MITCHELL | HAMLINE School of Law

William Mitchell Law Review

Volume 27 | Issue 3

Article 7

2001

Internet Regulation—Heavy Handed or Light Touch Approach? A View from the European Union Perspective

Robert T. J. Bond

INTERNET REGULATION— HEAVY HANDED OR LIGHT TOUCH APPROACH? A VIEW FROM A EUROPEAN UNION PERSPECTIVE

Robert T J Bond[†]

I. INTRODUCTION

> Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.
>
> We have no elected government nor are we likely to have one, so I address you with no greater authority than that with which liberty itself always speaks. I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear.
>
> Governments derive their just powers from the consent of the governed. You have neither solicited nor received ours. We did not invite you. You do not know us, nor do you know our world. Cyberspace does not lie within your

[†] BA, FSALS., CompBCS; © Robert Bond 2000. Robert Bond is a solicitor and notary public with Faegre Benson Hobson Audley Solicitors in their London office and legal counsel to the Electronic Commerce Project of the International Chamber of Commerce. He is also director of legal affairs at Trustis Limited. Tel: 020 7450 4556, Fax: 020 7450 4545, e-mail: rbond@faegre.co.uk.

> borders. Do not think that you can build it, as though it were a public construction project. You cannot. It is an act of nature and it grows itself through our collective actions.

These words from *A Declaration Of The Independence Of Cyberspace*[1] sum up one extreme in the many views as to whether or not Cyberspace should be, or indeed is, capable of being regulated.

At the other end of the spectrum are the many declarations and statements by journalists, politicians and concerned parents that Cyberspace is "like the wild west," is "a hot-bed of subversive activity" and a "boon to all criminals."

Somewhere in the middle of these extremes are the views of legitimate users of Cyberspace for communication and for business where Cyberspace is like "a Klondike of digital opportunity."[2]

Digital technology, including the web, provides convergent sectors such as telecoms and infotainment together with retail, travel, technology, banking, financial services and insurance industries with tremendous opportunities to maintain and increase business. The Internet and Internet technologies are also a threat, as well as an opportunity, from both commercial as well as legal perspectives as we shall see.

E-Commerce has been defined as "using an electronic network to simplify and speed up all stages of the business process, from design and making to buying, selling and delivering."[3]

Electronic commerce has also been described as "the facilitation of business by electronic means."[4]

The exponential growth of the Internet and on-line activity raises a myriad of new regulatory issues and legal questions. How does copyright apply to digital content? How can national laws apply to activities in Cyberspace? Can privacy and data protection exist on the Web? Can electronic commerce really be secure? Should governments tax Cybertraders? Who will control fraud on the Internet? Is Cyberspace regulable by one, or by many?

[1] Written in 1996 by John Perry Barlow, co-founder of The Electronic Frontier Foundation.

[2] Robert T. J. Bond, *Are There Black Holes In Cyberspace?*, TIMES (LONDON), Dec. 13, 1995.

[3] DEP'T OF TRADE AND INDUS., BUILDING CONFIDENCE IN ELECTRONIC COMMERCE (1999) (a Consultation document),*available at* http://www.dti.gov.uk/cii/ecommerce/ukecommercestrategy/archiveconsultationdocs/index.shtml.

[4] Trustis Limited, *at* http://www.trustis.com.

In seeking to apply the law to the Internet, problems arise owing to the fact that the laws largely apply to the world before Cyberspace really existed.

A. *What Is The Internet?*

- It is not one system
- It is not owned by one person
- It is not controlled by one entity
- It is not subject to one law
- It is not in one place

The Internet is, of course, a network of computers operating globally and the boundaries within which the Internet exists have been called Cyberspace. The name Cyberspace has been attributed to William Gibson from his book Neuromancer, which was published in 1984. Gibson described Cyberspace as a space or place that exists behind the computer screen which you cannot see but you know is there. He also described Cyberspace as a three dimensional representation of all the data in the networked world.

Although many journalists and politicians suggest that the Internet and Cyberspace are anarchic and lawless, they are in fact over-regulated, or more precisely, such laws as may be relevant, are not consistent in their application.

Which specific laws and which national applications of them concern you, will rather depend on your business and activities in Cyberspace and your physical location. How such laws are applied dramatically changes when activities are transferred from a paper world to an all electronic world.

B. *Who Are The Major Players In Cyberspace?*

- Infrastructure owners
- System operators and service providers
- Hardware and software providers
- Content providers
- Users
- Banks and electronic commerce players
- Consumers
- Citizens and governments

As an example of how uncertainty arises within Cyberspace, take a look at the issue of liability for statements made on the

Internet. When it comes to assessing who is liable in a situation of invasion of privacy or the making of defamatory statements, one often asks who divulged or published the data or statement and where a mis-description or misstatement has been made, the question is often asked, who advertises? The problem with the Internet is that at any one time in respect of a misuse of data or a misstatement or a defamatory statement, the following may be the advertiser or publisher:

- The provider of electronic copy
- Web site displayer of copy
- Server controller
- Data carrier
- On-line service provider
- End user who displays it
- All of the above

II. To Regulate Or Not?

The *Oxford Dictionary* defines regulate to mean "control by rule" and defines regulation to mean "the imposition by government of controls over the decisions of individuals or firms."

We have to ask ourselves, in relation to the regulation of the Internet, what exactly we should regulate? Should we regulate the carriers—those responsible for the infrastructure over which content is disseminated, or should we regulate the content providers who develop the content that is disseminated, or should we regulate the content itself?

With convergence we have to ask who should be the regulator? If we look at the carriers and the infrastructure, then our problems today are that, as a result of convergence, all manner of contents can now be transmitted over a number of different mediums. The previously separate infrastructures of broadcast, radio, computer networks, and telecommunications, including the copper wire satellite and cable, are becoming integrated in Cyberspace. The same content is deliverable over almost all of these different media and the new Internet services such as web TV and mobile commerce as well as voice telephony over the Internet cause massive headaches for the regulators. Now there may be a number of regulators in a particular country all claiming responsibility for a converged carrier infrastructure.

As Paula Samuelson, Professor of Law at Cornell Law School said in 1999: "It is, in fact, too early in the development of markets for delivery of electronic information, products and services to start ... heavy handed government regulation."

Perhaps we should also recognize that it may be too late to commence heavy handed government regulation.

Sometimes when government recognizes that it needs to control and close the stable door, the reality is that the horse has already bolted! The encryption control debate is a good example of where governments find themselves wrong footed. The United States has at last recognized that it is almost impossible to control the export of strong encryption. France, which had a strict regime on the use of encryption and did an about turn in 1998, and the British government have changed their tune in the Electronic Communications Act 2000 over mandatory encryption key escrow.

In some cases, Internet regulation may be better achieved by deregulating. For some businesses, the myriad of applicable laws are hindering the growth of e-commerce and for consumers the ability to buy on-line is often hampered by laws and regulations which are inapplicable to the dematerialized world.

Governments and security agencies who have argued for the control of strong encryption or access to encryption keys as a means of controlling Internet crime and Internet fraud cannot seriously believe that criminals and fraudsters will "play the game." Those who wish to defy authority will continue to do so whatever the controls that are compulsorily imposed. The reality is that the Internet and the new technologies actually assist the authorities in tracing criminal activities, perhaps faster and more quickly than they did in the paper world. Last century, the Dalton gang were not brought to justice merely by the gun and the noose, but more by the use of the new telegraph machine![5]

If we look at the net digital services coming on to the UK market then there may be at least four ways in which they can be controlled:

1. Regulation as telecommunication services dealing with such issues as access, interconnection and universal service.

2. Controlled as broadcasting using traditional content based regulatory criteria.

3. Regulated by self-regulation together with competition law.

[5] Rohan Kariyawasam, *Who Will Regulate The Internet?*, 7 COMPUTER TELECOMM. L. REV. 238 (1998).

4. Regulated on a horizontal basis rather than through sector specific or technology specific controls.

The European Union has considered a new regulatory model for existing and new services which will involve a fundamental reform of current regulation and the creation of a single European regulator for communications. A far reaching proposal such as this would consist of the manipulation of existing regulation and the creation of new regulations and certain deregulation. Inevitably it would involve a partnership between industry and government.

III. NATIONAL OR GLOBAL APPROACH?

Can a national approach work? Although the Internet is an instantaneously global medium, it is difficult to imagine that national governments will not want to apply their own controls.

Certain types of behavior in Cyberspace may require more regulation than others. Activities which are perceived as immoral or socially unacceptable, such as crime, fraud, pornography and defamation, are all matters which should be controlled. However, the level of control will vary depending upon the individual's values as well as governmental and cultural dictates. In relation to free speech and the dissemination of information, what might be acceptable in one country can be instantaneously unacceptable or illegal in another and to that end international guidance in the form of regulation may be required.

Regulation should only be used where necessary and should encourage that which is good and deter that which is bad. Regulation does not just mean governmental information and control but also includes management, moderation and clarification.

National governments should not be deterred from taking the initiative to regulate certain aspects of the Internet, but their regulation should have regard to the bigger picture. The speed with which the European Commission began implementing the Electronic Signature Directive was driven substantially by the fact that many member states were passing electronic signature legislation at the national level. The European Commission was concerned that without central control there could be a disharmonized approach to this aspect of e-commerce which would severely hamper "Fortress Europe."

On the other hand, data protection is an example of where the regional approach of the European Community has put us at odds with other continents and jurisdictions where the standards laid down by the European Commission are not met in relation to data protection and privacy.

So who is "we"? In the control of the Internet, who is to be the exemplar and who is to be the rule maker?

Each country has its own standards in relation to what is deemed pornographic and what is not. Some countries are more liberal than others. In the paper world, each country is free to make its own laws on what pornographic material will be made available to which sectors of the citizenry and has the right to control the dissemination of that material within their own borders. They do not have the right to impose their values on other countries.

The problem for governments in cyberspace is that it is difficult, except by heavy-handed regulation, to prevent the citizenry from accessing pornography that is disseminated from many locations.

At the same time, businesses large and small are complaining that that the differing laws and regulations around the world mean that once they operate a web site, they have to be compliant with the laws in every country of the world. This is more important in heavily regulated sectors than in those less regulated. However, the fact that a company chooses to advertise, market and deliver its services through a web site puts it in no different a position, in relation to compliance, with laws that exist in the paper world. Except perhaps for one important thing, and that is that in the paper world there is time within which to decide how to comply with the laws of countries to which you wish to sell or market and if there are countries with which you do not wish to do business, for one reason or another, then you may opt to do so. In Cyberspace the moment that you open up your web site for business, you are either instantaneously compliant around the world, or instantaneously in breach of regulations.

So it becomes important, as quickly as possible, to provide a level playing field for businesses and consumers to make use of the Internet and for citizens and governments to interact in a secure and trusted environment. But can we achieve this intergovernmental and cyber citizens charters as quickly as Internet time will allow? In many cases the answer is no. The fact that consumer and industry initiatives are coming together quickly indicates the belief in the maxim: "God helps those who help themselves."

And whilst we deliberate on how we regulate the Internet and who should set the standards and spend time deliberating the vast amount of statistics that show that the Internet is a massive opportunity and threat, we should remember that as someone recently said: "There are more telephone lines in Tokyo than in the whole of Africa." We should not lose sight of the fact that those counties that are not technically adept and technically served will be disadvantaged. As we regulate the Internet, we should also try to make the Internet American to the Americans, Japanese to the Japanese and Kenyan to the Kenyans.

IV. GOVERNMENTAL OR SELF-REGULATION?

As I have already said, whether on a national or on a global basis, there are clearly certain activities within Cyberspace which are best controlled by government. There will always be differing standards and different methods of enforcement which, in part, will come from cultural and social differences, but in part from the fact that some governments are elected and some are not.

Each concerned or affronted sector will demand government to react and for every sector or activity which is regulated there will be an outcry from those who are disadvantaged. When intellectual property rights become protected on the Internet, those who believe in the free use of data will argue that intellectual property can be protected by technology and should not be interfered with by governments. Those who fear to lose the economic returns from their proprietary rights will champion governmental control.

Entrepreneurial businesses who recognize the tax efficiencies of operating in low tax jurisdictions or by delivering intangible assets over the web and avoiding tax, will object to taxation on Internet business. However, the issues of taxation are of great concern to governments because the globality of the Internet challenges the global budgets. Moreover, the use of e-cash and e-payments by new banking entities takes the control of money further and further away from governments and denies them the previously existing audit trails that they have used to track the movement of illegitimate as well as legitimate money.

However, as more of us accept the use of net technologies, such as smartcards incorporating digital certificates and biometrics, and as citizens and governments start to interact through public key infrastructures, so the much debated identity card surreptitiously comes into being.

Governments and industry need to work together. The reality is that some areas of the Internet will require governmental control but many other areas may be best left to industry self-regulation. However, many consumers and businesses pick and choose issues where governments should or should not get involved. At the 1999 OECD conference in Ottawa, Louise Sylvan, Chief Executive of the Australian Consumers Association, described the government's new predicament: "Ministers: You are to lead! You are to follow! You are to get out of the way! And all at the same time!"[6]

The UK Financial Services Authority ("FSA") recognized that the Internet helps the Financial Services Regulatory body not only to communicate with its markets more efficiently but also to track frauds and scams.

The FSA has revealed five elements to its Internet strategy which are:

- Surveillance–"We must be out there, looking for trouble."
- Education–"We must get out there and explain the risks of day trading."
- Cooperation–"It is quite clear that the old concept of purely national regulation is not going to be adequate in the future."
- Security–"Our overall aim must be to ensure that saving and investing through the web is as secure as other investment routes."
- Enforcement–"This is always the least popular part of our activities. It is essential that we have the ability to make our regime stick, and that we are not afraid to use the odd stick, as well as the carrot."

The International Chamber of Commerce ("ICC"), as the leading world business organization, takes responsibility for providing guidance and self-regulatory codes for a range of business activities in the paper world as well as the Internet. Examples are INCOTERMS 2000, UCP 500, GUIDEC (Guidance for Uniform Internationally Digitally Ensured Commerce) URETS (Uniform Rules for Electronic Trade and Settlement)[7] and the Global Action Plan.

[6] Patrick Vittet-Philippe, Satelex '99 (Toulouse, France), The Governments of the Global Digital Economy (1999).

[7] Robert Bond is legal counsel to the ICC Electronic Commerce Project and was responsible for the initial drafting of this document.

The ICC's Global Action Plan[8] was developed by the ICC's Electronic Commerce Project as a road map to Internet self-regulatory projects and was subsequently adopted by the Alliance for Global Business whose members include: the Business and Industry Advisory Committee to the OECD,[9] the Forum for the Global Information Infrastructure,[10] the International Telecommunications Users Group,[11] the World Information Technology and Services Alliance,[12] and the ICC.

The first Global Action Plan was submitted on behalf of business to the OECD Ministerial in Ottawa, Canada in October 1998 and the second edition was submitted to the OECD's forum on electronic commerce in Paris, France on October 12th and 13th, 1999. The Global Action Plan urges governments to rely on business self-regulation and the voluntary use of empowering technologies as the main drivers behind the creation of trust across the whole spectrum of users and providers of e-commerce goods and services. It also states that governments should focus on the provision of a stable and predictable environment enabling the enforcement of electronic contracts, the protection of intellectual property and safeguarding competition. The Global Action Plan is perhaps the most comprehensive source of information on selections of industry self-regulatory initiatives.

V. COMMUNICATIONS, WEB SITES AND PRIVACY

As we have already seen, the issues of convergence in the field of the communications sectors means, in the words of one commentator:

> Regulating services is going to prove extremely problematic. For us, we have taken a very strong stand against regulating the Internet. We will expect to see video services provided over the Internet, but we will not apply the broadcast criteria to Internet regulation. The reason for

[8] *http://*www.iccwbo.org.

[9] *See generally* Business and Advisory Committee to the OECD, *at* http://www.biac.org (last modified Jan. 29, 2001).

[10] *See generally* Global Information Infrastructure Commission, *at* http://www.giic.org (last visited Feb. 15, 2001).

[11] *See generally* International Telecommunications Users Group, *at* http://www.intug.net (last visited Feb. 15, 2001).

[12] *See generally* World Information Technology and Services Alliance, *at* http://www.witsa.org (last visited Feb. 15, 2001).

> that from our perspective basically is, we have a situation with new technologies, lets let the market place flow. And it's doing a very good job of it as it stands today.[13]

The environment or infrastructure within which business is done on the Internet requires:

- Certainty
- Security
- Trust
- Confidentiality
- Legality
- Accountability

The development of public key infrastructure technologies provides the combination of legal and technical solutions to the above issues but the development of law and technology together highlights the needs for cross border standards and digital certificates cross certification procedures.

In order to inspire consumer confidence and trust, Internet policies and procedures need to be developed by industry with the blessing of government for issues such as marketing, advertising and privacy. In some cases, regulation needs to be deregulated and self-regulation needs to come to the fore.

But who should regulate Internet advertising? In the UK there are numerous bodies claiming a right or interest in this field including CAP and ASA, the regulatory authorities such as ITU and OFTEL, the Direct Marketing Association, The Alliance for Electronic Business and the ICC.[14]

When it comes to protecting privacy on the Internet and generally within communications, there is a balance to be struck between the needs of government to monitor or intercept communications and the rights of individuals to have privacy within their domestic environments. In e-commerce, data is the most valuable commodity. Ownership of data, however, brings risk and liability. Data must be protected and data transfer must be made in controlled environments such as public infrastructures.

Websites are wonderful data mining opportunities and technology allows website owners to obviously or surreptitiously obtain

[13] FCC Commissioner Susan Ness, Comments at Regulatory Roundtable, World Telecom '99, Geneva, Switzerland (Oct. 14, 1999).

[14] The ICC has recently published guidelines on advertising on the Internet in order to set standards of ethical conduct.

data and information about individuals. The EU Data Protection Directive and other similar regulations are intended to provide protection for the individual against the processing and use of data obtained without their consent. The laws are not global by nature but their implications are.

The ongoing data debate between Europe and the United States highlights the differences in standards and approaches laid down by governments and individuals as to the methods by which their rights and obligations are given and enforced. Whilst all of this debate over the right privacy is discussed, the more cloak and dagger aspects of the invasion of privacy are sometimes revealed.[15]

It was reported that in 1998, members of the European Parliament were provided with evidence that the U.S. National Security Agency ("NSA"), in collusion with the British government's communication headquarters ("GCHQ"), had created and maintained since the end of the second world war an almost seamless telecoms surveillance system, Project Echelon, across national borders allowing the interception of almost every fax, e-mail and telephone call. Simon Davies, the director of Privacy International in London, indicates that this reveals two profound conclusions: "First, the NSA and its partner agencies can now intercept most communication networks world-wide. Second, the distinction between traditional police and security agencies has been blurred to an unprecedented extent. The implications for privacy protection are profound."

It has been reported that Echelon is capable of intercepting and processing many types of transmissions and may intercept as many as three billion communications everyday. Echelon gathers all of these transmissions indiscriminately and then filters the information via artificial intelligence programs. Some sources have claimed that Echelon sifts through an estimated ninety percent of all traffic that flows through the Internet.[16]

When it comes to the surreptitious invasion of our privacy by governments, notwithstanding national security concerns, a variation on the well-known quote should be: "On the Internet no one knows you are a dog, but they know every tree and lamppost you visited!"

[15] 16 U.K. COMP. L. & SECURITY REP. (1999).

[16] *Id.*

VI. CONCLUSION

When discussing the regulation of the Internet, at Satelex '99 in Toulouse, France, Patrick Vittet-Philippe from the European Commission DGIII said that the inter-relationship between government, industry and the citizen presented "the leadership challenge of a life time. We are, like Marco Polo, charting the Silk Roads of the Future."

A Ditchley conference in the UK on the regulation of Cyberspace, at which Ian Taylor, MP, the former UK Tory Minister for Technology, was Chairman, and I was Rapporteur, concluded: "Regulations should be reflective rather than reactive. Regulations should control that which is bad and support that which is good. Regulations should be introduced on an international basis whilst acknowledging cultural and social individualities of nations and communities."

The Ditchley conference report noted that a balance had to be struck between the use of regulation to control and restrict unacceptable activities on the Internet, whilst at the same time not preventing the vast advantages that are derived from the Internet. As I said at the time: "When it comes to the regulation of Cyberspace, the business of Internet management should not hinder the management of Internet business."

***