans Frontieres. Report: The twenty enemies of the Internet. 1999.

Romano, R. "Law as product: some piece of the incorporation puzzle." Journal of Law Economics and Organization, Volume 1, Number 2, 1985, pp. 225-283.

Sklyarov. Free(d) Dmitry Sklyarov! 2002. Available from http://www.freesklyarov.org.

Sterling, J. A. L. World Copyright Law: protection of authors' works, performances, phonograms, films, video, broadcasts and published editions in national, international and regional law. London: Sweet and Maxwell, 1998.

Turkle, S. Life on the screen: Identity in the age of the Internet. London: Weidenfeld & Nicholson, 1996.

Walsham, G. "Globalization and IT: Agenda for Research." A paper delivered at the Organizational and social perspectives on information technology, Aalborg, Denmark, June 10-12 2000.

Wired News. DOJ Cracks Down on MP3 Pirate. Wired, 1999a. Available from http://www.wired.com/news/print/0,1294,21391,00.html.

Wired News. The Student Jukebox Sting. Wired, 1999b. Available from http://www.wired.com/news/print/0,1294,32444,00.html.

Wired News. Disney's Peer-to-Peer Pressure. Wired, 2001. Available from http://www.wired.com/news/business/0,1367,47806,00.html.

(All internet references checked 13 February 2003)

BIOGRAPHIES

Prodromos Tsiavos LLB, LLM, MSc, is a PhD candidate in the Department of Information Systems at London School of Economics and Political Science and is currently funded by the Greek Scholarship Foundation for conducting research on Information Technology Law.

Ian (Gus) Hosein is a Visiting Fellow and PhD candidate in the Department of Information Systems at the LSE. Components of this research were made possible by a grant from the U.S. Social Science Research Council.

Edgar A. Whitley is a Senior Lecturer in Information Systems at the LSE. He is Joint Editor in Chief for Information Technology & People.