
Journal of Information, Law and Technology

# Regulating Cyberstalking

**Subhajit Basu,**
**Queens University, Belfast**
s.basu@qub.ac.uk

**Richard Jones**
r.p.jones@livjm.ac.uk

---

This is a **Refereed** Article published on **22nd November 2007**

Basu, S. and Jones, R.P., "Regulating Cyberstalking", JILT 2007 (2), <http://go.warwick.ac.uk/jilt/2007_2/basu_jones/>

---

# Abstract

Through the use of examples of cyber stalking the paper will consider the nature of regulation required in relation to this behaviour in cyberspace. The paper will consider the differences between off line and cyber stalking, and review how these differences affect the regulation of such activities. The paper will review the boundaries between public and private law, between national and international law and between state law and self regulation, and consider whether the traditional positivist methodology of law, within these boundaries offers an adequate intellectual framework in which to consider the nature and form of regulation in cyberspace.


**Key Words**: Cyberspace, Cyber-stalking, Cyber-harassment, Regulation, Anonymity, Jurisdiction, Positivism

# 1. Introduction

> Right, you've got as far as finding yourself attracted to a guy on the net. But do you really know anything about him? He's said he's 39, divorced, has 2 kids, is tall, blond and enjoys driving fast cars and going to the theatre. How can you know for sure that he's not 46, married, 2 kids, 5'4", drives a Ford Fiesta and spends most of his time either in front of the PC or down the local watering hole with his mates? ASK! "Oh yeah," you may well think "he's likely to say "yes Sally, I've been lying to you all along". Of course he isn't. It's a matter of asking the right questions.

As illustrated from the above extract from a guide to cyber-flirting, flirting in cyberspace is different from physical space. These differences (an ever growing number), give an insight into the difficulties in regulating behaviour in cyberspace. Yet the perspectives offered by lawmakers, judges, and scholars are all grounded in various premises about online life and the search for solutions has been approached from the perspective that cyberspace is merely an extension or continuation of the real world. The peculiarities of cyberspace, particularly anonymity, mean it is not simply a question of transferring behaviours across from the physical world; individuals and communities in cyberspace are different and so is their behaviour. This paper will illustrate how the key concepts of social interaction, social bonding, and empirical experience differ in cyberspace from those in the physical world. Such differences should inform the debate about the nature and form of regulation of cyberspace.

Cyberspace is a distinct place for purposes of legal analysis with a legally significant border. As pointed out by Lessig, *"Cyberspace presents something new for those of us who think about regulation and freedom. It demands a new understanding of how regulation works and of what regulates life there?"* (Lessig L, 1999)

Through the examples of cyber stalking the paper will consider the nature of regulation required in relation to such behaviour in such a place. We suggest that the boundaries

between public and private law, between national and international law and between state law and self regulation, and indeed the traditional positivist methodology of law, no longer offer an adequate intellectual framework in which to consider the nature and form of regulation in cyberspace. For example the process may conveniently proceed as follows, as the *Protection from Harassment Act, 1997* makes no attempt to define the term stalking it may, by judicial interpretation, be extended to cyber-stalking, (some have suggested that cyber-stalking represents nothing more than an additional behaviour that can be associated with "offline stalking"), therefore with minor amendments to deal with the "technology" this Act is able to regulate cyber stalking. This approach, we would suggest, ignores the nature of the community in which this is happening and the nature and form of the behaviour itself. New technology inevitably leads to effects on culture and on forms of deviant behaviour that will naturally arise in order to exploit new opportunities. Cyber-stalking, for example, encompasses a wide range of new behaviours that are not associated with offline stalking. Cyber-stalking can be associated with the activities of paedophiles, and has been seen to include intimidation to achieve a variety of ends. Drawing on literature that both analyses the nature of the activities, the space in which they occur and the effect of technology on culture, the paper will argue that the foundation should be an investigation and an analysis of the community space over which the regulation is to apply. Such an analysis, will it is hoped, illustrates the inadequacies of traditional 'legal' deterministic approaches and offer workable approaches to the problem of regulation and enforcement.

## 2. Technology

Technological change does not occur within a social vacuum (Kuhn T, 1996) and social upheaval in the face of technological change is not new. Some of this change is undesirable, as Postman states:

> That is not to say that the computer is blight on the symbolic landscape; only that, like medical technology, it has usurped powers and enforced mindsets that a fully attentive culture might have wished to deny it. (Postman N, 1992 p.107)

Cyberspace brings together the potentially exciting cocktail of technology, and its unique group of users, within the context of anonymity and an environment lacking in consistent norms. Whilst the potentially democratizing effect is to be welcomed, the potential for perverse activity is not (Lessig L, 1999). It is this dichotomy- the democratic versus the perverting role of the internet within the context of the less discussed forms of crimes and deviance which makes the subject of this paper. As Sherizen comments:

> "Seldom is there an integrated socio-technological approach to the computer crime problem…we need to establish where the social and psychological lines are drawn between normal and deviant, between allowed and disallowed, between expected and unexpected, between wanted and unwanted".(Sherizen 1992 p.39)

Societies throughout the history of mankind have incorporated into their fabric technologies that have had a profound cultural effect. However what is arguably significant about internet revolution is the nature and pace of change; the pace surpasses any of the previous technological revolutions. This technological change has now reached a speed that is increasingly difficult for both society and individuals to accommodate, a situation expressed by the novelist William Gibson in his description of a typically urban environment of the near future:

> Night City was like a deranged experiment in social Darwinism, designed by a bored researcher who kept one thumb permanently on the fast-forward button. Stop hustling and you sunk without a trace, but move a little too swiftly and you'd break the fragile surface tension of the black market; either way, you were gone, with nothing left of you but some vague memory…though heart or lung or kidneys might survive in the service of some stranger (Gibson 1984 p.14)

Crime follows opportunity. Crime in 'Night City' is very different from crime in the physical world. Technology has provided an efficient and more effective means to commit the 'old' crimes; however the extent of their impact on our day-to-day life is much more profound and much more intrusive. In less than a decade the full spectrum of immorality covered in the real world transferred to the virtual world: cyber warfare, cyber-terrorism, identity theft, racial hate speech, organized crime, brutal child pornography, cyber-stalking, chat room crimes and questionable forms of hacking pervaded cyberspace. Activities have not only replicated those in the virtual world but also have taken on their own character fuelled by an environment where anonymity is the norm. Policies for policing and prevention of some cyber crimes are ineffective, we would argue, without an analysis of the society in which they occur.

## 3. Cyberspace Sociality – Space and Community

The notion of physical space saturates our ordinary everyday lives. It is a basic concept which underlies our understanding of the world around us, the entities within it and our own and other people's movements through it. Philosophy has traditionally understood questions about the nature of space in terms of the dichotomy between substantivalism (or absolutism) and relationalism, with Newton and Leibniz as the two key proponents. "Does something exist over and above spatial relationships between entities, something in which those entities inhere (i.e. absolute space)? Or does our concept of space amount to nothing more than those entities and the spatial relationships between them?" (Bryant R, 2001 p.138-155) Paul Teller explains this dichotomy:

> Is it [space] a substance, a collection of particulars ("points," or "regions"), existing independently, and providing an objective framework of spatial reference ("substantivalism")? Or should we say that substantival space is an illusion, there

> being nothing more than the spatial relations holding between physical objects or events ("relationalism")? (Teller 1991 p.363-97)

Is Cyberspace a *space* existing in the penumbral ether between the networked computers? In a rough conceptual equivalence of space and cyberspace: can cyberspace exist as an independent entity over and above those entities that it accommodates?

> In early days of computer networks it seemed a slightly far-fetched metaphor to describe…..sites as 'places', since bandwidth was narrow…as bandwidth burgeons and computing muscle continues to grow, cyberspace will present themselves in increasingly multi-sensory and engaging ways…we will just look at them; we feel present in them. (Williams 1995 p.114-5)

Most notable within the postmodernist view has been Jean Baudrillard's exposition of 'hyper-reality' (Baudrillard 1988), as it relates to the development of cyberspace and especially the potential capabilities of virtual reality technologies. Although based primarily upon mass communications media, Baudrillard's contention that such technologies are constructing an entirely new social environment, an electronic reality, has clear resonance for those arguing that cyberspace represents an alternative, virtual reality. In this hyper-reality of cyberspace it is contented that, time, place and individual identity are separated from modernist physical locations. However, what accompanies discourses on both these latest technologies and the new articulations of space-time that they express-whether utopian, dystopian, or measured – is an impoverished understanding of the real and the virtual. This lack of understanding infiltrates both the virtual and the real, to the point where the virtual is invariably collapsed into a badly analysed version of the real – wherein the real and virtual are no longer distinguishable according to qualities, but only according to quantities. Regardless of the nature of the space what cannot be questioned is the fact that cyberspace is everywhere, omnipresent, in other words ubiquitous.

So is cyberspace a place? Whatever answer we give to the normative question, there is significant evidence that, purely as a descriptive observation, individuals do think of cyberspace as a place. Cognitive science investigations into how people think provide ample evidence of this. The legal fraternity have unwillingly accepted that our physical assumptions about property should also apply to this new 'space'. Owners of internet resources consider their website or e-mail address as their own little 'claim' in cyberspace which should given similar level of protection against any infringement to that which would be provided in the physical world.

The sociology of cyberspace raises some crucial questions, not only about the emergence of new forms of community and sociality, but also of how these are best understood. Viable 'societies' exists in cyberspace. It is a space where people experience all that they may experience in real space, or almost all anyway. It is also an international community with social interaction, social bonding, and empirical experience.

> . . .rather than being constrained by the computer, the members of these groups creatively exploit the systems' features so as to play with new forms of expressive communication, to explore possible public identities, to create otherwise unlikely relationships, and to create behavioural norms. In so doing, they invent new communities. (Reid 1995 p.164-183)

Defining 'community' will help frame the ensuing legal discussion, and will enable us to better evaluate various form of crimes against the virtual community. So, what do we mean by community? Many scholars have noted the elusiveness of a definition of 'community,' (Post 1997 p.473) a term that is complicated by its central position in the debate between communitarians and liberals (Alexander 1989). Traditionally, geography has helped to indicate community. Although geography arguably remains important in defining virtual community, we are better served in the Internet context by an 'experiential' conception of community, rather than a geographic one (Alexander 1989). Is the use of the phrase 'virtual community' a perversion of the notion of community? Not all scholars accept that cyber subcultures are worthy of our attention or whether they are simply ephemeral, imagined communities, too fleeting, too superficial, and too 'virtual' to warrant serious exploration. Calhoun (1991) argued that the modern condition is one of 'indirect social relationships' in which connectivity with others is more imagined, or parasocial, than 'real.' The media's ability to broaden the range of our experiences creates the illusion of greater contact or membership in large-scale social organizations. Rather than creating 'communities', however, were are merely developing 'categorical identities' or 'imagined communities,' that are nothing more than the 'feeling' of belonging to some group. He further argues that a true 'community' requires direct relationships among its members:

> . . .that there is a great deal of difference between social groups formed out of direct relationships among their members, although often sharing an imaginatively constructed cultural identity, and social categories defined by common cultural or other external attributes of their members and not necessarily linked by any dense, multiplex, or systematic web of interpersonal relationships" (Calhoun 1991 p.95-121)

In contrast, Oldenburg (1989) argues "online communities might fill a need that has been all but abandoned in modern societies, where the closeness and social bonding of the gemeinschaft has been replaced by the emotional disconnect of the gesellschaft. An individual moves about through three basic environments: where he works, where he lives, and the place where he joins with others for conviviality." According to Thomsen *et el* (1998) it is the latter environment, the place of "idle talk and banter with acquaintances and friends," where is often the sense of membership in a 'community' is achieved and experienced. According to some theorist this environment also maximizes individual's creativity, imagination. Cafes, barbershops, and pubs once provided this environment, but in the age of shopping malls, drive-in fast food, shrinking public space, and residential 'cocooning', this need for conviviality is left unfulfilled (Thomsen et el: 1998). Modernity, Oldenburg argues, has established a culture in which the home and the workplace remain as the only two interactive spheres of existence. It should not be

surprising, then, that millions of people throughout the world turn to the Internet to re-create and re-establish the third sphere of conviviality (Oldenburg 1989). Cerulo (1997) has argued that in order to effectively study online communities, sociologists and communication researchers must reframe the way in which they view the computer-mediated world and past assumptions about human interactions:

> recent developments have touched issues at the very heart of sociological discourse--the definition of interaction, the nature of social ties, and the scope of experience and reality. Indeed, the developing technologies are creating an expanded social environment that requires amendments and alterations to ways in which we conceptualize social processes (Cerulo1997 p.48-58).

Technology does not have to dictate the way our social relations change, but we can only influence change if we understand how people use technologies. Hence, technologically generated communities have forced us to reformulate the way in which we view three key analytic concepts: social interaction, social bonding, and empirical experience, the traditional stance in sociological analysis. “Cerulo explained that physical co-presence is the determining factor in judging the significance and quality of a communicative exchange” (Cerulo1997 p.48-58). So is there something disturbing about finding community through a computer screen? “We speak of the closeness and trust born of such mediated connections using terms such as pseudo-gemeinschaft, virtual intimacy, or imagined community” (Thomsen et el: 1998). “Such designations reify the notion that interactions void of the face-to-face connection are somehow less than the real thing” (Cerulo1997 p.50). Purcell contradicted this view, suggesting:

> Co-presence does not insure intimate interaction among all group members. Consider large-scale social gatherings in which hundreds or thousands of people gather in a location to perform a ritual or celebrate an event. In these instances, participants are able to see the visible manifestation of the group, the physical gathering, yet their ability to make direct, intimate connections with those around them is limited by the sheer magnitude of the assembly” (Purcell 1997 p.101-112).

If accepted that interactions within cyberspace are considered by the participants to be real, such a conclusion will impact upon consideration of the motive and the nature of harm in stalking.

# 4. Regulation of Cyberspace

As we commented earlier it is apparent that owners of internet resources consider their website or e-mail address as their own little ‘claim’ in cyberspace, which should give a similar level of protection against any infringement to that which would be provided in the physical world. Such views have found acceptance in the courts.[1] It is questioned whether such acceptance has occurred through an understanding of virtual community or

space or merely through a process where the virtual is collapsed into a badly analysed version of the real.

Regulation is required and will occur in cyberspace (Mnookin 1996). In general, communities generate and perpetuate their own legal norms (Giordano1998). Community norms receive deference when "community standards" are used to determine whether a crime or tort has been committed (Byassee 1995 p.207-208). Legal rules: statutes, court decisions, and deference to extra-legal mechanisms such as norms, markets, and programming code (Lessig1998) are crucial in determining what sorts of communities thrive in cyberspace and what sorts of communities do not. Territorial sovereigns can recognize communities not only by leaving these groups alone, but also by enforcing community rules. The law may give communities a sphere of autonomy through the principle of freedom of association, or it may grant communities such as churches, corporations, and civic associations the power of self-governance, enforceable in courts of law. As cyberspace becomes more entwined with real-space life, the rules governing virtual communities may also in time begin to influence our real-space communities.

The nature and extent of regulation is where the debate lies. For some the virtual is the same as the physical. The perspectives offered by lawmakers, judges, and scholars are all grounded in various premises about online life and have been approached with the idea that cyberspace is an extension or continuation of the real world. For others Cyberspace is a distinct 'place' for purposes of legal analysis with a legally significant border between Cyberspace and the 'real world.' Johnson and Post (1997) for example argued that cyberspace should have "its own law and legal institutions," and that state-based government would generally have no jurisdiction over online activity. To Johnson and Post, then, the law of cyberspace is, quite literally, the law of another place (Johnson and Post 1997 p.62). It is the law of cyberspace -- the same way that we might think of the law of the State of New York or the law of the United Kingdom.[2] Latterly there has been recognition of distinctions between the real and virtual but also a merging of the idea of how we think about cyberspace, with the normative question of how cyberspace is or may be regulated. This is most clearly seen where Lessig, (1999) comments: *"cyberspace presents something new for those of us who think about regulation and freedom. It demands a new understanding of how regulation works and of what regulates life there."* (Contrast Post 2000).

We argue that the debate has been wrongly constrained and that we need to retrace our route and begin again, we suggest, with an analysis of space and community, a space and community with distinct interactions, social ties and experiences. A virtual[3] community in which the balance between law and sanctions and legal and self regulation are subtly different, and where the nature of the interactions require a review of the acceptance or non acceptance of various behaviours.[4] Simple legislative extension to cyberspace is unlikely to lead to a reduction in criminal internet activity, such responses have been inadequate in the peculiar environment of cyberspace. Will internet citizens be forced to resort either to forms of situational crime prevention either individually or in consort with internet service providers to provide adequate protection from such behaviour? The debate is often encapsulated in the terminology of Lessig (1999, fn 5, p53-4) between

East Coast responses, centring on the law, and West Coast responses based upon technology. The failure of the traditional legal responses in cyberspace has led to fall back response relying unthinkingly on technology rather than an examination of the reasons why laws have failed to regulate behaviour effectively. A fundamental review will free the debate to enable a breach of the traditional conceptual boundaries that have railroaded the debate so far. These boundaries include but are not limited to the divisions between public and private law, between national and international law and between state law, self regulation and code, within the nature of the community itself (Paliwala A, 2004, Brownsword 2005)

## 5. The 'Anonymous' World of Cyberspace

As we previously commented technologically generated communities have forced us to reformulate the way in which we view three key analytic concepts: social interaction, social bonding, and empirical experience. Before considering the nature and form of regulation that will establish and enforce baseline rules of conduct that is unique for cyberspace and define, punish and prevent wrongful actions that harm others through online means (Paliwala 2004) we begin as we have suggested with an analysis of the nature of the community and in particular one aspect of the virtual community – anonymity.

Anonymity in the cyberspace can be seen as the norm and not a deviation. Anonymous interaction in cyberspace has become commonplace. Cyberspace makes anonymity easy so long as no physical manipulation is involved. Some benefits of social interaction can be achieved, whilst still maintaining a sense of privacy. In short cyberspace has created infinitely new possibilities to the deviant imagination, for as contemporary life has been described as a world of spectacle, narcissism and performance (Abercrombie and Longhurst 1998), cyberspace provides a space for all three. The virtual worlds are 'laboratories for the construction of identity', where individuals frequently feel more like their 'real' selves than in the physical world (Turkle 1996 ). In this space, one can excogitate new identities.

Identity is a complex and multifaceted concept that plays a central role in delineating the parameters of *inter alia* ethnicity, nationality and citizenship, thus generating an immense amount of debate across various disciplines (Bendle 2002). Individual identity can be seen as the sense of self that is based upon the internationalization of all that is known about oneself. For Goffman, (1959) the key characteristics of what he termed- after Freud- 'id' (re felt) identity are subjectivity and reflexivity. Hence individual identity is more than simply self-perception; rather it is the subjective construction of self that is modified by reflections on the views of others and the individual interactions in the social world (Goffman1963). As such, individual identity is not a static construction but one that is constantly evolving and readjusting in line with an individual's life experience (Finch 2002 p. 87).

Identity plays a key role in virtual communities. In communication, which is the primary activity, knowing the identity of those with whom you communicate is essential for understanding and evaluating an interaction. Yet in the disembodied world of the virtual community, identity is also ambiguous. In the physical world there is an inherent unity to the self, for the body provides a compelling and convenient definition of identity. The norm is: one body, one identity. Though the self may be complex and mutable over time and circumstance, the body provides a stabilizing anchor. The virtual world is different. It is composed of information rather than matter. Information spreads and diffuses; there is no law of the conservation of information. The inhabitants of this impalpable space are also diffuse, free from the body's unifying anchor. One can have, some claim, as many electronic personas as one has time and energy to create.

A single person can create multiple electronic identities that are linked only by their common progenitor, that link, though invisible in the virtual world, is of great significance. What is the relationship among multiple personas sharing a single progenitor? Do virtual personas inherit the qualities - and responsibilities - of their creators? Such questions bring a fresh approach to ancient inquiries into the relationship between the self and the body - and a fresh urgency. Online communities are growing rapidly and their participants face these questions, not as hypothetical thought experiments, but as basic issues in their daily existence. Large amount of text-based affairs embodies part of the cyberspace, while people’s illusion embodies other parts of it. In the everyday world of cyberspace strangers meet, exchange some right or wrong information and shift more or less their personality.

A man creates a female identity; a high school student claims to be an expert on viruses. Other explorers in virtual space develop relationships with the ostensible female, relationships based on deep-seated assumptions about gender and their own sexuality; believing them to be backed by real-world knowledge (Mnookin 1996). Identity is essential for assessing the reliability of information and the trustworthiness of a confidant. And care of one's own identity, one's reputation is fundamental to the formation of community. This is the misfortune of the Internet for it allows people to experiment with their identity, and instantly change their gender with a few strokes of the keyboard.

Identity cues are sparse in the virtual world, but not non-existent. People become attuned to the nuances of email addresses and signature styles. New phrases evolve that mark their users as members of a chosen subculture. Virtual reputations are established and impugned. By looking closely at these cues, at how they work and when they fail, we can learn a great deal about how to build vibrant on-line environments. Instead of being judged by others through birthright, and other social and economic categories, interacting in cyberspace allows to choose where and how to belong. It becomes very easy to send mail, messages, and information without anyone knowing who sent it and without having to account for the actions.

In Goffman's analysis, he sees us performing in different types of settings. Usually, the setting stays constant during our performance and it is only rarely that the setting follows

us. Basically, we fit into the setting (Goffman 1959). When looking at the interaction in cyberspace, we see that the setting forces the user to transform themselves, the setting fits the user. The Internet offers different scenarios and creates a setting that is conducive to anonymity and psuedonymity; many find it easy and sometimes necessary to change their persona, or to change their front. Being anonymous in cyberspace is helpful to those who live in countries where freedom of speech and press may not be so widely upheld. It creates an open forum to communicate and inform others without danger to themselves. Also, anonymity creates a situation where there is no gender, race or prejudice, it transcends these boundaries and everyone can be seen as equal. The cyberspace environment is constantly changing, the setting is never constant, and thus it makes it easier for people to remain "hidden". Anonymous interaction maintains privacy, but not at the expense of social isolation. What other medium will allow you to enter new worlds and meet new people without having to follow rules of specific conduct? It becomes possible to exit a setting or change a setting that you do not like where in face to face communication, this is not easy. But, what are the consequences for operating this way in cyberspace?

Just as anonymity conceals an individual's real identity in online communication, pseudonymity also serves to disguise it. Similar to anonymity, psuedonymity involves the sender changing their name as opposed to not sending one at all. And, just like anonymity, psuedonymity is both untraceable and traceable (Jacobson 1996). With untraceable psuedonymity the sender will change their real name to something else. If the sender becomes worried that someone may try to masquerade under their pseudonym, the sender can sign their name with a digital signature created specifically for the pseudonym. This will help detect any forged signatures and create a digital persona or a "nym" (Froomkin 1996). Traceable psuedonymity is communication with a "nom de plume" attached which can be traced back to the author. Why would people want to communicate in such a manner?

There are many benefits to anonymous interaction on the Internet, but do these benefits outweigh the social reality? In our lives, we do present various fronts, but when we do, we are accountable for our actions. This is a disadvantage to anonymity, because there is no face to face communication or interaction. You no longer have to be accountable for what you say or do. Often, Internet users evade or hinder accountability which allows them to express feelings without taking into perspective how someone else may feel. In the real world of face to face communication, such outbursts of inappropriate behaviour would bring about retaliation. Also, with anonymity, the Internet's communal nature is broken. The once open forum of open communication and debate is vastly transferred when you are bombarded with anonymous rhetoric. Since the user is able to put on as many fronts without being held accountable, a high level of uncertainty is created among users. Therefore, positive personal relationships on the Internet are rare and infrequent. It takes longer to move towards shared points of views and it becomes easier to engage in more verbal aggression. Unfortunately, there is no easy way to balance the benefits from the consequences, which means that all users out there must beware because things may not be as they seem.

The key concepts of social interaction, social bonding, and empirical experience differ in cyberspace from the physical world. Such differences should inform the debate about the nature and form of regulation of cyberspace. We will now illustrate how this appreciation of community and identities can inform the debate on regulating stalking in cyberspace.

# 6. Stalking

In the United States, California was the first state to adopt stalking laws, most often identified as a result of the murder in 1989 of actress Rebecca Schaeffer by Robert Bardo, an obsessed fan (Zona et al 1993). Legislation was subsequently enacted in 1990. Other States followed but most of the US states laws do not refer specifically to, nor can be interpreted to include the concept of cyber-stalking. Stalking directly impacts upon the individual lives of victims creating in them,

> a fear for personal safety and security; anxiety for the future and a loss of quality of life; uncertainty and unpredictability, as the uncontrolled acts intrude upon the lives of victims in a random fashion, making the re-establishment of a normal life difficult (Miller 2001).

In the UK without specific legislation to deal with stalking and harassment case law had begun to expand the concept of bodily harm found in the *Offences Against the Person Act*, 1861 to cover the rapidly developing social phenomena of stalking and harassment. In *R. v Ireland (Robert Matthew) R. v Burstow (Anthony Christopher)* (HL) [1998] A.C. 147 (1997) 141 S.J.L.B. 205 the defendant had made several malicious telephone calls to women. It was held that a recognisable psychiatric illness suffered by a victim of malicious telephone calls amounted to "bodily harm" within the meaning of the Act. The relevant UK domestic laws on harassment (of which stalking is a form) are a rag bag of statutes, many predating the explosion of the internet and the development and use of mobile phones. The *Telecommunications Act*, 1984 *Malicious Communications Act*, 1988 and the *Protection from Harassment Act*, 1997 provide a number of options to deal with stalking but none attempt to define the term. Section 1 of the *Malicious Communications Act*, 1988 make it an offence to send an indecent, offensive or threatening letter, electronic communication or other article to another person. In addition s.43 *Telecommunications Act*, 1984 creates a similar offence to send a telephone message which is indecent, offensive or threatening. The 1988 Act is the wider ranging, although still rather dated in its language, making provision for the "punishment of persons who send or deliver letters or other articles for the purpose of causing distress or anxiety." Under section.1, an offence is committed by a person "who sends a letter or other article which conveys

i. a message which is indecent or grossly offensive;
ii. a threat; or
iii. information which is false and known or believed to be false by the sender; or any other article which is, in whole or part, of an indecent or grossly offensive nature."

Should there be more than one offensive event then it will be possible to prosecute under the *Protection from Harassment Act*, 1997. The 1997 Act was introduced following a campaign by Diane Lamplugh whose daughter Suzy was murdered. The 1997 Act requires a 'course of conduct' before an offence is committed. The Act, introduces both civil and criminal wrongs and enables the court to make a Restraining Order (s.5) preventing the offender from contacting the victim again. Such an order is not available under the 1984, nor the 1988 Act. The 1997 Act introduces two main criminal offences, under section 2, a person who pursues a course of conduct (harassment) in breach of section 1 is guilty of an offence. The more serious offence is in section 4 where a person whose "course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions." More seriously if the harassment is racially aggravated then charges could be brought under section 32 *Crime and Disorder Act*, 1998. If the offender is 'associated' with the victim then a non-molestation order may be available under the *Family Law Act*, 1996 (section 42, 62).

## 7. 'Where Evil Dare: Stalking in Cyberspace'[5]

> *When you're growing up your parents tell you not to talk to strangers, but the whole point of the Internet is to talk to strangers*

While there is no universally accepted definition of cyberstalking, the term generally refers to using the internet or other telecommunication technology to harass or menace another person. Though the behaviour widely identified as stalking has existed for centuries, the legal system has only codified its presence in the statutes in recent decades. As a result, cyberstalking could truly be identified as a crime of the nineties owing to its reliance on computer and communications technology which have only reached maturity in the past decade. The Crown Prosecution Service defines cyber stalking:

> Cyber stalking generally takes the form of threatening behaviour or unwanted advances directed at another using the Internet and other forms of online communications. Cyber stalkers can target their victims through chat rooms, message boards, discussion forums, and e-mail. Cyber stalking can be carried out in a variety of ways such as: threatening or obscene e-mail; spamming (in which a stalker sends a victim a multitude of junk e-mail); live chat harassment or flaming (online verbal abuse); leaving improper messages on message boards or in guest books; sending electronic viruses; sending unsolicited e-mail; and electronic identity theft amongst others.[6]

The nature and extent of cyberstalking is difficult to quantify. It is perhaps more difficult to assess than physical stalking, given the anonymity and breadth of electronic

communication. In addition cyberstalking is difficult to assess in terms of its incidence and prevalence within any given population because some victims may not consider the behaviour to be dangerous, indeed they may even be unaware they are stalked.

There is no comprehensive data on the extent of cyberstalking and limited research has been carried out in the area of cyberstalking. In August 1999 the US Justice Department published a report examining the problem of online harassment and cyberstalking. The report accepts that the nature and extent of cyberstalking is difficult to quantify, however the report suggests that the potential magnitude of the problem may be estimated by reference to the problem of real life stalking (Ellison 2001 p142)

In U.K., the findings of the 1998 British Crime Survey suggested that only 11.8 percent of the population had been victims of stalking in the past (Budd 2000 as cited in Bocij 2003) as yet there are no separate statistics for cybercrimes but overall harassment rose 23 per cent to 137,460 incidents in 2002/3. There are no reliable estimates of the number of cyber stalking incidents that take place each year. That it may be more common has been suggested by Bocij and McFarlane (2002) who argue that

> A number of factors may encourage an otherwise peaceful and law-abiding individual to take part in deviant or criminal acts via the Internet. One such factor is that modern technology helps to ... enable participation without fear of sanctions. Technology provides both the mechanism through which the individual can act and the protection needed against arrest or other punishment.

We would suggest that cyberstalking is not merely stalking using the internet but that there are qualitative differences between stalking in the physical and cyberspace. As to the differences between physical world and cyber world crimes Wall (2005) has suggested a so called 'elimination test' to define differing forms of 'cyber crimes'. Using this test he concludes that there are three types of cyber crimes, firstly traditional crimes where the internet is simply a tool for to assist in the crime, an example of this would be the use of email by those planning a robbery. Secondly, hybrid crimes which he describes as where "the internet has opened up entirely new opportunities" for existing criminal activities and finally, true cyber crimes which are "solely the product of the internet and can only be perpetrated within cyberspace" (e.g. spamming). Using this analysis cyber stalking would appear at first sight to be a hybrid crime. However the significant differences between off line and on line stalking are such that we are hesitant to describe cyber stalking as a mere variant of physical stalking. This may not be what Wall and the elimination test are implying, but the use of the term hybrid for us has a diluting effect, which may hide the true characteristics, and effects of this activity and as a result lead to the misinterpretation of its consequences.

What then are these substantial differences? Firstly the nature and form of the behaviour lead to differences. For the investigator or concerned net-user, information relating to the behaviour often exhibited by a stalker will be important, as this may provide insight into possible motivations behind the offender. The fact that cyberstalking does not involve physical contact may create the misperception that it is more benign than physical stalking. This is not necessarily true. As the Internet becomes an ever more integral part

of our personal and professional lives, stalkers can take advantage of the ease of communications as well as increased access to personal information. In addition, the ease of use and non-confrontational, impersonal, and sometimes anonymous nature of Internet communications may remove disincentives to cyberstalking. Where a potential stalker may be unwilling or unable to confront a victim in person or on the telephone, he or she may have little hesitation sending harassing or threatening electronic communications to a victim. This lack of knowledge means that the harm suffered by victims of cyberstalking is often dismissed. However:

> "*to argue that an act of cyberstalking is less serious than stalking will grant an would-be offender the right to harass, humiliate or defame individuals simply on the basis that it is not 'real'. There is always attempt made by some commentators to oversimplify what is a far complex act of crime for "the sake of a presumed theoretical, methodological or philosophical bias*" (Williams 2004, p143).

The second area of difference surrounds the relationship of stalker and victim. We can speculate that a significant number of cyberstalking victims do not know the identity of their harassers. Given the enormous amount of personal information available through the Internet, a cyberstalker can easily locate private information about a potential victim with a few mouse clicks or key strokes. This contrasts with offline stalking, where research has shown that the majority of stalkers know their victims. However the nature of internet and the proximity it creates makes it possible for cyberstalking to be committed by strangers. This would lead to a qualitative difference between offline and online stalking.

The third difference surrounds the nature of the acts, cyber stalkers tend to concentrate on very different activities from physical stalkers. Particularly cyberstalking has been said to comprise three major types:

> *"Email Stalking: Direct communication through email. Internet Stalking: Global communication through the Internet. Computer Stalking: Unauthorized control of another person's computer."* (Ogilvie 2000)

To these should be added SMS and text messaging through mobile phones. [7] These show obvious parallels between offline and online stalking, for instance, "attempting to cause damage to data by inserting a computer virus onto the victim's computer system is comparable to the vandalism experienced by some victims of offline stalking, yet there are also a number of important differences in the behaviours associated with offline and online stalking" (Standage 1998). Ogilvie (2000) and Jenson (1996) [8]who have investigated the characteristics of cyberstalking claim, cyberstalkers have similar characteristics to the offline stalkers, with most cyberstalkers motivated to control the victim (Maxwell 2001). A cyberstalker can dupe other Internet users into harassing or threatening a victim by utilizing Internet bulletin boards or chat rooms. For example, a stalker may post a controversial or enticing message on the board under the name, phone number, or e-mail address of the victim, resulting in subsequent responses being sent to the victim. "The harm caused by 'cyber-smearing' is often far more serious than any equivalent offline acts. This is because information posted to the Internet is available to a huge audience and can remain easily accessible for a great deal of time". Finally, the time

scale over which a typical cyberstalking case unfolds. Again the lack of detailed evidence leads to differing speculations. Jenson argues "that as internet provides anonymity and simplicity for stalkers whereby, the cyberstalkers identity can be concealed which allows the cyberstalking to continue longer than offline stalking" (Jenson 1996), whilst it is possible to argue that cyberstalking cases take place over a shorter period.

# 8. Regulating Cyberstalking

Whilst significant, the above differences do not tell the whole story. The nature of the community and those who populate it are fundamentally different from the physical world such that the nature and form of any regulation should be different. What does this brief analysis of the nature of cyberstalking does is to enable us to reflect upon the nature of regulation required for this activity. Fundamentally the nature of cyberspace is such that it is seen to encourage stalking. However it can be argued that merely having the ability to do something does not necessarily motivate a person to carry out that action. As we previously suggested a key element in the cyber community is the sense of anonymity which reduces inhibitions, users of the internet often manifest reduced self-restraint and a significant percentage of them engage in behaviours in this medium that are not in concordance with social norms which includes both pro- and anti-social behaviour, including self-disclosure and cause variety of interpersonal behaviour (Bubaˇs 2001). It's well known that people engage in behaviors they would normally deem inappropriate in physical world. They feel more uninhibited, express themselves more openly. Researchers call this the 'disinhibition effect'. Kiesler S, Siegal J, and McGuire T.W, (1984) have argued that internet encourages anti-normative, aggressive, uninhibited behaviour.

> *"The most general cause of problematic behaviours when using Internet is related to the phenomenon of behavioural disinhibition. In face-to-face communication, individuals are constrained by the social rules that govern interpersonal interaction, immediate negative feedback, and visible consequences of their inappropriate behaviour, as well as by possible social sanctions. However, when using the Internet the users reside in relative anonymity and physical safety, distant from others in interaction, often unaware of their identities and personalities, as well as of the negative consequences of their risky or potentially damaging behaviour. This contributes to the expression of anger or aggression, inappropriate self-disclosure, or personal use of socially doubtful material on the Internet, like pornography."*

It is possible to offer several explanations for this, including the freedom to idealize that the lack of visual cues provides, the ability for communicators to choose which aspects of the self to disclose and when to disclose them, however, according to Kiesler et el (1984) "*computer-mediated communication seems to comprise some of the same conditions that are important for 'deindividuation'*" Furthermore, Rowland (2000) suggests:

> Over the last century there have been a number of social psychological studies of what has been termed `deindividuation', the state of alienation, reduced inhibition and lack of self-awareness which occurs when a personal sense of identity is overwhelmed and subjected to the group. (Rowland 2000).

Disinhibition experienced by many Internet users has been identified as a result of 'deindividuation'. Isolation is one of a number of factors that produce a condition that Zimbardo (1969) termed 'deindividuation'. "Deindividuation occurs when people are in anonymity-producing situations that reduce their concerns about being evaluated by others. They lose self-consciousness and, in turn, are more likely to do things that they would otherwise not do." (Diener 1980) It can be argued that when 'deindividuation' occurs, this actually increases the individual's sensitivity and disobedience to situational norms. These situational norms and cues would normally indicate what appropriate and desirable behaviour is in a particular context. "Hence deindividuation effects on private self awareness, as result of a group membership, can impair the ability to regulate one's behaviour." (Willison 2001). However, this view of the average internet user as deindividuated has been strongly criticised (Lea et al 1992). Although there is some evidence that both task-focus and negative, anti-social behaviour does occur; however Lea et al (1992) rejected the assumption that the lack of contextual cues and the relative anonymity lead to crass anti-normative behaviour, and argue that "…may represent a more intrinsically 'social' medium of communication than the apparently richer context of face-to-face interaction, and one that gives fuller rein to fundamentally social psychological factors." (Lea et al 1992).

Joinson (1998) criticised the idea that many Internet users may be deindividuated. He recommended from a social identity explanation of deindividuation effects an alternative explanation for the hostile or aggressive behaviour of some Internet users. Joinson (1998) cites Reicher (1984) to suggest *"most deindividuation effects reported by Zimbardo onwards can be explained without recourse to deindividuation. Anonymity, because of the lack of focus on the self as an individual, tends to lead to the activation of social identities rather than the activation of personal identities." "This would lead to the regulation of behaviour based on the norms associated with the salient social group."* (Joinson 1998 p.27). Many studies of online communities have described how groups develop norms for their interaction and that some users take on the norms associated with the social group(s) to which they belong. The term 'ways of speaking' is used in the ethnography of communication to describe how group values, beliefs and social structures are embodied in a culture's language form and use. If this stereotype is known to somebody identifying with that group, the person will strive to adhere to the group norms in order to stay in favour with the group.

McKenna and Bargh (2000) claim that "*it is not surprising then that de-individuation and the negative results that often accompany it … readily occur on the Internet*" so it is reasonable to believe that people belonging to groups in which aggression is not the exception, but the norm, and which promote hate speech or racist ideologies may eventually take on the norms of these groups and begin to behave accordingly. In this

view, group members following group norms that are at odds with wider social norms are not engaging in anti-normative behaviour.

> *When people pursue activities that are harmful to others for reasons of personal gain or social pressure, they avoid facing the harm they cause or minimize it. If minimization does not work, the evidence of harm can be discredited. As long as the harmful results of one's conduct are ignored, minimized, distorted or disbelieved, there is little reason for self-censure to be activated. It is easier to harm others when their suffering is not visible and when injurious actions are physically and temporally remote from their effects*." (Bandura 1999)

It can be argued that cyberspace helps to support such behaviour on pretext of anonymity and a false sense of power. Hidden in cyberspace is the mystery of the invisible hand of aggression, of control without authority.

The manifestation of this misconduct is most likely to be charged under statutes in place in the respective jurisdictions. The range of activities associated with cyber stalking is such that the content of emails and texts may contravene laws on pornography, blasphemy and incitement to racial hatred. The regulations relating to cyber stalking are merely an adaptation of existing laws to extend and cover the behaviours evident in cyber stalking. The UK's Criminal Justice and Police Act 2001 extends the Malicious Communications Act 1988 to include electronic communications. This is in addition to the relevance of specific computer crime offences created by the Computer Misuse Act 1990.[9] The Act was designed in a time of mainframes and terminals, but the offences are deemed sufficiently broad to cover several cyberstalking activities including internet stalking and computer stalking.[10] How effective then are the laws adapted from those primarily designed to deal with physical stalking? Comparisons with other cyber crimes show that for example SPAM increased following the introduction of the US anti-spam legislation (Gaudin 2004 cited by Wall 2004, p332). Using Wall's definitions of cyber crimes (Wall 2005, fn13) SPAM is true cyber crime and these may be less receptive to solution through strictly legal means. Cyber stalking which in Wall's terms is not a true cyber crime, does not seem to sit comfortably within the hybrid definition particularly when the impact of cyber society and deindividuation are considered. Brenner has taken a first step in this analysis by examining the nature of the behaviour in cyber crimes, she concludes:

> Unlike the offences heretofore discussed, cyber-stalking cannot be addressed simply by tweaking the principles we use to impose liability for stalking in the physical world…we have to create a new crime, one that encompasses the actus reus, mens rea and attendant circumstances characteristic of the activity we now call cyber-stalking. We can do this in two different ways: One is to revise the elements we use to impose liability for traditional stalking so that they remedy the deficiencies noted above and identify the result as a new crime: cyber-stalking. A better approach is to study the components of this activity as it exists and as we think it may come to exist, and parse these components into the constitutive

> elements (actus reus, mens rea, attendant circumstances and harm) of one or more new crimes" (Brenner 2001).

We respectfully agree, but would comment that this analysis moves from the assumption of criminalising the activity**,** and from considering regulation only through law. Cyberspace has as we commented earlier rekindled the debate between regulatory forms, often encapsulated in the terms East Coast (law) West Coast (technology) (Brownsword 2005, Brownsword 2006). Whilst writers vacillate between the two we would suggest that a wider analysis involving the nature of cyber communities would enable a consolidation of the three elements we consider fundamental to discussion of the nature of the regulation (role of self help etc.) required to deal with cyberstalking. The differences between physical and cyberstalking, the character of cyberspace and its community and the effects on the social inter-actions, the nature of social ties, and the scope of experience and reality. With such an analysis it is not obvious that either form of regulatory regime is appropriate, (Brownsword, 2006) nor is it obvious how formal legal identities and responsibilities can be imposed upon such "virtual" actors.

For example the scope, timescale and anonymity of the perpetrator of cyberstalking impact upon the harm suffered by the victim. The scale of the cyberstalking may be considerable in terms of its breadth, covering emails, chat rooms and even the victim's computer; this could be seen to be aggravated by the fact that the perpetrator is unknown to the victim. Yet the context is such that the threat is a non physical one and the victim may themselves have taken advantage of anonymity, may have created and furthered an imaginary character and life which is now the subject of the attack. To what extent is the victim who is happy to play the part of an imaginary character be able to complain if that character is stalked or indeed requisitioned by others, given that self help may be both simple and effective. What would be the place of traditional defences and sanctions in this scenario? To which legal identity does one impose regulation and liability? Political reactions to this situation often jump at measures aiming at restoring the transparency of potentially criminal behaviour without understanding the true nature of the crime and against whom it is being perpetrated. There is a symbiotic relationship between an individual and social identity which Goffman argued is based upon the categorisation of an individual to determine the acceptability of the membership of certain social group. The imaginary character and life of the victim has that social identity just because of belonging to a community that exits in the cyberspace. It is also the very anonymity of the internet that raises the question of what constitutes 'normal' and 'deviant'. In a society dominated by the social norms that protects 'social identity', any behaviour that infringes the 'norm' is deviant and is open to sanctions.

Regulation of cyberstalking will not only hinge upon laws which are flexible enough to deal with electronic harassment (Ellison 2001, p146). Cyberstalking is a relatively new criminal phenomenon. Often law enforcement agencies do not have the resources or the technology to deal with the offences. In several instances, victims have been told by the law enforcement agency simply to turn off their computers (Ellison 2001). Therefore victims of online harassment and threats, often in collaboration with victim service providers and advocates, have had to step in to fill the void by developing their own

informal support networks and informational websites to exchange information about how to respond to these crimes effectively (US Attorney-General 1999).

Further, many of the solutions to cyberstalking will come about through personal intervention. A mixed solution involving not only regulation but also a mix of personal and technological strategies.[11] A move to gender and age neutral identities would clearly reduce the risk of stalking, as again would the use of ISP's that provide specific policies, schemes and technological deterrents prohibiting harassment and abusive behaviour. Situational crime prevention, self help responses or joint activities between users and ISP's are not without their difficulties, those involving regulations or strategies are unlikely to be transparent or accountable as would legislation (Katyal 2003)**.**

While many may object that personal protection strategies are an infringement upon people's right to travel freely in cyberspace, the fact is that personal prevention is taken on a daily basis in the physical world, and the cyber world is no different and as Ogilvie (2000) argues people should therefore become more responsible and should follow simple strategies such as not providing personal information to strangers that are just as, if not more, applicable in cyber space. People who participate in the cyber world will minimise the likelihood of their being stalked by using techniques such as gender neutral and age neutral names. Personal information should not be recorded on the Internet and people should hesitate before filling in electronic forms which request names, age, addresses, together with personal likes and dislikes. Similarly, people can be pro-active before signing on to an ISP provider by researching beforehand on whether there are specific policies prohibiting harassment, abusive behaviours, and cyberstalking.
But this then must bring us back to regulation. Are we, as Brenner (2002) suggests, merely tinkering at the edges of the problem of regulation? For Wall (2004) the nature of the regulation depends upon the categorisation of the crime, for him a clear distinction can be made between pure and hybrid cyber crime, the former requiring "a mix of private legal action and technology", as he describes a "digital realist approach." This would lead us to subcategorise cyber stalking to differentiate between mere extension of physical stalking, where the victim is known to the stalker and technology is merely being used to provide new opportunities and pure cyber stalking, where the victim and stalker may be hidden in pseudo characters, in a virtual world far removed from reality. Whilst there would appear to be little to prevent the former hybrid stalking from being rightly brought within existing criminal law (stalking with new tools), it would be equally perverse to simply extend legislation to cover pure cyber stalking. As Lacey (2002) comments "

> Criminal Law is therefore implicitly justified not only in terms of its role in proscribing, condemning, and (perhaps) reducing conduct which causes or risks a variety of harms, but also in treating its subjects with respect, as moral agents whose conduct must be assessed in terms of attitudes and intentions and not merely in terms of effects.

Whether cyber stalking is considered a hybrid or as a pure cyber crime we would argue that the nature of the activity and the community requires a more radical review of the issues and not fall back on merely extending existing legislation and/or technological

solutions. Whereas a digital realist perspective would suggest that internet users should tolerate some stalking as users choose to enter cyberspace with knowledge of the nature of the community and pervasive anonymity, we would question whether the behaviour should be categorised as criminal. Is not this behaviour acceptable within that community? Put more starkly looking at the differences between physical and cyberstalking, the character of cyberspace and its community and the effects on the social inter-actions, the nature of social ties, and the scope of experience and reality - should we be criminalising or indeed even regulating this behaviour? In essence the question comes down to the perceived need to regulate this particular behaviour in cyberspace and criminalise this behaviour. The attraction of regulation depends very much on who one is, where one stands and the community in which this behaviour operates. Legislators and writers steeped in rule of law see the only solution to be some form of regulation fixed on legal identities (Lessig 1999, Bocji and McFarlane, L., Brownsword, 2006). Fixed within the physical world imposed, formal and bureaucratic regulation is a given. This need not be the case. Communities and activities thrive both within and without formal regulatory mechanisms, (Jones and Cameron, 2005, McCann, 1998). Cyberspace has stretched the applicability of such regulation beyond breaking point and we would question whether given the nature of the community and the often anonymous actors whether it is appropriate to impose a formal identity and regulation. There is a place for non regulatory environments, and cyberspace is such an example. Regulation may destroy the very form and nature of the behaviour and the environment will be left the poorer. Two examples may serve to illustrate the point. Firstly spam where East coast technologies could be used to prevent all unsolicited emails. However cyberspace with all spam removed would be a very different, and some would say poorer place (Wall, 2004). Secondly the opportunities for creativity in cyberspace and the clash with tradition rules of intellectual property. Whilst noting the oppressive nature of intellectual property regimes writers have struggled to hold down the emancipating role of cyberspace in the creative environment and have succumb to the need for some regulation albeit in a more limited form. (Lessig 2004, Gowers Review, 2006). Such watered down regulatory forms have failed to find favour with either the creative industries or the artists and are seen as used only by nerds or hobbyists. Regulation may therefore be at best futile and at worst damaging.

# 9. Conclusion

The main problem of the Cyberspace is linked to its ubiquitous nature and its immateriality: Cyberspace is not rooted in a kind of material reality; it is, instead, the result of its substitution with its iconic counterpart. The concept of border limits disappear and then the concept of nationality. The peculiarities of Cyberspace, particularly anonymity, mean it is not simply a question of transferring behaviours across from the physical world, communities in cyberspace are different and so is their behaviour. We would reiterate, the key concepts of social interaction, social bonding, and empirical experience differ in cyberspace from the physical world. Such differences

should inform the debate about the nature and form of regulation of cyberspace. The debate, we have argued has taken a wrong turn, and we would suggest the debate should now rethink the basic concepts upon which regulation is based. These boundaries between public and private law, between national and international law and between state law and self regulation, nor indeed the traditional positivist methodology of law, no longer offer an adequate intellectual framework in which to consider the nature and form of regulation in cyberspace. As with all analysis of the process and concept of law the foundation should be an investigation of the community over which the regulation is to apply, we cannot regulate cyberspace without an understanding of cyberspace. In the case of pure cyber stalking, the nature of the community, the activity and the actors lead us to the conclusion that rather than considering the form of the regulation we should considering whether there can be any regulation at all. Rather than accept inappropriate regulation we would urge that in relation to pure cyberstalking consideration be given to a regulatory free approach. As Bowrey (2005) comments in relation to the imposition of intellectual property rules in cyberspace "…a law free sign still has some currency in it…"

# References

Abercrombie, N and Longhurst, B (1998), Audiences, (London: Sage).
Alexander, Gregory S. (1989), Dilemmas of Group Autonomy: Residential Associations and Community, 75 *Cornell Law Review*, 1: 17–33

Bandura, A. (1999), 'Moral Disengagement in the Perpetration of Inhumanities,' *Personality and Social Psychology Review* 3:193–209.

Baudrillard, J. (1988), Selected Writings, edited by M. Poster, (Cambridge, Polity Press).
Bendle, M.F. (2002), 'The crisis of Identity in High Modernity', *British Journal of Sociology* 53: 1-18

Bocij, P. (2002), 'Corporate Cyberstalking: An invitation to build theory,' First Monday, 7/11, <http://firstmonday.org/issues/issue7_11/bocij/>

Bocij, P. (2003), 'Victims of cyber stalking: An exploratory study of harassment perpetrated via the Internet' 8/10 <http://firstmonday.org/issues/issue8_10/bocij/index.html>

Bocij, P. and McFarlane, L. (2002), 'Online harassment: Towards a definition of cyber stalking', *Prison Service Journal,* 139:31-38

Bocij, P. and McFarlane, L. (2002), 'Cyber stalking: Genuine problem or public hysteria?' *Prison Service Journal,* 140: 32-35

Bowrey, K. (2005) Law and Internet Cultures, (Cambridge University Press:Melbourne)

Brenner, S.W (2001), 'Is There Such a Thing as "Virtual Crime"?' California Criminal Law Revie*w* 4/1

Brownsword, R (2005) "Code, control, and choice: why East is East and West is West", *Legal Studies*) Vol.25 No 1, p.1.

Brownsword, R. (2006) Neither East Nor West, Is Mid-West Best? Script-ed Vol.1_Issue 3

Bryant, Rebecca (2001) What Kind of Space is Cyberspace?, Minerva - An Internet *Journal of Philosophy* 5 (2001): 138–155

Buba˘s, G. (2001), 'Computer Mediated Communication Theories and Phenomena: Factors that Influence Collaboration over the Internet'. Paper presented at the 3rd CARNet Users Conference, Zagreb.

Budd, T., Mattinson, J. and Myhill, A. (2000), 'The extent and nature of stalking: Findings from the 1998 British Crime Survey'. (London: Home Office Research, Development and Statistics Directorate).

Burgess W.A. and Baker T. (2002), 'Cyberstalking', in J. Boon and L. Sheridan eds., Stalking and Psychosexual Obsession: Psychological Perspectives For Prevention, Policing and Treatment. London: Wiley

Byassee, William S. (1995), 'Jurisdiction of Cyberspace: Applying Real World Precedent to the Virtual Community', 30 *Wake Forest Law Review* 197: 207–08

Calhoun, C. (1991), 'Indirect Relationships and Imagined Communities: Large-Scale Social Integration and the Transformation of Everyday Life' in Pierre Bourdieu and James S. Coleman eds., Social Theory for a Changing Society, (San Francisco- Oxford :Boulder).

Cerulo, K. A. (1997), 'Reframing Social Concepts for a Brave New (Virtual) World', Sociological Inquiry, 67/1: 48-58

Diener, E. (1980) Deindividuation: The absence of self-awareness and self-regulation in group members. In P. B. Paulus (Ed.), The psychology of group influence (pp. 209-242). Hillsdale, NJ: Lawrence Erlbaum

Ellison, Louise (2001), 'Cyberstalking:Tackling Harassment on the Internet', in David Wall (editor) Crime and the Internet, pp 141-151 (London: Routledge).

Fein, R., Vossekuil, B, and Holden, G. (1995), 'Threat Assessment: An Approach to Prevent Targeted Violence. National Institute of Justice: Research in Action', http://treas.gov/usss/ntac/ntac_threat.pdf

Finch, Emily (2002), 'What a tangled web we weave: Identity theft and the Internet' , in Yvonne Jewkes, ed., Dot. Cons, (Devon:Willan Publishing)

Froomkin, A. M. (1996), 'Flood Control On The Information Ocean: Living With Anonymity, Digital Cash And Distributed Databases', U. Pittsburgh Journal of Law and Commerce 15:395. Online via
<http://www.law.miami.edu/~froomkin/articles/ocean1.htm>

Gaudin, S (2004) U.S sending more than half of all spam. Internetnews.com 1 July. http://www.internetnews.com/stats/article.php/3376331

Gibson, W. (1984), Neuromancer, (London: Grafton)

Giordano, Philip (1998), 'Invoking Law as a Basis for Identity in Cyberspace', Stanford Technology Law Review, 1/ 8 http://stlr.stanford.edu/STLR/Articles/98_STLR_1/

Harvey, D (2003), 'Cyberstalking and Internet Harassment: What the Law Can Do', NetSafe II: Society, Safety, and the Internet Conference Proceedings, available at <http://www.netsafe.org.nz/downloads/conference/netsafepapers_davidharvey_cyberstalking.pdf>

Kuhn, T. (1996), The Structure of Scientific Revolutions, 3rd edition, (University of Chicago IL:Chicago Press).

Goffman, E (1963), Stigma: Notes on the Management of spoiled Identity, (Englewood Cliffs, NJ: Prentice-Hall)

Goffman, E (1959), The Presentation of Self in Everyday Life, (London: Penguin Books).

Goldsmith, Jack (1998), 'Against Cyberanarchy', *University of Chicago Law Review*, 65: 1239-40

Gowers Review of Intellectual Property (2006) *http://www.hm-treasury.gov.uk/independent_reviews/gowers_review_intellectual_property/gowersreview_index.cfm*

Jacobson, D. (1996) Contexts and cues in cyberspace: The pragmatics of naming in text-based virtual realities, Journal of Anthropological Research *52(4):* 461-79.
Jenson, B. (1996). Cyberstalking: Crime, Enforcement and Personal Responsibility of the On-Line World. *S.G.R. MacMillan*. Available at http://www.sgrm.com/art-8.htm

Johnson, David and Post, David (1997), 'And How Shall the Net Be Governed? A Meditation on the Relative Virtues of Decentralized, Emergent Law', in Brian Kahin and James Keller, eds., Coordinating the Internet 62 MIT Press

Joinson, A. (1998), 'Causes and Implications of Disinhibited Behaviour on the Internet,' in J. Gackenbach, ed., Psychology and the Internet: Intrapersonal, Interpersonal, and Transpersonal Implications, (San Diego, CA: Academic Press).

Katyal, N.K.(2003) Digital architecture as crime control. *Yale Law Journal*, 112 pp.2261-2289

Jones, R and Cameron, E. (2005) Full Fat, Semi-skimmed No Milk Today – Creative Commons Licences and English Folk Music, *International Review of Law, Computers and Technology*, (2005) Vol. 19 No 3, p.259-275.

Kiesler, S., Siegal, J. and McGuire, T. W. (1984) Social psychological aspects of computer mediated communication. American Psychologist, 39, 1123-1134

Lacey, N. "Legal Constructions of Crime" in The Oxford Handbook of Criminology, 3rd Ed. Maguire M. et al eds. OUP:Oxford, (2002)

Lea, M., O'Shea, T., Fung, P., and Spears, R. (1992) 'Flaming' in computer-mediated communication, in M. Lea (ed) Contexts in computer-mediated communication London: Harvester Wheatsheaf

Lessig, Lawrence (1998), 'What Things Regulate Speech: CDA 2.0 vs. Filtering', Jurimetrics Journal, 38/4*:* 629- 669

Lessig, L. (1999), *Code and Other Laws of Cyberspace*, (London:Routedge)

Lessig L. (2004) Free Culture. How Big Media Uses Technology and Law to Lock Down Culture and Control Creativity. Penguin: New York) 2004. and the Creative Common movement *http://creativecommons.org/about/legal/*

Maxwell, A. (2001), 'Cyberstalking' Auckland University Department of Psychology <http://www.netsafe.org.nz/ie/downloads/cyberstalking.pdf>

McCall, Randy (2003), 'Online Harassment and Cyberstalking: Victim Access to Crisis, Referral and Support Services in Canada Concepts and Recommendations', Victim Assistance Online Resources, available at <http://www.vaonline.org>

McCann, A., (1998) *Traditional Music and Copyright – The Issues.* Presented at "Crossing Boundaries," the seventh annual conference of the International Association for the Study of Common Property, Vancouver, British Columbia, Canada, June 10-14, 1998. page 9

McGrath, M. G. and Casey, E. (2002), 'Forensic Psychiatry And The Internet: Practical Perspectives On Sexual Predators and Obsessional Harassers In Cyberspace', Journal of the American Academy of Psychiatry and the Law, 20: 81-94.

McKenna, K.Y. A and Bargh, J (2000) "Plan 9 from Cyberspace: The implications of the Internet for personality and social psychology". *Personality and Social Psychology Review* 4.

Miller, N (2001), 'Stalking Laws and Implementation Practices: A National Review for Policymakers and Practitioners', Institute for Law and Justice, available at <http://www.ilj.org/stalking/FinalRpt.pdf>

Mitchell W (1995) *City of Bits- Space, Place and the Infobahn* ,114-5 as cited in Hunter D 2002 *Cyberspace as Place and the Tragedy of the Digital Anticommons* Project Report funded by Singapore Management University and The Wharton School, University of Pennsylvania April 2002

Mnookin, J. (1996), 'Virtual(ly) Law: Emergence of law on LambdMOO' in A. Branscomb, *ed.*, Special Issue on 'Emerging Law on the Electronic Frontier, Journal of Computer-Mediated Communication 2/1

O'Connell R, Price J and Barrow C (2004) Cyberstalking, Abusive Cyber Sex and Online Grooming: A Programme for Education of Teenagers, Cyberspace Research Unit, University of Lancaster, www.uclan.ac.uk/cru p.5-6

Ogilvie, Emma (2000), 'Cyberstalking Trends and Issues in Crime and Criminal Justice', 166 Australian Institute of Criminology, available at http://www.aic.gov.au/publications/tandi/ti166.pdf

Oldenburg, R. (1989), The Great Good Places. (New York: Paragon House).

Paliwala, A (2004), 'Information Society e-Legal Education: Integrating the Social Economic and Political Context' LEFIS Workshop Proceedings, University of Durham, <http://www.lefis.org>

Pathé, M. and Mullen, P. (1997) 'The impact of stalkers on their victims', British Journal of Psychiatry, 170:12-17

Petherick, W. (1999), 'Cyber-stalking: Obsessional pursuit and the Digital criminal', <http://www.crimelibrary.com/criminology/cyberstalking/index.html>

Post, David (2000), 'What Larry Doesn't Get: Code, Law and Liberty in Cyberspace' Stanford Law Review 52: 1439

Post, Robert C. (1997), 'Community and the First Amendment', 29 Arizona State Law Journal, 473.

Postman, N. (1992), Technopoly: The Surrender of Culture to Technology, (New York: Knopf).

Purcell, K. (1997), 'Towards a Communication Dialectic: Embedded Technology and the Enhancement of Place', *Sociological Inquiry*, 67/1:101-112

Reicher, S. D. (1984) "Social influence in the crowd: Attitudinal and behavioural effects of deindividuation in conditions of high and low group salience" *British Journal of Social Psychology*, 23, 341-350

Reid, E. (1995), 'Virtual Worlds: Culture and Imagination' in S. G. Jones ed., Cybersociety: Computer-Mediated Communication and Community' p.164-183. (London: Sage).

Reno, J. (1999), 'Cyber Stalking: A New Challenge for Law Enforcement and Industry', at <http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm >

Diane Rowland (2000) Anonymity, Privacy and Cyberspace, ttp://www.bileta.ac.uk/Document%20Library/1/Anonymity,%20Privacy%20and%20Cyberspace.pdf

Sheridan, L. Davies G. and Boon J , (2002). "The course and nature of stalking: A victim perspective," Howard Journal, volume 40, number 3, pp. 215-234

Sherizen, S. (1992) 'The End of the (ab)user Friendly Era' , NCCV: 39

Spitzberg, B.H. and Hoobler, G. (2002), 'Cyber stalking and the technologies of interpersonal terrorism', New Media and Society, 14/1:71-92.

Standage, T. (1998), The Victorian Internet, Walker: New York

Stern, S and Handel, Alysia D. (2001) Sexuality and mass media: the historical context of psychology's reaction to sexuality on the internet, *Journal of Sex Research*

Teller, P. (1991), 'Substance, Relations, and Arguments about the Nature of Space-Time', *Philosophical Review*, 100: 363-97

The All Party Internet Group (2004) , "Revision of the Computer Misuse Act." (2004) http://www.apig.org.uk/CMAReportFinalVersion1.pdf

Thomas, D. and Loader, B. (2000) Cybercrime: Law Enforcement, Security And Surveillance In The Information Age, (London: Routledge).

Thomsen, Steven R., Straubhaar, Joseph D. and Bolyard, Drew M. (1998), 'Ethnomethodology and the study of online communities: exploring the Cyber Streets' *Information Research*, 4/1.

Turkle, Sherry (1996), 'Virtuality and its Discontents: Searching for community in Cyberspace', The American Prospect, 24: 50-57.

United States Attorney General (1999) *Report on Cyberstalking- A New Challenge for Law Enforcement and Industry*. Available at www.usdoj.gov/criminal/cybercrime/cyberstalking.htm

Wall, D.S. (2004) "Digital Realism and the Governance of Spam as Cybercrime" *European Journal on Criminal Policy and Research* (2004) 10;309-355.

Wall, D.S. (2005) The Internet as a conduit for criminals. In A. Pattavina (Ed.) *Information Technology and the Criminal Justice System*, 77-98. Thousand Oaks, CA: Sage.

Williams M (2004) The language of cybercrime in David Wall (editor) *Crime and the Internet* , London: Routledge, p 153

Willison, R. (2001), 'The Unaddressed Problem of Criminal Motivation in is Security: Expanding the Preventive Scope through the Concept of Readying,' Working Paper Series, (London: London School of Economics).

Young, M. (2001), 'Psychological Trauma of Crime Victimization: Victim Assistance Frontiers and Fundamentals', National Organization for Victim Assistance, http://www.try-nova.org/Victims/Trauma.pdf

Zimbardo, P. G. (1969). The human choice: Individuation, reason, and order vs. deindividuation, impulse and chaos in W. J. Arnold & D. Levine (Eds.), Nebraska symposium on motivation Lincoln: University of Nebraska Press,(pp. 237-307

Zona, M.A., Sharma, K.K., & Lane, M.D. (1993) "A Comparative Study of Erotomanic and Obsessional Subjects in a Forensic Sample" *Journal of Forensic Sciences*, 38, p. 894 – 903 http://www.crimelibrary.com/criminal_mind/psychology/cyberstalking/1.html

# End Notes

[1] *Ebay Inc v Bidders Edge Inc*, 100 F. Supp. 2d 1058 (N.D. Cal. 2000) , *America Online Inc v. LCGM Inc.* Civ. Act. No. 98-102-A, (E.D. Va., Nov. 10, 1998) S*hetland Times v Wills* [1997] FSR 604

[2] Those critical of such a view, including Goldsmith, argued that cyberspace was not a unique challenge, that similar challenges had been resolved by unexceptional jurisdictional rules and legal mechanisms derived from conflict of laws. Transactions in cyberspace, it is argued, are no different from those occurring in the "physical space" of international trade or international crimes. (Goldsmith 1998)

[3] Lessig (1999) argues a community based on code

[4] A large number of self help and self regulatory bodies exist on the internet to deal with harassment and stalking. Internet users can use blocking and filtering systems. 'Net Nanny', 'Safe Surf, Surf Watch provide directories of offensive sites, Internet Watch and Cyber Angels provide mechanisms for reporting offenders.

[5] Parts of this section are drawn from Bocij (2002) and are used with his permission.

[6] *http://www.cps.gov.uk/Home/LegalGuidance/5/5-E.pdf* as cited in O'Connell et al (2004)

[7] It is somewhat ironic that the latest forms of cyber stalking have reverted to the telephone network given the internet has grown out of this network. (Standage 1998).

[8] Jenson, B. (1996). Cyberstalking: Crime, Enforcement and Personal Responsibility of the On-Line World. *S.G.R. MacMillan*. Available at http://www.sgrm.com/art-8.htm

[9] The 1990 Act creates three new offences, unauthorised access (s.1), unauthorised access with intent to commit or facilitate the commission of further offences (s.2) and unauthorised modification of computer material (s.3)

[10] The All Party Internet Group (2004) of Parliament was of the view that the Act had adapted to contemporary events reasonably well .

[11] Purely technological solutions could make matters worse by hardening the resolve of the stalker**.**