Regulation of decentralised networks:
Necessities and problems for freedom of the media

Sandy Starr, ***spiked***
Sandy.Starr@spiked-online.com

Presentation to the OSCE conference on 'Freedom of the media and the internet', Amsterdam, 14 June 2003

1. Introduction

When I was asked to speak on the subject of 'Regulation of decentralised networks: Necessities and problems for freedom of the media', my initial reaction was very simple. In order for the media to be free, it is *necessary* that decentralised networks should *not* be regulated, and it is a *problem* if people think that they *should*.

But I if I left it at that, my presentation would be a bit short. So I'll try to elaborate.

On the surface, there appears to be a lot of healthy debate about internet regulation and internet freedom these days. We have organisations like the OSCE, putting on conferences like this, where we look at the dangers of freedom of the media being undermined. We have a diverse number of civil liberties organisations and lobby groups, who campaign internationally against draconian forms of internet regulation and internet surveillance. And we have governments and regulators taking the internet seriously, and looking at the detail of how their policy affects the internet.

But if you look beneath the surface, I think you'll find that the state of debate about internet regulation is less healthy than it looks. And I want to look at four broad, related reasons why I think this is:

- *Those who favour internet regulation today harbour false assumptions*
- *Those who oppose internet regulation today harbour false assumptions*
- *Both those who favour internet regulation and those who oppose it fail to distinguish the state from other actors*
- *Both those who favour internet regulation and those who oppose it assume that individuals are generally weak and require protection*

2. Those who favour internet regulation today harbour false assumptions

When the dotcom bubble burst, there was a widespread and unhelpful sense of *schadenfreude*. The general sentiment seemed to be: 'You had it coming – we told you the dotcom boom couldn't last forever.' Similarly, since the dotcom bubble burst, and particularly since the terrorist attacks of 11 September 2001, there has been a smug sentiment among those who favour internet regulation: 'You had it coming – we told you the internet couldn't remain an unregulated wild west forever.'

It's true to say that the internet has posed a special challenge to regulators, and that in the past, it has enjoyed a certain exceptional freedom from regulation – just as earlier publishing and communications tools did, when they first emerged.[1] But it would be a

[1] See 'A brief history of censorship', Christopher Hunter, in *Filters and Freedoms 2.0: Free Speech Perspectives on Internet Content Controls*, Electronic Privacy Information Centre, Washington: Electronic Privacy Information Centre, 2001, pp33-42; and 'From quill to cursor: freedom of the media in the digital era', Karin Spaink, in *From Quill to Cursor: Freedom of the Media In the Digital Era*, Organisation for Security and Cooperation in Europe, Vienna: Organisation for Security and Cooperation in Europe, 2003, pp9-30 [http://www.osce.org/documents/rfm/2003/04/41_en.pdf]

mistake to characterise this as a bad thing. In fact, I think it's an entirely good thing. New publishing and communications technologies force us to question the principles and assumptions that underlie the way we regulate speech and association.

Unfortunately, I believe that we've turned down the opportunity to answer the questions that the internet has posed to us and is continuing to pose to us. Instead, we're attempting to silence the internet – to prevent it from asking us uncomfortable questions. And in this, sadly, we're succeeding.

The internet has provided us all with an unprecedented opportunity to encounter new individuals, experiences and ideas, with little interference from any authority presuming to decide on our behalf what's good for us. If only for this, the internet should be championed – even if it's true to say that many of the internet's early champions were utopian and idealistic.

Yes, John Perry Barlow was naïve when he issued his 'Declaration of the independence of cyberspace' in 1996, a document whose opening lines were:

> '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.'[2]

You can sense in these words a certain narrow-minded projection, by the wired-up digerati, of their elite inner world on to the world around them – and at the same time, a fear that their inner world would be contaminated. But Perry Barlow's words also contain a fundamentally democratic aspiration, for a sphere where people can mingle and exchange ideas without interference or censure.

This aspiration is different from today's more touchy-feely discussions of edemocracy, social inclusion, cultural preservation, and how to close the 'digital divide'. This original aspiration doesn't presume to help people use the internet to empower themselves – after all, if you empower somebody on their behalf, that's hardly empowering for them, is it? This aspiration merely asks that decentralised networks be preserved as a place where people can communicate and associate freely.

Sadly, but predictably, the authorities had other ideas. When they found themselves frustrated by decentralised networks, and up against the limits of what traditional forms of media regulation can achieve with decentralised networks, their response was not to throw their hands up in despair and give up – which is probably what John Perry Barlow hoped would happen. Rather, the response of the authorities was to introduce methods of regulation that mimicked the decentralisation of the network.

It was therefore useful to the authorities, when regulation devolved from accountable arms of the state to para-state, international and industry bodies. Never mind protesting to a court of law that your content has been suppressed – you have to talk to your internet service provider (ISP); who (if you're lucky) will refer you to their terms and conditions; before (if you're lucky) passing you on to the Internet Watch Foundation (UK), the Internet Service Providers Association of Ireland Hotline (Ireland), Stopline (Austria), the Internet Hotline Against Child Pornography (Netherlands), the Northern Hotline (Finland), the CyberTipline (USA), the Australian Broadcasting Authority (Australia), or some other similar body; who will then (if you're lucky) refer you back to the individual who complained to them about your content to

[2] 'A declaration of the independence of cyberspace', John Perry Barlow, Electronic Frontier Foundation, 8 February 1996 [http://www.eff.org/~barlow/Declaration-Final.html]

begin with, and who could have had any reason for doing so, but whose given reason was accepted in good faith.[3]

Or perhaps it was sufficient, under existing law, for an individual or organisation to complain directly to your ISP, and then the ISP removed your content for fear of being financially liable for something illegal. This would certainly be the case if it had been alleged that your content was copyright-infringing, because in a growing number of countries, your ISP would then have been forced to accept the complaint in good faith and remove the content, or else risk being financially liable for copyright infringement.

Under the USA's Digital Millennium Copyright Act, you at least have a mechanism whereby you can demand that content removed in this way is put back, and so you can force the dispute into a court of law.[4] The equivalent European legislation, contained in the Ecommerce Directive, doesn't even give you that.[5]

Don't get me wrong – I don't love courts of law, and the courts of law in which disputes over content have traditionally been resolved never offered a guarantee of justice being served. Nor is a court of law the best place to take a dispute, of any kind – far from it.

But where regulation is concerned, courts of law often offer the individual the most equitable footing available, in an otherwise unequal society. The minimum requirement for a fair hearing is a separation between the party pursuing a grievance, and the authority presiding over the case – which is something you don't get with self-regulation.

When regulation mimics the decentralisation of networks, and devolves into self-regulation, such quaint notions as the presumption of innocence, the right to free speech, and the importance of fair use, are dismantled. Those who favour internet regulation would have it that such dismantling is necessary, because otherwise, content transmitted and shared in decentralised networks would – heaven forbid – go unregulated.

But this assumption is entirely the wrong way around. Far from it being the case that political and legal principles should be dismantled in the face of new technology, we should be asking ourselves: what can new technology remind us about the essence of our political and legal principles?

- *If it is becoming increasingly difficult to police hateful and prejudiced opinions on the internet, do we conclude that we need tougher penalties for those who express such opinions? Or do we recognise that human beings are rational actors, capable of exercising judgement about what they read, watch, listen to and download, and that –*

[3] See the Internet Watch Foundation [http://www.iwf.org.uk], Internet Service Providers Association of Ireland Hotline [https://www.hotline.ie], Stopline [http://www.stopline.at], Internet Hotline Against Child Pornography [http://www.meldpunt.org], Northern Hotline [http://www.pela.fi], CyberTipline [http://www.missingkids.com/missingkids/servlet/PageServlet?LanguageCountry=en_US&PageId=169], and Australian Broadcasting Authority [http://www.aba.gov.au] websites

[4] See the Digital Millennium Copyright Act (HR 2281), 1998, Title II, Sec 202 [http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=105_cong_public_laws&docid=f:publ304.105.pdf]

[5] See Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market (Directive on Electronic Commerce), Article 14 [http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_178/l_17820000717en00010016.pdf]

in the words of one senior UK judge – 'freedom only to speak inoffensively is not worth having'[6]*?*

- *If ISPs are the only easily identifiable actors in the hosting and making available of content, do we conclude that ISPs deserve to be treated as publishers, and deserve heavy legal burdens and penalties? Or do we recognise that ISPs have a fundamentally different relationship to content than traditional publishers do, and that in any case, restricting speech is inimical to a healthy democracy?*
- *If the content industry claims that the unauthorised digital distribution of content is damaging its profits (a claim which, incidentally, has yet to be proven*[7]*), do we conclude that the internet should be shackled and dragged back in time, until it resembles older publishing and communications technologies? Or do we conclude that the content industry has long been lazily dependent on the shortcomings of technology for its profits, and now needs to become more inventive?*
- *If child pornography is the issue that provokes the greatest moral outcry and call for internet regulation worldwide, do we see it as the ultimate justification and benchmark for internet regulation? Or do we acknowledge that child pornography is the most talked about, but also the least understood or rationally evaluated, problem on the internet, so that even the director of the Combating Internet Paedophiles in Europe project admits 'it is difficult to find another area of substantial policy development that has been based on such little empirical evidence'*[8]*?*

3. Those who oppose internet regulation today harbour false assumptions

Having said all of that, I also intend to give the opponents of internet regulation a hard time. There's an unhelpful smugness among many of the technologically literate, where they assume that ultimately, decentralised networks simply cannot be regulated – that they are intrinsically resistant to regulation. At the heart of this assumption is technological determinism, where technology is thought to be the independent variable in social change, rather than people.

Even my colleague Felipe Rodriguez, founder of XS4ALL, whose views I otherwise largely agree with, succumbs to this fallacy. He correctly points out that 'effective censorship on the internet is incredibly difficult'[9], and that in order to achieve effective censorship in China, 'the government employs as many as 30,000 people to enforce internet censorship'[10]. But he concludes falsely from this that on the internet, 'any censorship can, and will, be defeated'[11].

From such a conclusion comes the lazy belief that free expression on the internet will be protected by technical default, rather than as a result of principled conviction and

[6] Judgement of Lord Justice Sedley in the case of *Redmond-Bate v DPP*, 23 July 1999, reported in *The Times* (London) law report, 28 July 1999

[7] See 'RIAA's statistics don't add up to piracy', George Ziemann, Mac Wizards Music, 11 December 2002 [http://www.azoz.com/music/features/0008.html]

[8] 'Child Pornography and the Internet: Challenges and Gaps', Max Taylor, Combating Internet Paedophiles in Europe, December 2001 [http://copine.ucc.ie/attachments/challenges.pdf]

[9] 'Burning the village to roast the pig: censorship of online media', Felipe Rodriguez, in *From Quill to Cursor: Freedom of the Media In the Digital Era*, Organisation for Security and Cooperation in Europe, Vienna: Organisation for Security and Cooperation in Europe, 2003, p86 [http://www.osce.org/documents/rfm/2003/04/41_en.pdf]

[10] Ibid, p93

[11] Ibid, p108

argument. This is entirely wrong. It may be difficult to regulate decentralised networks, but experience tells us that wherever such networks *can* be regulated, they *will* be regulated. However insignificant such regulation may initially appear, it can have an insidious effect, as dangerous precedents are set.

The legal theorist Lawrence Lessig puts it best, when he talks about the fallacy that 'the net has a nature, and that nature is freedom'. In truth, Lessig argues, 'the possible architectures of cyberspace are many.... Some architectures make behaviour more regulable; other architectures make behaviour less regulable.'[12] In other words, freedom is not the essence of the *technology* of decentralised networks, but rather is the essence of the *human principles* that guide the development of decentralised networks.

There are two levels at which freedom in decentralised networks might be undermined, if we fall back on the assumption that the technology will look after our freedom for us. The first is self-regulatory regimes – the exporting of regulation into the marketplace, where regulation disappears from public view, and from the court of public opinion. As I described earlier, when it comes to decentralised networks, governments find it useful to export their regulatory tasks to the marketplace – for example, by imposing ambiguous liabilities upon ISPs, that make ISPs regulate out of fear.

Such invisible regulation is more of a problem than you might initially think. Yes, if you're a techno-literate activist and your ISP removes something from your website, you can kick up a stink on the SLAPPs section of the Electronic Frontier Foundation website[13], or on the Chilling Effects Clearinghouse website[14]. But if you can't be bothered to contest the removal of content from your website, or if you don't understand that the content might have been removed wrongfully, then that means that nobody else in the world will ever see that content – or even know that it existed. Self-regulation has a chilling effect upon free expression for *all* internet users, not just content providers and customers of ISPs.

The second level at which freedom in decentralised networks might be undermined is the purely technical. Just because hackers and crackers always seem to be able to find a way to get around encryption and evade the authorities, is no reason to assume that subtle changes can't be made, at the level of technology, that result in a less free internet overall. Besides, hackers and crackers are a techo-literate minority – while their activities might be significant, they are not necessarily a reliable barometer of the freedom generally exercised on the internet.

There's not even any reason to assume that the most fundamental standards and protocols that enable the internet to function couldn't be changed in some way, to work against freedom. These standards and protocols are neither eternal nor God-given – somebody had to make them, and somebody can unmake them. Just because the Internet Engineering Task Force and related standards-developing organisations are international communities, open to any interested individual, doesn't mean that the gulf that separates them from the exercise of political interest can't be traversed – or hasn't been traversed in some way already.[15]

[12] *Code and Other Laws of Cyberspace*, Lawrence Lessig, New York: Basic Books, 1999, p30

[13] See the the SLAPPs section of the Electronic Frontier Foundation website [http://www.eff.org/IP/IP_SLAPP]

[14] See the Chilling Effects Clearinghouse website [http://www.chillingeffects.org]

[15] See the 'Internet Engineering Task Force overview' section of the Internet Engineering Task Force website [http://www.ietf.org/overview.html]

One final fallacy, that stems from the technological determinism of those who oppose internet regulation, is the notion that civil disobedience is equivalent to a proper political debate. Another version of this fallacy is that if you get *mass* civil disobedience, then *that* must be equivalent to a proper political debate – which was a popular notion surrounding the Napster controversy of recent years, where large numbers of people were, strictly speaking, flouting copyright law by downloading files from Napster.

Yes, civil disobedience can be important to politics, and I'm the last person to denigrate it. But unless civil disobedience is accompanied by informed and principled political debate, there is a danger that it will result merely in an escalation of cynicism on both sides of a dispute[16], and will encourage the authorities to respond in an even more authoritarian manner. Civil disobedience without proper debate also lets the authorities off the hook, by failing to engage with them intellectually.

4. Both those who favour internet regulation and those who oppose it fail to distinguish the state from other actors

As I've mentioned, we live in a time where self-regulation by private commercial bodies can be coopted in the service of state regulation by public statutory bodies. An excessive example of this can be found in the European Ecommerce Directive, which not only enforces regulation of online copyright infringement by the marketplace, but also passes the responsibility for coming up with the specifics of the regulatory system it enforces to the marketplace.[17]

So as you can see, in practice, state regulation and industry regulation have become somewhat confused. In an age of international law and international regulatory bodies, it has also become more difficult to characterise our political elite as acting in the interests of the nation state. But none of this is any reason to cease being suspicious of state interests, and of the state's latitude to interfere in our freedoms. If anything, these developments give us more reason to be wary of the state, because state interests aren't always easily discernible.

Unfortunately, it's a particular weakness of contemporary discussions about internet regulation, that the state is treated as simply one element of an amorphous, oppressive blob that supposedly threatens our freedoms on all sides. While this notion is very good at making us all paranoid, it doesn't leave us with any perspective on genuine threats to our freedom.

As individuals, we exist in an equal relationship to one another, and in an unequal relationship to commercial organisations. When commercial organisations are responsible for technology that shapes the way many of us communicate and interact

[16] The academic Siva Vaidhyanathan argues that the cynicism of hackers and other online activists actually has noble roots 'in ancient Greece where Diogenes of Sinope was exiled from Athens for masturbating in the marketplace in the 4th century BCE'. While I disagree with him as to whether these roots are honourable, I find the parallel he draws entirely apt. See 'The contract of copyright: towards an ethical cynicism?', Siva Vaidhyanathan, openDemocracy, 10 August 2002 [http://www.opendemocracy.net/articles/ViewPopUpArticle.jsp?id=8&articleId=245]

[17] The Directive states that governments must 'encourage...the drawing up of codes of conduct...by trade, professional and consumer associations or organisations' for copyright regulation. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market (Directive on Electronic Commerce), Article 16.1 (a) [http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_178/l_17820000717en00010016.pdf]

online – as is conspicuously the case with Microsoft Corporation – then we are right to be critical of those commercial organisations.

But the potential threat to freedom posed by a single actor in the marketplace, motivated by profit – however important or successful that actor may be – is of a different, and far inferior order of magnitude, than the potential threat to freedom posed by the state, motivated by politics.

This distinction, between threats to freedom from the marketplace and threats to freedom from the state, has been blurred by the framework of human rights, as codified in international (and latterly, national) law since the Second World War.[18] Within this framework, the state is characterised as a benevolent actor, proactively enforcing our freedoms on our behalf. But unless we grasp the distinction between state and marketplace, we will always find ourselves fighting a losing battle for freedom, when it comes to decentralised networks.

A good example to illustrate this, which brings together the internet, the confusion of state and commerce, and the framework of human rights, is the current debate about privacy on the internet. One of the more highly regarded publications among privacy campaigners is *Privacy and Human Rights: An International Survey of Privacy Laws and Developments*, an annual report on the global state of privacy conducted by the Electronic Privacy Information Centre and Privacy International.[19] The 2002 edition of this report opens with the bold statement: 'Privacy is a fundamental human right.'[20]

The research that has gone into the report is phenomenal – it provides a detailed catalogue of erosions of privacy in 53 different countries. But while the report focuses on national laws relating to privacy, it makes no categorical distinction between the significance of laws pertaining to incursions upon privacy by the state, and laws pertaining to the regulation of business practice. The implication is that the greater the number of laws, of any kind, enforcing privacy, the better for the individual.

This implication is problematic. We can, and should, aspire to comprehensive privacy from the state. But our privacy from the marketplace is always qualified, because as long as we consume goods and services, then to some extent our private pursuits occur within the marketplace. Shoddy business practice deserves to be criticised, but lambasting the marketplace simply for using our personal information in pursuit of profit not only downplays the importance of privacy intrusions by the authorities – it implicitly calls upon the state to do more to invade our privacy, in order to protect us from other people and organisations.

The paradox at the heart of privacy legislation is that by definition, the authorities cannot do anything proactive about our privacy without undermining it.[21] It is unfortunate, then, that instead of prescribing limits to state power in order that individual freedom may flourish, human rights legislation directly prescribes the rights that individuals are entitled to exercise. Where the First Amendment to the US

[18] For an excellent critical history of human rights, see *The Rise and Rise of Human Rights*, Kirsten Sellars, Stroud: Sutton Publishing, 2002

[19] See the Electronic Privacy Information Centre [http://www.epic.org] and Privacy International [http://www.privacyinternational.org] websites

[20] *Privacy and Human Rights: An International Survey of Privacy Laws and Developments 2002*, Sarah Andrews (ed), Washington/London: Electronic Privacy Information Centre/Privacy International, p1 [http://www.privacyinternational.org/survey/phr2002/phr2002-part1.pdf]

[21] See 'Privacy: open up the debate', Sandy Starr, *spiked*, 8 October 2002 [http://www.spiked-online.com/printable/00000006DA9B.htm]

Constitution begins 'Congress *shall make no law*...'[22], Article 1 of the European Convention for the Protection of Human Rights and Fundamental Freedoms begins 'The High Contracting Parties *shall secure to everyone*...'[23].

Some would argue that even if you believe in the importance of separating threats to freedom from the state and threats to freedom from the marketplace, such a distinction has been made redundant in any case, by information technology. When significant quantities of personal information can be easily circulated digitally, does it really matter who captures or misuses that data? After all, if the data could end up anywhere, isn't the important thing to prevent it from being captured or misused to begin with?

There are some good examples that initially appear to back up this argument. For instance, the leading auction website eBay has a policy of handing over to the authorities any requested information about its users gathered since 1995, without even insisting upon a court order.[24] And in the UK, there have been instances of the authorities selling data from the electoral register – which everyone over the age of 18 is obliged to fill in, unless they are mentally ill – to commercial organisations.[25] In the first instance, a commercial organisation is passing on personal information to the state; in the second instance, the state is passing on personal information to commercial organisations.

But despite this, the distinction between the threats to privacy posed by the state and by the marketplace remains crucial. In the two examples I have given, commercial organisations deserve to be criticised for poor business practice, and the state deserves to be criticised for the far more serious matter of invading our privacy. While there is a legitimate discussion to be had about the commercial management of personal information in an age of new technology, this is an entirely separate question from the limits that should be placed on state snooping.

Even when unscrupulous companies misuse our personal information, such misuse is motivated by fairly narrow business concerns. A telling passage in the *Privacy and Human Rights* report, which explains how 'companies...sell, trade or share...information among third-party companies without the consumer's expressed knowledge or consent', goes on to note that 'the perceived value of this kind of information is behind the stock market valuations of many dotcom companies'[26]. Companies are not conspiring to invade our lives, but rather are nervously trying to cover up their flimsy business models.

If there's a single institution that you can guarantee leads to a confusion over threats to internet freedom, whenever it is discussed, then that institution is Microsoft

[22] Amendments to the Constitution of the United States of America, Article I, my italics [http://www.house.gov/Constitution/Amend.html]

[23] Convention for the Protection of Human Rights and Fundamental Freedoms as Amended by Protocol no 11, Council of Europe, Article 1, my italics [http://conventions.coe.int/Treaty/en/Treaties/Html/005.htm]

[24] See 'Big Brother is watching you – and documenting', Yuval Dror, *Ha'aretz*, 20 February 2003 [http://www.haaretz.com/hasen/pages/ShArt.jhtml?itemNo=264863]

[25] This practice has been outlawed – in theory, at least – by the ruling in the case *of R v City of Wakefield Metropolitan Council* (16 November 2001), where it was judged to be a contravention of the Data Protection Directive and the Convention for the Protection of Human Rights and Fundamental Freedoms

[26] *Privacy and Human Rights: An International Survey of Privacy Laws and Developments 2002*, Sarah Andrews (ed), Washington/London: Electronic Privacy Information Centre/Privacy International, p59 [http://www.privacyinternational.org/survey/phr2002/phr2002-part1.pdf]

Corporation. It is beyond the scope of this paper to comment on the anti-trust proceedings that have dogged Microsoft from June 2000 to the present[27], but I will venture to say that misguided, knee-jerk criticism of Microsoft has posed an obstacle to rational discussion of both the company's achievements and its failings.

Microsoft is far from a perfect organisation. Indeed, it deserves serious criticism – among other things, for its initiatives in the area of digital rights management, and in the area of trusted computing (a subject I will return to in a moment). But nor is Microsoft the antichrist, as many people seem to believe. Criticism of Microsoft today goes beyond concerns that it is monopolistic, and seems to hold the company in contempt simply for having the audacity to be successful and make money.

Unfortunately, the logical corollary of the belief that Microsoft – or any other information technology company, for that matter – is the antichrist, is the belief that the regulatory authorities are Christ incarnate. After all, who else is going to protect you from the big bad wolf?

5. Both those who favour internet regulation and those who oppose it assume that individuals are weak and require protection

This brings me to my last criticism of contemporary discussions about internet regulation. The prevailing assumption that informs internet regulation – and that, increasingly, informs policy and law more broadly – is that individuals are weak, vulnerable to the myriad ills of the world, and in desperate need of protection. At the heart of most discussions about internet freedom and internet regulation is the weak individual, or what might be called in philosophical terms the diminished subject.

This conception of the weak individual was given a new legitimacy by the terrorist attacks of 11 September 2001, which reinforced a false counterposition between freedom and security. After 11 September, governments with a longstanding interest in prying into our lives were allowed to present such intrusion as being in our interests, necessary to prevent future terrorist attacks.[28]

But it isn't just the threat of terrorism that looms large in justifications for internet regulation. Increasingly, the very act of communication – through words, images and sounds – is characterised as something that can do injury to others and cause trauma.

Increasingly, the distinction between communication and action is being erased. It is assumed that communication is directly harmful to its recipients, that communication impels its consumers to act, that communication is equivalent to the abuses it describes and depicts. This has led to the bizarre legal notion that an individual can be complicit in an act that originally took place without their knowledge or involvement.[29]

[27] See the 'United States v Microsoft' section of the United States Department of Justice website [http://www.usdoj.gov/atr/cases/ms_index.htm]

[28] The 2002 *Privacy and Human Rights* report notes that erosions of privacy following the 11 September 2001 terrorist attacks were not 'necessarily new; the novelty is the speed in which these policies gained acceptance, and in many cases, became law'. *Privacy and Human Rights: An International Survey of Privacy Laws and Developments 2002*, Sarah Andrews (ed), Washington/London: Electronic Privacy Information Centre/Privacy International, p27 [http://www.privacyinternational.org/survey/phr2002/phr2002-part1.pdf]

[29] See 'Fetishising images', Barbara Hewson, *spiked*, 23 January 2003 [http://www.spiked-online.com/printable/00000006DC06.htm]

The problem is, there aren't really any good guys when it comes to this conception of the weak individual. Campaigners for freedom who might pour scorn upon the conception in one instance, embrace it opportunistically in another. Take the American Civil Liberties Union (ACLU) – one of the world's staunchest defenders of freedom, and one which is robust enough on the subject of child pornography to point out that 'there is a real difference between touching children sexually and touching computer keys to create images'[30].

Shortly after the 11 September terrorist attacks, ACLU president Nadine Strossen argued that 'we're never going to be safe...but at least we can be free'[31] – a statement which suggested that she understood the danger of making freedom subordinate to safety. But since the terrorist attacks, the ACLU has also mounted a campaign around the slogan 'keep America safe and free'[32] – which suggests that the organisation is shortchanging its principles by appealing to people's feelings of insecurity.

In the debate around privacy, conceptions of the weak individual have allowed privacy to become confused with anonymity. To be sure, anonymity can be politically important – most obviously, for individuals living under particularly repressive regimes. But anonymity can also become a pretext for not taking responsibility for one's words and actions, and it can become a pretext for retreating from social engagement. Ultimately, the private is only worth defending so long as it can act as a bedrock for the public.

One area where regulators and campaigners alike have done a great disservice to the notion of the robust, free individual, is in the bizarre discussion surrounding unsolicited bulk email, or spam. Spam is increasingly a practical problem for many people, as I'm sure anyone with an email account is aware – one recent piece of research, conducted by BT Openworld and Brightmail, concluded that nearly half of all emails sent today are spam.[33]

But instead of being recognised as a practical problem requiring a practical solution, spam is often discussed in terms that characterise it as something resembling physical abuse. And despite the fact that spam is a problem that we all experience differently – one person's spam is another person's steak, and vice versa – blunt legal and technological sledgehammers are being applied to the problem, when more practical remedies, allowing for greater personal choice, are available.

October 2003 is the deadline for European Union member states to implement the Directive on Privacy and Electronic Communications, which outlaws 'unsolicited communications for purposes of direct marketing...without the consent of the subscribers concerned'[34]. This directive employs the definition of 'consent' laid out in

[30] Brief of the American Civil Liberties Union *et al*, as *amici curiae*, *Free Speech Coalition v Reno*, 1997

[31] Nadine Strossen, interviewed in 'We can never be safe – but at least we can be free', Jennie Bristow, *spiked*, 15 November 2001 [http://www.spiked-online.com/printable/00000002D2C6.htm]

[32] See the 'Safe and free' section of the American Civil Liberties Union website [http://www.aclu.org/SafeandFree/SafeandFreeMain.cfm]

[33] See 'Before Friday comes spamday', Wendy Brewer, PC World, 8 May 2003 [http://www.pcworld.com/resource/printable/article/0,aid,110639,00.asp]

[34] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive On Privacy And Electronic Communications), Article 13.3 [http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf]

the earlier Data Protection Directive, where a person's 'consent' means 'any freely given specific and informed indication of his wishes'[35].

Interpreted strictly, this would make it illegal to send anyone an email that they weren't expecting, if that email could be construed as in any way commercial. This is a ridiculous restriction to place upon internet communication, and threatens to make us all hesitate and tread cautiously before daring to communicate online. Far from saving the internet, as it is purportedly intended to do, such legislation can only serve to stifle the internet.[36] Nonetheless, similar legislation is being proposed and implemented worldwide.[37]

The technology currently used to combat spam is often equally problematic, as it tends to make overly presumptuous decisions on behalf of users, resulting in 'false positives' – where desired email is incorrectly categorised as spam, and never reaches its intended recipient. With at least two of the most popular technological methods of combating spam today – Realtime Blackhole Lists/Relay Blocking Lists (RBLs)[38] and 'challenge-response' systems[39] – this problem is endemic.

Fortunately, a technology has been pioneered – Bayesian filtering – that filters spam effectively while accommodating differences of individual use and preference, thus restoring autonomy over email to the user.[40] But it is symptomatic of the spam debate that while this solution has been recognised for its technical merits, its political significance has hardly been commented upon. Instead, it is assumed that any measure to reduce spam is a good thing, regardless of the consequences.

Brad Templeton, founder of ClariNet, eloquently describes the erosion of political principles, when the response to a problem such as spam is defined entirely by assumptions about the victimhood of internet users:

> 'People who would defend the end-to-end principle of internet design eagerly hunt for mechanisms of centralised control to stop it. Those who would never agree with punishing the innocent to find the guilty in any other field happily advocate it to stop spam. Some conclude even entire nations must be blacklisted from sending email. One-time defenders of an open net with anonymous participation call for authentication certificates on every email. Former champions of flat-fee unlimited net access who

[35] Directive 95/46/EC of the European Parliament and of 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, Article 2 (h) [http://europa.eu.int/comm/internal_market/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf]

[36] See 'Should we can spam?', Sandy Starr, *Tech Central Station Europe*, 9 April 2003 [http://www.techcentralstation.be/2051/wrapper.jsp?PID=2051-100&CID=2051-040903N]

[37] For an excellent international overview of anti-spam legislation, see the Spam Laws website [http://www.spamlaws.com]

[38] The technologist Philip Jacobs argues that whereas the standard definition of an RBL is 'a list of servers which send out spam or are known to be open relays', in fact a more accurate definition would be 'a system for arbitrarily rejecting email messages (spam or otherwise) based on an unknown entity's unknown criteria'. 'The spam problem: moving beyond RBLs', Philip Jacob, 3 January 2003 [http://theory.whirlycott.com/~phil/antispam/rbl-bad/rbl-bad.html]

[39] Technology commentator Declan McCullagh points out that 'challenge-response systems, ironically, share some characteristics with spam: in small quantities, both are only mildly annoying to the recipient. But as quantities increase, they make it more difficult to use email at all.' 'Spam blockers may wreak e-mail havoc', Declan McCullagh, News.com, 27 May 2003 [http://news.com.com/2102-1071_3-1009745.html]

[40] See 'A plan for spam', Paul Graham, August 2002 [http://www.paulgraham.com/spam.html]

> railed against proposals for per-packet internet pricing propose per-message usage fees on email.'[41]

Another aspect of the individuals-as-victim approach to internet regulation, is the use of children as a moral shield. To listen to many regulators and legislators, you would think that our entire society should be reorganised so as not to traumatise children. The US civil liberties campaigner Marjorie Heins has documented the copious history of child-based justifications for censorship, going back to the notorious 'Hicklin test' of 1868.[42] But with the scaremongering that now surrounds the internet, such child-based justifications have found a new legitimacy.

The UK government, for example, has done everything in its power to characterise the internet as a dangerous place for children, even to the extent of manipulating statistics. In 2001, the statistic that one in every five children using internet chatrooms is approached by a paedophile became received wisdom in the UK – despite having been misappropriated by a member of parliament from a US report which concluded nothing of the sort.[43]

Then the UK Home Office published its report *Chat Wise, Street Wise: Children and Internet Chat Services*, which recommended supervising children while they surf the web, anonymising children's email addresses, using software to filter internet content accessed by children, advising children not to open suspect email attachments, and countless other safety measures – for fear of children encountering paedophiles.

But of the report's 183 paragraphs, only 22 were devoted to quantifying the risk to children from paedophiles (the rest were dedicated to unsubstantiated scaremongering), and the report concluded that 'it is extremely difficult to make any accurate assessment of the level of sexual approaches to children in chat rooms in the UK'[44]. In the end, the report could list only four instances where an adult was convicted after arranging online to meet a child in person – hardly grounds for a government-sponsored panic, then.

The idea that the information and communications technology needs to be made more safe and trustworthy – which inevitably means greater regulation – goes beyond moral panics and paedophile scares, to the technology itself. In 1999, Compaq, Hewlett-Packard, IBM, Intel, and Microsoft formed the Trusted Computing Platform Alliance (TCPA), with the aim of making *computing* more 'trustworthy'.[45]

[41] 'Reflections on the 25th anniversary of spam', Brad Templeton, [http://www.templetons.com/brad/spam/spam25.html]

[42] The ruling in the British case of *Regina v Hicklin* (1868) concluded that material should be outlawed if it might harm its most vulnerable consumers. See *Not in Front of the Children: 'Indecency', Censorship, and the Innocence of Youth*, Marjorie Heins, New York: Hill and Wang, 2001

[43] The statistic was taken, completely out of context, by UK member of parliament Paul Burstow, from *Online Victimisation: A Report on the Nation's Youth*, a June 2000 report by the National Centre for Missing and Exploited Children. The statistic actually referred to the proportion of 10-17-year-olds who had received a 'sexual solicitation or approach over the internet in the last year', which included solicitations and approaches not just from adults, but from other children – the online equivalent of adolescent fumbling. The report also pointed out that only 'one quarter of young people who reported these incidents were distressed by them'.

[44] See *Chat Wise, Street Wise: Children and Internet Chat Services*, Internet Crime Forum IRC sub-group, March 2001 [http://www.internetcrimeforum.org.uk/chatwise_streetwise.pdf]

[45] See the Compaq [http://www.compaq.com], Hewlett-Packard [http://www.hp.com], IBM [http://www.ibm.com], Intel [http://www.intel.com], Microsoft [http://www.microsoft.com] and Trusted Computing Platform Alliance [http://www.trustedcomputing.org] websites

This was no empty marketing exercise. In an unprecedented move, Microsoft's chairman Bill Gates instructed 8,500 developers to put all other work on hold for two months and concentrate on fixing security holes in Windows source code – costing him $100million – as part of the trustworthy computing initiative.[46] Of course, this is not necessarily a bad thing – if the sole aim of the initiative was to make technology function better, then the initiative would be welcome.

But the TCPA goes further than seeking to make technology function better. It seeks to make us able to 'trust' technology, and it defines 'trust' as 'the ability to feel confident that the software environment in a platform is operating as expected'[47]. This ignores the fact trust is a *social* category – quite distinct from reliability – that cannot be imposed as a standard upon a *technological* system.

Trust is not about expected outcomes, but rather depends precisely upon people being open to *unexpected* outcomes. Demanding 'trust' from technology can only result in ever-increasing regulation[48], especially when it comes to decentralised networks – which are, in many ways, the ultimate technological embodiment of unexpected outcomes.

Characterising technology as a crutch for weak individuals, rather than as a tool that individuals can use for progressive ends, militates against innovation and sets technology up for a fall. Another area where technology is being used to cosset individuals in this way is the growing field of 'social software', where software is used to proactively try to build trust and foster interaction between people – as though society cannot be healthy if people are left alone to interact with one another as they see fit.[49]

Organisations including the British Broadcasting Corporation (BBC) are increasingly interested in social software, with the BBC's major social software initiative iCan due to be launched in October 2003.[50] Social software is also attracting the attention of governments, because it dovetails with their interest in 'edemocracy' – an interest that has little to do with actua;l democracy, and more to do with an isolated political elite desperately attempting to use technology to connect with people.[51]

Note how far we've come from the idealism and the democratic aspirations that I described at the beginning. Far from decentralised networks being a place where people communicate and associate freely, decentralised networks have become a place where content is removed by unaccountable organisations; where it's difficult for you to decide what email you do and don't want to send and receive; where you (and especially your children) are made to feel vulnerable and at terrible risk; where it's alright for the state to interfere in your business, so long as it makes you feel safer;

[46] See 'Microsoft shelled out millions on security', Dennis Fisher, eWeek, 19 July 2002 [http://www.eweek.com/print_article/0,3668,a=29285,00.asp]

[47] 'Frequently asked questions, rev 5.0', Trusted Computing Platform Alliance [http://www.trustedcomputing.org/docs/Website_TCPA%20FAQ_0703021.pdf]

[48] See 'Trusting technology', by Norman Lewis, *spiked*, 26 March 2003 [http://www.spiked-online.com/printable/00000006DD04.htm]

[49] See 'Social software – get real', by Martyn Perks, *spiked*, 20 March 2003 [http://www.spiked-online.com/printable/00000006DCF1.htm]

[50] See 'Web antidote for political apathy', Leander Kahney, *Wired News*, 5 May 2003 [http://www.wired.com/news/print/0,1294,58715,00.html]. For a comprehensive overview of the field of social software, see *You Don't Know Me, But...: Social Capital and Social Software*, William Davies, London: Work Foundation, 2003 [http://www.theworkfoundation.com/pdf/1843730103.pdf]

[51] See 'State machinery', Sandy Starr, *spiked*, 28 November 2002 [http://www.spiked-online.com/printable/00000006DB5B.htm]

where you have to trust technology (even though ultimately, you can't), because you don't feel you can trust other people; and where other people have to step in to empower you and to help you interact with others.

6. Conclusion

There's a tendency to be defensive about decentralised networks, and that's entirely wrongheaded. The fact that they're decentralised and that they defy regulation is precisely what's good about them, and we shouldn't feel afraid to say so – while at the same time, being critical of social trends toward insularity and anonymity.

The internet should be neither a snooping ground for the state where individuals fear to tread, nor an atomised collection of fearful, anonymous individuals (and it is presently in danger of becoming both), but rather a place where members of society can communicate and collaborate freely, to progressive ends.

We need to recall and reclaim the principles that guided the early development of the internet. Some of those principles were sound, and some of them were misguided or utopian. But those principles contained aspirations that were precious, and that are rapidly being whittled away and redefined.

If we defend freedom on the internet in the name of the weak, anonymous, unaccountable individual who needs protection from all the evils of the world, then we're going to get absolutely nowhere. We need to defend internet freedom on behalf of the active human subject who speaks and associates freely, without interference from the state.