

# Contested Space: the Internet and Society

A briefing paper for the 21<sup>st</sup> Century Trust<sup>1</sup>

John Naughton<sup>2</sup>

## Introduction

Although the Internet currently looms large on our horizons, we should try to retain a sense of perspective about it. Many of the extravagant claims made in the media about the network and its significance are reflections of the *zeitgeist* rather than assessments informed by knowledge. Most of what was written and said about the 'new economy' during the dot-com boom which abruptly ended in April 2000, for example, was wish-fulfilment or fantasy masquerading as journalism. And what we face at the moment (Summer 2001) is the mirror image of that phenomenon: irrational exuberance<sup>3</sup> has given way to an equally irrational pessimism. And the new ideology makes as little sense as its predecessor.

Besides, these are early days to be making grandiose assessments.

To illustrate the point, let us take just one example – the claim that the World Wide Web is as revolutionary a transformation of mankind's communications environment as was Gutenberg's invention of printing. Suppose this is true. Gutenberg's first bibles were printed around 1455. The Web was invented by Tim Berners-Lee in 1989-90 but did not become a popular medium until 1993-4. That means we are just eight years into the supposed 'revolutionary' transformation – i.e. roughly in the same position as a citizen of Mainz would have been around 1463. Imagine asking such a citizen if she realised that Gutenberg's technology would undermine the authority of the Catholic church, trigger the Reformation and the rise of the Romantic movement, enable the rise of modern science and even – if some commentators<sup>4</sup> are to be believed – lead to the invention of 'childhood' as an extended, protected period in the lives of young people. One only has to conduct this thought-experiment to realise how absurd it is for us to make confident predictions about where the Internet will lead us.

In other words, some humility might be in order!

Nobody disputes that the rise of the Internet is a significant development in human affairs.<sup>5</sup> There are plausible grounds for supposing that it is potentially – if not actually – a

subversive technology, i.e. one which could challenge or undermine established political or economic structures. Whether it succeeds in doing so remains to be seen. But the impossibility of making authoritative assessments on the impact of the Net does not absolve us of responsibility for trying to do the best we can with the material to hand. And that, in a way, is what this Seminar is about.

## Part 1: Understanding the technology

One of the deficiencies of contemporary discussion about the social and economic effect of the Net is that it more or less ignores the actual technology of the network. Social scientists and political analysts take the technology as a *given* and move on to what they regard as the really interesting questions. This is understandable (life is too short, is it not, to tangle with technical jargon?), but in this case misguided. The technology is central to understanding what the Net might do – and what might be done to it. For that reason, we need to venture first into territory where normally only engineers dare to tread.

## **The Internet is not the Web**

The first thing we need to do is to distinguish between the Internet and the World Wide Web because the two are often regarded as synonymous in media accounts of the phenomenon. This is problematic because it obscures some very important issues and leads to a distorted view of the Internet. One way of thinking about the relationship between the two is to treat the Internet as analogous to the track and signalling infrastructure of a railway system. In this view, the Web is then one particular kind of traffic which runs on the infrastructure. Other types of traffic include e-mail and files being transferred from one location to another. In terms of bit traffic, the Web probably accounts for much of the activity on the Internet, but the main way in which most of the Net's 400 million users directly interact with the network on a daily basis is via e-mail. Since e-mail messages have up to now tended to be small they account for a disproportionately low proportion of overall network traffic.

## **The evolution of the network**

Although the Internet is popularly portrayed as a *computer network*, it is more accurately defined as 'a global network of computer networks' which operates using a set of open technological protocols of which the TCP/IP suite<sup>6</sup> is the most important. The current [2001] Internet came into being in January 1983, having evolved from the ARPANET, a packet-switching network conceived and funded by the US Department of Defense's (DoD) Advanced Research Projects Agency (ARPA). The ARPANET came into operation in October 1969 and was a uniform system comprised of a number of identical nodes and accessible only to researchers funded by ARPA. Shortly after it came into operation, a number of other computer networks came into being in the US and elsewhere<sup>7</sup>. Although all of these non-ARPA networks also used packet-switching technology, they were functionally incompatible with one another and the DoD system. After the successful demonstration of the ARPANET as a working system in 1972, ARPA turned its attention to the problem of how to 'internetwork' these networks to create a bigger, transnational network. The solution, which originated with Vinton Cerf and Robert Kahn, evolved over the decade 1973–'83 and involved the creation of a set of protocols (technical conventions) which would enable computers to act as gateways between different networks so that messages could be passed reliably from any node to any other node via an indeterminate number of routing stations. These protocols eventually became a 'family' of upwards of 100 detailed standards known collectively as the 'TCP/IP' suite.

## The impact of the Web

For the first decade of its official existence (1983-93) the Internet was essentially a resource for academics researchers. Many of the facilities we use today were available to this community, but accessing them required mastery of computer technology and in particular of the Unix operating system. When Tim Berners-Lee invented the Web in 1989-90, he took the first steps towards making the Net usable by lay users by portraying its resources as clickable links. But the original Web browsers still reflected their computer science origins, and it was only with the appearance of the first graphical browser -- the *Mosaic* browser -- in 1993 that the Web really took off and became a mass medium.<sup>8</sup>

The Web brought millions of new users to the Internet. In order to accommodate them, the structure of the network was distorted. Where previously the Internet had been a network of *peers* – computers with equal status which enjoyed unique addresses and permanent connections – it metamorphosed into a two-tier system in which a minority of privileged machines (servers) dispensed web pages and other services to millions of lower-status machines (PCs which functioned as passive ‘clients’ and were denied permanent addresses or persistent connections).

This may seem like a technical detail, but in fact it had an important implication – namely that everything important on the Web had to happen on a machine which belonged to the privileged class of servers. Anyone seeking to publish a Web site, for example, had to arrange for it to be hosted on such a machine: there was no practical method of hosting the site on a machine which had only dial-up access to the Net. And it turned out that the privileged class of servers was more vulnerable to corporate and government control and interference than was initially expected. We will return to this later.

## The architecture of the Net

The significance of the ‘internetting’ technology based on TCP/IP is that it enabled the creation of a global network with an open, permissive architecture. There was no central control, and therefore it would not make sense to try and pre-specify the kinds of networks which would be permitted to join. Anyone could hook up a network to the emerging ‘internetwork’ so long as they had a gateway computer which ‘spoke’ TCP/IP. This principle enabled the emerging network to grow organically at such astonishing speed.

An important implication of the Cerf-Kahn design was that the overall network was essentially ‘dumb’. Its only function was to pass electronic packets from one point to another – the so-called ‘end to end’ principle<sup>9</sup>. As far as the network was concerned, those

packets might be fragments of e-mail, photographs, recorded music or pornographic videos -- they were all the same to the network and are treated identically. This indifference to content made the Internet<sup>10</sup> radically different from previous communications networks which had been owned or controlled by agencies which determined the uses to which their systems could be put. In the UK and many European countries, for example, the national telephone networks were owned for most of the 20<sup>th</sup> century by national Post Offices, which partly explains why FAX technology was so slow to take off in the West: organisations devoted to delivering letters by hand were not disposed to take kindly to the idea of sending letters down a telephone wire. In sharp contrast, uses and applications of the Internet in contrast were determined entirely by the ingenuity of its users and those who developed applications which could harness its message-passing capabilities. Some commentators<sup>11</sup> have attributed the explosion of economic activity and creativity generated by the Internet in recent years to this factor.

## **Anonymity and its implications**

Another feature of the original Internet architecture which is significant for our purposes is that fact that authentication of users was not required. Each machine which is connected to the Net needed to have a unique 'IP' (Internet Protocol) address<sup>12</sup>, and all of that machine's transactions with other machines on the network could be logged. But there was no provision for linking IP addresses to known individuals. This meant that the architecture facilitated anonymity – a feature famously encapsulated by the celebrated 1993 *New Yorker* cartoon showing two dogs in front of a computer. 'The thing about the Internet', says one, 'is that nobody knows you're a dog'.

The implications of the architecture's facilitation of anonymity have been far-reaching. On the one hand it permits a wide range of reputable and disreputable uses of the Net because the identity-based sanctions of the real world do not apply in Cyberspace. On the other hand, anonymity enables the free expression and dissemination of views in ways that would be more difficult in real-world arenas. The architecture makes it difficult, for example, for security services to track down or silence dissidents<sup>13</sup>, and for corporations to identify whistle-blowers or campaigning groups disseminating critical information or hostile propaganda.

The technical architecture of the Net has thus been a prime determinant of how the network has been used. As in the physical world, architecture enables some things and prevents others. The significant point from our point of view is that the architecture of the Net is cast in terms of technical protocols – that is to say, as computer code. And, as

Larry Lessig has pointed out,<sup>14</sup> there is nothing immutable about code. It is pure ‘thought-stuff’ and, as such, can be changed. This is something to which we will return.

## Scale of the Internet

The Internet is a global system in that it has nodes in virtually every country, but the density of users and connections is very uneven across the globe. It is estimated, for example, that 69 per cent of Internet users are located in the North America and Europe, and that Africa, with 13 per cent of the world’s population, has less than one per cent of the world’s Internet users.

Nevertheless the scale of the network’s coverage is still remarkable. Because of the ‘organic’ architecture created by the TCP/IP architecture, it’s impossible to say how many Internet users there are, but authoritative estimates at the time of writing (February 2001) suggest numbers in the region of 400 million.<sup>15</sup>

**Table: Estimated Internet User Population November 2000**

Region	Users (millions)	% of total
Africa	3.11	0.76
Asia/Pacific	104.88	25.76
Europe	113.14	27.79
Middle East	2.40	0.59
Canada & USA	167.12	41.05
Latin America	16.45	4.04
<b>World Total</b>	<b>407.1</b>	

Source: Nua Internet Surveys ([www.nua.ie](http://www.nua.ie))

## The Internet as a communications space

The Internet represents a radical development in our communications environment. There is a widespread belief that in areas where ‘information is power’, the rise of the Net has to some extent levelled the playing field on which citizens and civil society organisations compete with established economic, media and governmental interests for public attention.

As a communications space, the Internet:

- Facilitates access to published data, information and knowledge
- Lowers the barriers to publication and enables groups and individuals to bypass traditional gatekeepers in media and publishing
- Makes it more difficult for governments and corporations to keep sensitive material out of the public domain
- Facilitates rapid communication on a global scale
- Facilitates the sharing of information resources
- Facilitates the formation and maintenance of 'virtual communities' of people or institutions with shared interests.

#### **ACCESS TO PUBLISHED DATA, INFORMATION AND KNOWLEDGE**

The volume of data and information now published on the World Wide Web (WWW) is phenomenal, and indeed threatens to overwhelm the capacity of search engines and directories to index and categorise it.<sup>16</sup>

#### **LOWERING BARRIERS TO PUBLICATION**

For many individuals and organisations, online publication is preferable to publication in traditional media because it is relatively inexpensive, provides global coverage and bypasses the gatekeepers who control access to traditional media. It makes it possible, for example, to publish an attractive, full-colour pamphlet and distribute it globally at a cost which is determined almost entirely by the remuneration required by those who produce it. There is no need to set up a distribution network; and distribution costs are paid by readers. Furthermore, online publication is not limited simply to documents. Anyone with a modicum of skill and a simple recording device<sup>17</sup> can create audio, photographic or digital files which can be loaded onto a Web server and made available for download to all comers – again on a global basis<sup>18</sup>. The Internet thus lowers the barriers not just to document publication but also to multi-media publication.

#### **MAKING IT HARDER TO KEEP SECRETS**

The Internet makes it increasingly difficult for governments to maintain secrecy or prevent (e.g. by legal injunction) publication within their jurisdictions. In the 1980s, for example, the British government successfully used legal methods to prevent *Spycatcher* -- the memoirs of a former MI5 officer named Peter Wright who alleged that the security service had conspired to undermine the Labour government led by Harold Wilson in the 1960s --

from being read by British subjects, even though the book had been widely published abroad. Newspapers which attempted to publish excerpts were legally enjoined and British residents who wished to read Wright's allegations had to resort to absurd measures like making a day-trip to the Irish Republic in order to obtain a copy. This would be unimaginable today. At the first sign of a British or European injunction, the contents of the book would appear on a Web-server in the US where they would enjoy the protection of the First Amendment and be available to anyone with a browser and an Internet connection.

### **RAPID AND INEXPENSIVE COMMUNICATION ON A GLOBAL SCALE**

The Internet offers a wide range of facilities for individual and group communication and discussion, including:

- Electronic mail and discussion lists
- Asynchronous conferencing systems

The most prominent asynchronous conference system is Usenet – a global system of online conferences called 'news groups'<sup>19</sup>. These allow participants to create topical groups in which a series of messages akin to e-mail messages can be strung together to form discussion 'threads'. Usenet is, like the Internet itself, a self-organising system which operates on the basis of agreed protocols – in this case a standard message format.<sup>20</sup> Something like 45,000 discussion groups – devoted to every conceivable specialism and interest – currently exist, each containing anything from a dozen to thousands of messages.

- Chat systems

'Chat' systems enable various kinds of synchronous conversation. By far the most widespread technology is that of 'text chat' in which a number of people exchange typed messages in real time in a shared virtual space known as a 'chat room'. In recent years, as modem speeds and the bandwidth of Internet connections have increased, systems which permit voice chat and even primitive video-conferencing have become common.

- Instant Messaging (IM)

IM enables an Internet user to create what is in effect a private chat room with another individual. Typically, the instant messaging system alerts the user whenever somebody on her private list is online. She can then initiate a chat session with that particular individual. Instant Messaging has proved remarkably

popular since its introduction some years ago and is an effective technology for keeping friends and colleagues in touch with one another.

### **SHARING OF INFORMATION RESOURCES**

Because of the ease of online publication, the Internet makes it much easier for groups and individuals to share information resources. Archives of documents and other resources can be digitised and placed on Web or FTP<sup>21</sup> servers from which they can be accessed by anyone with the appropriate permissions. The hyper-linking technology of the Web makes it easy for collaborating organisations to compile indexes and guides to one another's materials without having to maintain multiple archives. This facility is widely used by civil society groups.

### **VIRTUAL COMMUNITIES**

Much of the discussion about 'virtual communities' – social groups which conduct most of their relationships in Cyberspace – focusses on whether such communities are the same as 'real' communities – i.e. social groupings, usually based on geographical location, to which people belong in the real world. The truth is that there is probably less of a dichotomy between online and real-world communities than is currently supposed. Even what we think of as normal, place-oriented communities 'can stretch well beyond the neighborhood'.<sup>22</sup> And one of the few ethnographic studies which exists<sup>23</sup> suggests that 'we need to treat Internet media as continuous with and embedded in other social spaces' – implying that people use the Net in ways that complement rather than disrupt their social lives.

## **What next?**

The Internet is changing -- though the changes are not yet apparent to the mass media. This is because their view of the network is obscured by the dominance of the Web. But although the Web was the 'killer application' which turned the Internet into a mass medium, in the long view of history we may come to see it as a blip or a diversion.

As hinted earlier, the explosion of the Web led to the evolution of a two-tier network consisting of a minority of privileged servers within the Domain Name System (i.e. with fixed Internet addresses) and a majority of 'dumb' PCs running browsers and having non-persistent connections to the Net. In this unequal world of active servers and passive clients, organisations with economic and political power were always likely to wield undue influence over the server network. And in the event, this is what seems to be happening.

It has been reported, for example, that four companies -- AOL Time Warner, Microsoft, Yahoo and Napster – now [Summer 2001] control half of all minutes spent online by U.S. users<sup>24</sup>. This represents a consolidation of a trend that has been obvious for some time. The number of companies controlling 60 per cent of time spent online by US Internet users, for example, has fallen from 110 in March 1999 to 14 in March 2001. If these trends continue, then the Web may follow the same pattern of media-conglomerate dominance that have been observed in print, film and television.

But even as this happens, other major trends are converging which may, in the end, lead to another explosion of innovation. These trends are:

- The increasing processing power and storage capacity of 'ordinary' PCs.

In the early days of the Web, most personal computers lacked the processing power, storage capacity and operating systems needed to enable them to function as servers. The average PC circa 1994 was accurately described as 'a life support system for a browser'. That, together with the fact that most PCs had only dial-up access to the Net and therefore lacked permanent IP addresses, effectively precluded them from acting as servers. Moore's Law has removed the functionality barrier. Today's PCs are more powerful than most of the servers of 1994, and there are industrial-strength operating systems (Windows 2000 Pro, Linux) available for them.

- Changes in the Internet addressing system brought about by a new technical standard – Ipv6.

One of the reasons for the two-tier system which evolved to cope with the explosion of consumer demand triggered by the Web was the fact that the original Internet addressing system would not have provided enough permanent addresses for all the machines which needed to connect to the Net. But the addressing system is now migrating to a new standard – Ipv6 – which provides a large enough address space for every conceivable purpose and certainly sufficient to allocate a permanent address to every computer on the planet.

- The spread of broadband connectivity.

Although Broadband (high-bandwidth) connections have been slower to reach the consumer than originally predicted, nevertheless there is a steady rise in the proportion of Internet users who have connections in the 256 kbit/s to 10 Mbit/s range. Further more, most of these broadband connections are of the persistent – 'always-on' – type.

- The advent of new Peer-to-Peer (P2P) technologies

The rise of Napster has focussed public attention on a cluster of newish technologies collectively – and in some ways misleadingly -- categorised as P2P.<sup>25</sup> What makes these different is that they enable computers with non-persistent connections to function as servers and to engage in collaborative working even though they are outside the DNS. P2P is potentially revolutionary because it may presage a return of the Internet to its roots, enabling people to communicate and collaborate freely outside the (easily regulable) DNS.

## **Part 2: Some issues raised by the Internet**

Having briefed ourselves on the technological background, let's now briefly examine some of the issues and questions which are prompted by the Net. Most of these issues are complex so what follows is intended only as an introduction to them. Treat the material as starting points for discussion.

## Access and the digital divide

In one sense the Internet appears to promise the realisation of Thomas Paine's dream of a society in which everyone has a voice. If this dream is ever to be fully implemented, however, a fundamental problem will have to be addressed and solved. This is the issue of inequality of access to the Internet – the so-called 'digital divide', the term popularly used to describe the gap between those who are 'information rich' and those who are 'information poor'. If the benefits and facilities of the Net are available only to a selected few, then its democratising potential (not to mention its economic potential) will never be realised.

At the moment, these benefits are available only to a select minority of mankind – variously estimated between 2% and 6% of the global population.<sup>26</sup> The digital divide operates both within societies, and between regions and countries. 'Current access to the Internet', reports a UNDP Report, 'runs along the fault lines of national societies, dividing educated from illiterate, men from women, rich from poor, young from old, urban from rural'.<sup>27</sup>

But the digital divide also has an international dimension. According to the UNDP, in mid-1998 the industrial countries of the world accounted for 88% of all Internet users, despite having only 15% of the world's population. North America – with 5% of the people – had more than 50% of Internet users. And South Asia – home to 20% of the world's population – had less than 1% of the planet's Internet users.<sup>28</sup>

These disparities are well known, as are the reasons for them. Internet access requires technological, social and educational infrastructures which are unevenly distributed across global society. On the technological side, for example, the key element to date has been access to a telephone network. Using 'teledensity' (the number of telephones per 100 people) as a metric we find huge disparities in access, as the following table demonstrates.

Country	Teledensity (Telephone mainlines per 100 people)
Monaco	99
US	64
Italy	44
United Arab Emirates	40
Costa Rica	17
Kenya	0.8
Sierra Leone	0.4
Bangla Desh	0.3
Uganda	0.2

Source: International Telecommunications Union, 1998.

The existence of a suitable communications infrastructure is a necessary but not sufficient condition for ensuring equality of access to the Internet. A broadband network connection is useless to someone who is illiterate. The ability to tap into and harness the information and communication resources of the Net is predicated on literacy and education. This implies that tackling the digital divide is not just a matter of creating telecommunications infrastructures where none previously existed, but also of developing universal literacy programmes and building up social capital generally. Of the two tasks, the first is likely to be the simpler to accomplish – especially given the development of wireless technologies which are much less resource intensive than conventional landline telephone networks. The inescapable conclusion is that the gap between the information rich and the information poor is unlikely to narrow in the medium-term future and may even widen as Internet penetration in industrialised societies gathers pace.

This is very bad news from any perspective. In economic terms, it means that under-developed societies will continue to be denied the economic benefits of the Net. Just to give one illustration, the UNDP Report points out that the cost of sending a 40-page document from Madagascar to Cote d'Ivoire is \$75 by five-day courier or \$45 by 30-minute fax whereas the same document can be sent by e-mail for about 20 cents (not to mention the fact that it can be dispatched to multiple recipients all over the world for the same cost).<sup>29</sup>

The digital divide is also bad news in terms of human rights. Western countries have increasingly regarded universal access to telecommunications services as an important public goal (it was first written into US federal telecommunications law in 1934). The European Union requires countries seeking membership to implement policies and legislation aimed at enabling universal access to telecommunications services. The 1948 Universal Declaration of Human Rights declared that everyone has the right to freedom of expression and the right to 'receive and impart information and ideas *through any media and regardless of frontiers*'. (Emphasis added.) The digital divide implies that in a world increasingly dependent on networked information, this right will be anything but universal for a large proportion of the global population.

## Control of the Net

The Internet – as we have seen – emerged from the ARPANET, which itself was a product of the 1960s. Although its early development was funded by the military, the network was designed and built – and for the most part used – by academic researchers who inhabited a liberal, uncommercialised organisational culture. In the decade 1983 to 1993 – in other words from the launch of the TCP/IP-based network to the release of the first graphically-oriented Web browser – the Internet was essentially an intellectual sandpit and working environment for academic researchers. Although there were official regulations about what the network could and should be used for, in practice there was little supervision and applications were limited only by the ingenuity of users. So long as the application involved the passage of data packets, the Internet would – and did -- handle it.

The result was not just an explosion in creativity but also the evolution of a freewheeling, anarchic, non-commercial, permissive ethos sometimes summarised by the phrase 'geek culture'. This culture, however, went largely unnoticed in the outside world. Because there was no commercial activity on the Net, the business world paid little attention to it. And because the community of Internet users was relatively small and cloistered, governments were even less interested.

The release of the *Mosaic* browser in the Spring of 1993 led to a sea change in commercial and governmental attitudes to the Net. *Mosaic* was significant because it made it easier to place pictures on Web pages. Where there were pictures, there was the possibility of entertainment. And where there was entertainment there was the prospect of commercial profit -- especially when it was perceived that the Web was the fastest-growing communications medium in history, reaching its first 50 million users in four years (as compared with 36 years for radio and 13 for television). The perception began to dawn in the minds of legislators and businesspeople that this phenomenon was too important to be left to geeks.

The initial intrusions of business and government into the Internet were clumsy and ill-conceived and appeared to confirm the contemptuous disdain of the Internet community towards anyone with a profiteering or regulatory mindset. A kind of complacent arrogance took hold, based on the assumption that Cyberspace was somehow different in kind from 'real' space, that it was intrinsically subversive of established ways of doing things and that it lay beyond the reach of conventional control structures.<sup>30</sup> Within the Cyberlibertarian community, for example, it was widely believed that censorship would always be impossible on the Net.<sup>31</sup> This conjecture may have been reasonable at one time, but

events have not borne it out: the Internet is potentially much more susceptible to political and commercial control than was once thought. Cyberspace will not remain a 'digital commons' without vigorous political action to defend its freedoms. Left to their own devices, the forces of official regulation and commercial exploitation will gradually enclose the commons.

## **Governments and the Net: the ambivalence of power**

All governments – including those in Western democracies -- are ambivalent about the Net. On the one hand they see it as a symbol of modernity and an engine for economic growth which may change the balance of economic advantage in their country's favour. On the other hand, they perceive it as a potentially destabilising force, undermining traditional political and legal structures, facilitating subversion and eroding official control of what is published and read within their jurisdictions. They are also concerned at the potential erosion of their tax bases as a result of information goods crossing their frontiers as undetected (and untaxed) bitstreams.

### **AUTHORITARIAN RESPONSES**

Governments differ greatly in the ways they react to what they see as the Internet's 'threats'. Authoritarian regimes generally attempt directly to control their populations' access to, and use of, the Net. A report by Reporters Sans Frontieres (RSF) has identified 45 nations which impose blocking and filtering or all-out bans on Internet access. Of the 45 nations, RSF said 20 could be described as real 'enemies of the Internet' for their actions in restricting citizens' connections to the Net or in censoring what they see on the Web.

### **'LIBERAL' RESPONSES: PRE-EMPTIVE LEGISLATION**

More liberal administrations aim to reassert control by passing legislation which defines certain kinds of online activities illegal, and then relying on the 'force of law' and the reluctance of ordinary citizens and ISP companies to become martyrs for liberty or freedom of speech to bring about the desired level of regulation. This is the approach favoured, for example, by the UK government – as demonstrated by its Regulation of Investigatory Powers Act 2000 (RIPA), which gives sweeping powers to the Home Secretary (i.e. Minister of the Interior) to intercept and read e-mail and other online traffic. The Act gives the authorities the power to demand the surrender of encryption keys, and to require that ISPs install a monitoring computer which is hardwired to a surveillance centre at MI5 headquarters, thereby enabling the authorities to gather *all* the bit traffic

flowing through the servers of bugged ISPs and – when armed with the appropriate statutory order – read the text of messages encoded in those monitored packets. It also gives the authorities the power to monitor an individual's 'clickstream' – i.e. the log of sites visited by that person on the Web – without even having to seek a warrant.<sup>32</sup>

### **LESSONS OF UK EXPERIENCE**

Although the RIPA is a piece of UK legislation, it raises a number of generic issues.

Firstly, the fact that such an illiberal measure passed through the UK Parliament with relatively little difficulty highlighted the extent of legislators' ignorance of the issues involved in Internet regulation and the lack of public awareness of what was at stake. This is likely to be a pattern for the future in relation to Internet regulation, in that governments (and, on occasion, industry lobbies) will seek to make pre-emptive legislative strikes ahead of public opinion and before civil society activists can raise public awareness. Environmental campaigners have long experience of this official strategy.

Secondly, the RIPA highlighted the extent to which the Internet community underestimated the efficacy of new legislation in achieving anti-libertarian ends. All a sovereign government has to do is to pass legislation which defines specified activities as illegal. Unless the proposed restrictions are widely perceived as intolerable by the populace, they will be adhered to by the vast majority of people and by all companies involved in the area. Governments would have found it difficult to impose their will on the original Internet community of researchers, programmers and libertarians; but the metamorphosis of the Net into a mass medium has transformed the possibilities for regulation and official intimidation.

Thirdly the RIPA highlights the fact that ISPs have become a key target for regulatory action. All Internet users have to go through an ISP in order to gain access to the Net. The vast majority of ISPs are private or public companies whose directors are obliged to obey the law and do their best to maximise shareholders' returns. This means that as corporate bodies they are unlikely to challenge legislation or legal action on principle. They see themselves as businesses and wish to be regarded, legally speaking, as common carriers rather than members of the Fourth Estate.

### **ENCRYPTION IS NOT THE ANSWER**

The RIPA also refutes the Internet community's long-held assumption that encryption was the ultimate guarantor of libertarian freedoms. Given that unencrypted communications over the Net are intrinsically insecure, encryption is the only way of guaranteeing that

private communications remain private. One could argue that in the emerging online world, access to encryption tools becomes a basic human right, and any infringement of that right must be circumscribed by law and a respect for the right to privacy enshrined in Article 10 of the European Convention on Human Rights and Fundamental Freedoms.

Historically, cryptography was something over which the state exerted total control. But the development of Public Key Cryptography by university researchers in the 1980s created fresh waves of institutional paranoia about the subject.<sup>33</sup> Most governments seem to have conceded that, technically speaking, the encryption genie has escaped from the bottle. To the Internet community, this concession was interpreted as an historic victory. But such celebrations may be premature. The UK RIPA suggests that instead of trying to crack codes surreptitiously, governments will concentrate instead on putting legal pressure on individuals and companies. And the chances are that this approach will be highly effective: how many people will make a principled refusal to surrender a decryption key when the consequence of doing so is a two-year prison term?

### **The longer arm of the (civil) law**

The heady days when people believed that the Internet's transcendence of legal jurisdictions would render it immune to conventional legal pressures is giving way to a more realistic appraisal of the power of legal codes to control online behaviour, and to a more realistic appraisal of the power of the nation state. As with encryption, the legal system seeks out critical points in the system and applies pressure on them. In 2000, for example, a university teacher sued Demon Internet, a British ISP, because it had continued to relay Usenet news-groups in which allegedly defamatory comments about him were posted, despite previous complaints from him. Demon lost the case and then appealed, but withdrew from the appeal at the last minute, paid damages to the plaintiff – and established a legal precedent in the UK. This says that an ISP is legally bound to remove Usenet postings (or Websites) if an individual alleges that material published therein is defamatory.

This has opened up an interesting can of worms – and the effects of this precedent are being felt already by campaigning civil society organisations. For example, a London pressure group campaigning for imaginative use of a disused power station castigated the new owners of the property for failing to proceed quickly enough with their plans for rejuvenating the building. A letter from the owners' solicitor to the ISP carrying the pressure-group's web site was sufficient to persuade the ISP to pull the site, 'just to be on the safe side'. Use of the law for purposes like this -- which are essentially intimidatory

-- is certain to increase and is likely to cramp the freedoms of many campaigning organisations.

Other examples of the powers of national or international legislation to influence online behaviour include: the decision of a French court to require Yahoo!, an American company, to filter its auction sites selling Nazi memorabilia so that French Web users could not access them; new EU laws which enable European consumers to sue EU-based Internet sites in their own countries; the endorsement by the US of the Council of Europe's Cybercrime treaty, which aims to harmonise laws against hacking, online fraud and child pornography; and the way the US Digital Millennium Copyright Act has been used to intimidate, for example, authorities at Oxford University into deleting the Web pages of a student who was pretending to publish on his site the code of DeCSS, a computer program written to enable DVD disks to be played on computers running the Linux operating system.

## E-commerce: prospects and implications

### **A new economy?**

Forget the dot-com bubble. It was just one of those periodic stock-market frenzies in which investors assign absurd valuations to the shares of some companies. The fact that the boom is over doesn't tell us much about what underlying economic changes might be wrought by the Net.

A frequent mantra of business publications and managerial gurus during the boom was that 'the Internet changes everything'. Andy Grove, co-founder of Intel, created a storm with his prediction that 'companies that aren't Internet companies by 2005 won't be companies at all' – i.e. will go out of business.<sup>34</sup> These kinds of slogans are a poor substitute for thought. The truth is that the Internet changes some aspects of doing business while leaving others relatively untouched.

It can dramatically reduce transaction costs, for example, in ways that may have long-term implications for the structure of firms and their supply chains. It increases transparency by making product and price information available to consumers, which in turn *may* exert increased competitive pressure on suppliers. This may make the markets for some types of goods more competitive, if only because consumers can be more fickle and switch easily from one supplier to another.

In addition to making existing business processes more efficient, the Internet can also make it possible to create new kinds of businesses – i.e. businesses that would not be possible without it. The best-known example to date is probably the reverse-auction models like LetsBuyIt.com which enable customers to band together to obtain bulk discounts for goods.

On the other hand, the Net doesn't suspend the laws of economic gravity. Online traders have to generate revenues and (ultimately) profits. And the Net does not eliminate the need for 'bricks and mortar' shops, or for execution systems that can reliably deliver goods to customers, provide after-sales support and so on.

There is much talk about an 'information economy', and information as a commodity seems very different to physical goods. It can take a lot of upfront investment to create an information good (Windows XP, say, or a feature film), but thereafter it costs almost nothing to stamp out copies. Likewise, distribution of information goods over the Net costs

almost nothing. And consumption of information does not deplete the supply. To that extent, an economy based on information goods requires different analytical tools.<sup>35</sup>

We should also be wary of confusing what the Net is capable of doing with what is actually happening. For example, one of the articles of faith of 'Webonomics' is that the Net has great power to disintermediate – i.e. to cut out the middlemen in many transactions and enable producer to sell directly to end user. Well, so it does. But look at what's happening on the ground. Those middlemen threatened with disintermediation are not sitting by idly; instead they are using judicial, regulatory, and legislative means to thwart competitors who seek to use the net to sell a product or service. For example, US car dealers have succeeded in getting 49 states to pass laws preventing auto manufacturers from selling cars online. Wine wholesalers have lobbied Congress and the states to prevent wineries from selling wine over the net.<sup>36</sup> And so on.

Overall, the extent of the Internet's economic significance remains a contested issue. Robert Gordon, for example, has argued persuasively that computers and the Internet have had much less impact on society than earlier technologies such as electricity, motor and air transport, motion pictures, radio and indoor plumbing.<sup>37</sup>

### **Impact of e-commerce on anonymity and privacy**

The Internet's libertarian characteristics are a product of the network's technological architecture. But if the underlying architecture were to change, then its usefulness to civil society might be reduced. There are compelling reasons to suppose that the development of e-business poses a major threat, because online commerce requires modification of the existing 'permissive' architecture in ways that will make it a more controlled space.

The problem is that a space in which 'nobody knows you're a dog' is not an environment in which one can safely trade. E-commerce requires security, authentication and confirmation of transactions. An online trader needs to know with whom he or she is dealing; messages and transactions have to be secure from surveillance and interference; contracts have to be legally enforceable and incapable of arbitrary repudiation; ways have to be found for appending 'digital signatures' which have legal validity to electronic documents; and so on.

Technical solutions exist for all of these requirements, though many of them are currently rather clumsy. But the economic imperatives of online commerce are so urgent that vast improvements in the necessary protocols are under way. An entire new technical

architecture to facilitate e-commerce is being created, in other words, ready to be grafted onto the older, libertarian architecture of the Net. And therein lies the danger.

The implication is that the Internet in 2005, say, could look very different from the Internet as it was in 1995. The old – libertarian -- layer will still exist, but a new layer – the e-commerce stratum – will sit above it. And the values implicit in the architecture of this new layer will be radically different from those embodied by the old one.

However, it is already clear that the rise of e-commerce will have significant impact in some areas – particularly in the area of privacy.

### **THE END OF ANONYMITY**

The key difference will be that the new layer will adapt the technical facilities of the old layer to eliminate anonymity and erode privacy. Again, an understanding of the technology is vital to appreciate how this might happen. At present, every machine on the network has a unique address for the duration of its connection, and every transaction that machine conducts leaves a record. When an individual requests a Web page from a site for example, the address of the requesting machine and the nature of its request are logged by the server. Anyone who runs a web site can therefore find out the address of every machine which has accessed his or her site. What they cannot ascertain, however, is the *identity* of the persons who initiated those accesses.

But the new e-commerce layer could change all that. It would enable sites, for example, to refuse access to people who refused – or were unable -- to provide a digital signature authenticating their identity.<sup>38</sup> Once admitted, everything those authenticated visitors did – which web pages they viewed, and for how long, which items they purchased, what they appeared to be most interested in, and so on – can be logged against their real identities. And of course the information thus gathered could be sold or disclosed to other agencies – and all without the subjects' knowledge or consent. And because all the information gathered within such a layer would be in machine-readable form, it would be technologically and economically feasible to compile massive databases on the online behaviour of named individuals.

This possibility will be further reinforced by forthcoming changes to the Internet's address space. The explosive growth of the Net means that the world is rapidly running out of Internet addresses. Accordingly, a new version of the address protocol – IPv6 – is now being implemented. This provides a vast address space, but also includes a provision for an expanded IP number, part of which is the unique serial number of each computer's

network-connection hardware, thereby making it possible in principle to track the online behaviour of every connected device.

#### **ANONYMOUS READING AND PRIVACY**

The erosion of privacy implicit in such systems is an obvious danger. Less obvious, perhaps, is their potential for limiting access and widening the 'digital divide' between those who have a foothold in the new economy and those who do not. Apologists for the new e-commerce layer point out that nobody will be forced to have a digitally-authenticated signature and that they don't have to visit any site which requires one. True. Neither is there an obligation on anyone to have a credit card – but try renting a car or checking into an hotel nowadays without one.

Add to the authentication threat the provisions for digital copyright which the publishing industries are demanding from legislatures around the world and one can see the makings of an Orwellian nightmare. Every document published on the Web can be encrypted, so that only readers who have paid for a decryption key can access it. Alternatively, an unencrypted document can have a secret 'digital watermark' embedded in it, enabling publishers to tell at once whether a given digital copy is a legitimate, paid-for, version or a pirated one. And even if the document is published free, unencrypted and unmarked, on a Net where authentication protocols are in place the publisher could determine the precise identity of every single person who accesses the document online – and sell that information to other customers, or abuse it in other ways. With such an architecture, the practice of anonymous reading – one of the great bulwarks of intellectual freedom -- could be rendered impossible, at least in relation to online documents.

The inescapable implication is that Cyberspace -- the most open, uncensored and unregulated public space in human history – could easily become the most controlled environment imaginable. Or, to use Lessig's phrase, 'the invisible hand of cyberspace is building an architecture that is quite the opposite of what it was at cyberspace's birth. The invisible hand, through commerce, is constructing an architecture that perfects control'.<sup>39</sup>

## **Intellectual Property Rights (IPRs)**

When the Internet first appeared on corporate radars, it was universally seen as a threat to IPRs. Publishing organisations regarded the Web as a global machine for making and circulating bootleg copies of texts, music, videos and software. Their response has had three strands:

- Aggressive legal action – for example the successful action to shut down Napster – aimed at punishing and outlawing infringements of IPRs.
- Intensive lobbying of compliant legislatures (the US Congress, European Parliament) to pass legislation (for example the US Digital Millennium Copyright Act) extending the rights of copyright owners.
- Intensive research into technological ways of preventing piracy.

There is already evidence that this strategy is resulting in what amounts to a ‘copyright land grab’ -- in which rights owners are not just consolidating their hold on their property, but clawing back the ‘fair use’ and other concessions which have been hammered out over a century and a half. It is conceivable therefore that the digital revolution which originally threatened to undermine copyright protection could in fact be used to undermine the rights of readers and consumers, restrict the free circulation of ideas and even limit the rights of academic researchers to publish the results of their research.<sup>40</sup>

If we are indeed moving towards an ‘information society’, then it’s hardly surprising that intellectual property is becoming as central to our concerns as land or industrial capital were in earlier times. This has led some commentators like James Boyle to argue that ‘intellectual property and its conceptual neighbours may bear the same relationship to the information society as the wage-labor nexus did to the industrial manufacturing society of the 1900s’.<sup>41</sup> And we might find that a technology that once threatened to undermine copyright ends up reinforcing it in ways once thought unimaginable.

## Security and vulnerability in a digital age

The Internet is intrinsically an open – and therefore insecure -- system. And although encryption, firewalls and other technologies can make it less insecure, the only way of guaranteeing that a network is safe from online penetration is to disconnect it from the Net, which rather undermines the whole point of being online. If – as many informed commentators expect – the Internet continues to spread and becomes essentially ubiquitous in economic and social life, then the inescapable conclusion is that our societies are going to be increasingly dependent on a fragile and insecure information infrastructure.

The ease with which relatively unsophisticated ‘Distributed Denial of Service’ attacks have crippled major e-commerce sites in 2000-01 provides a graphic illustration of these vulnerabilities.<sup>42</sup> Given that, it is likely that the military establishments of most states are researching the offensive and defensive aspects of Information Warfare (IW). A study of the subject by the RAND Corporation for the US Department of Defense<sup>43</sup> concluded that

'key national military strategy assumptions are obsolescent and inadequate for confronting the threat posed by strategic IW'. The low entry costs to the IW business will also make it attractive to rogue states and terrorists using aggressive hacking and network penetration techniques in preference to more conventional weapons. The RAND study indicates that these risks are taken seriously in national security circles, but up to now they have not been much discussed in the mass media. Sooner or later, though, they will have to become the focus of political discussion.

## Notes

---

<sup>1</sup> Copies of this paper in various formats are available at <http://molly.open.ac.uk/21c/>

<sup>2</sup> Systems Group, Faculty of Technology, The Open University and Wolfson College, Cambridge. .E-mail: [Naughton@pobox.com](mailto:Naughton@pobox.com). Web: [molly.open.ac.uk](http://molly.open.ac.uk)

<sup>3</sup> Shiller, Robert, J: *Irrational Exuberance*, Princeton University Press, 2000.

<sup>4</sup> Neil Postman, *The Invention of Childhood*, Vintage, 1994.

<sup>5</sup> Naughton, John: *A Brief History of the Future: the origins of the Internet*, Phoenix, 2001, pages

<sup>6</sup> Transmission Control Protocol / Internet Protocol. The Internet works by breaking messages into small parcels of data known as packets and then passing those packets through the system until they reach their destination. TCP takes care of the disassembly of messages in to packets at the transmission end and their reassembly at the receiving end. IP handles the addressing of data packets.

<sup>7</sup> For example the ALOHA network in Hawaii, the Cyclades network in France and the NPL network in the UK's National Physical Laboratory.

<sup>8</sup> Naughton, *op. cit.*, page 248.

<sup>9</sup> The 'end-to-end argument' was articulated by network architects Jerome Saltzer, David Reed and David Clark in 1981 as a principle for allocating intelligence within a large scale computer network. It has since become a central principle of the Internet's design. See [lawschool.stanford.edu/e2e/](http://lawschool.stanford.edu/e2e/).

<sup>10</sup> The term 'internetwork' was quickly shortened to the less cumbersome 'Internet'.

<sup>11</sup> Lessig, Lawrence, "Open Code and Open Societies: The Values of Internet Governance", 1999 Sibley Lecture, University of Georgia, Athens, Georgia, February 16, 1999.

<sup>12</sup> A number made up of four sets of digits – e.g. 255.212.12.40. Computers accessing the Net via dial-up lines are assigned temporary IP addresses from a bank held by their Internet Services Provider (ISP). Computers on local area networks generally access the Net through a gateway machine so that all transactions by an individual machine are logged against the IP address of the gateway computer.

<sup>13</sup> For example, the use of the Internet by a disaffected MI5 operative, David Shayler, to publicise his case. See [www.guardianunlimited.co.uk/shayler/](http://www.guardianunlimited.co.uk/shayler/).

<sup>14</sup> Lessig, Lawrence, *Code and other Laws of Cyberspace*, Basic Books, 1999.

<sup>15</sup> See [www.nua.ie](http://www.nua.ie)

<sup>16</sup> In June 2001, Google, a leading search engine, was claiming to index 1,346,966,000 Web pages, which it estimated as about half of the total number of Web pages published at that time. Other estimates of the total number of Web pages are much higher.

<sup>17</sup> E.g. minidisk recorder, still camera, video camera, scanner.

<sup>18</sup> Though of course there are bandwidth (channel capacity) limitations – i.e. users with slow dial-up connections will take much longer to access non-text files.

<sup>19</sup> Because originally they were used for circulating news about bugs and updates to managers of Unix systems.

<sup>20</sup> [www.linuxdoc.org/LDP/nag/node258.html#SECTION0018300000](http://www.linuxdoc.org/LDP/nag/node258.html#SECTION0018300000)

<sup>21</sup> File Transfer Protocol – one of the oldest Internet protocols. FTP provides a relatively fast and reliable way of exchanging files over the Net. Most software downloads are handled by FTP.

<sup>22</sup> *Ibid.*

- 
- <sup>23</sup> Miller, Daniel and Don Slater, *The Internet: An Ethnographic Approach*, Oxford, 2000.
- <sup>24</sup> The report was issued by research firm Jupiter Media Metrix. See [www.jup.com/company/pressrelease.jsp?doc=pr010604](http://www.jup.com/company/pressrelease.jsp?doc=pr010604)
- <sup>25</sup> See Oram, Andy (Ed.), *Peer-to-Peer: Harnessing the Power of Disruptive Technologies*, Sebastapol: O'Reilly Associates, 2001. See [www.ora.com](http://www.ora.com) for details.
- <sup>26</sup> The 1999 Report of the UN Development Program estimates that only 2% of the world's population had Internet access in mid-1998. Higher estimates are based on a user population of 400 million.
- <sup>27</sup> UNDP, Human Development Report 1999, p. 62.
- <sup>28</sup> *ibid*
- <sup>29</sup> UNDP Report, p.58.
- <sup>30</sup> As expressed, for example, in John Perry Barlow's celebrated 1996 'Declaration of the Independence of Cyberspace' which begins: '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.' For the full text, see [www.eff.org/~barlow/Declaration-Final.html](http://www.eff.org/~barlow/Declaration-Final.html)
- <sup>31</sup> John Gilmore's observation that 'the Internet interprets censorship as damage and routes around it' captured this sentiment precisely.
- <sup>32</sup> For more information about the RIPA see [www.fipr.org/rip/](http://www.fipr.org/rip/)
- <sup>33</sup> See Levy, Stephen, *Crypto: Secrecy and Privacy in the New Code War*, Allen Lane, 2000.
- <sup>34</sup> Grove is still at it. The cover story in a recent issue of *Wired* magazine claims that his latest message is 'believe in the Internet more than ever'.
- <sup>35</sup> For a good guide see Shapiro, Carl and Hal Varian, *Information Rules: A Strategic Guide to the Network Economy*, Cambridge: Harvard Business School Press, 1998.
- <sup>36</sup> Atkinson, Robert D., "The failure of Cyberlibertarianism: the case for a national e-commerce strategy", Progressive Policy Institute, June 1, 2001. Available at: [www.ppionline.org/documents/E-com\\_Strategy.pdf](http://www.ppionline.org/documents/E-com_Strategy.pdf)
- <sup>37</sup> Gordon, Robert J., "Does the 'New Economy' Measure up to the Great Inventions of the Past?", available online at: [faculty-web.at.nwu.edu/economics/gordon/351.html](http://faculty-web.at.nwu.edu/economics/gordon/351.html)
- <sup>38</sup> This has already happened with the UK government's key 'Gateway' web site via which citizens are supposed to conduct electronic transactions with government departments. In its first manifestation [Spring/Summer 2001], the site allows only those users running Microsoft software to use its authentication services. See [www.observer.co.uk/business/story/0,6903,504363,00.html](http://www.observer.co.uk/business/story/0,6903,504363,00.html) for details.
- <sup>39</sup> Lessig, *op. cit.*, p.6.
- <sup>40</sup> See Naughton, John, "The American Crocodile that Swallowed Freedom", *Observer*, April 29, 2001. Available at: [www.observer.co.uk/business/story/0,6903,480027,00.html](http://www.observer.co.uk/business/story/0,6903,480027,00.html)
- <sup>41</sup> Boyle, James, *Shamans, Software and Spleen: Law and the construction of the Information Society*, Cambridge: Harvard University Press, 1997, page 13.
- <sup>42</sup> See [grc.com/dos/grcdos.htm](http://grc.com/dos/grcdos.htm) for a vivid case study.
- <sup>43</sup> Molander, Roger C., Andrew S. Riddile and Peter A. Wilson, "Strategic Information Warfare: A New Face of War", available at [www.rand.org/publications/MR/MR661/MR661.html](http://www.rand.org/publications/MR/MR661/MR661.html)